II

(Icke-lagstiftningsakter)

BESLUT

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2022/254

av den 17 december 2021

enligt Europaparlamentets och rådets förordning (EU) 2016/679 om Sydkoreas adekvata skyddsnivå för personuppgifter enligt lagen om skydd av personuppgifter

[delgivet med nr C(2021) 9316]

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) ([1]), särskilt artikel 45.3, och

av följande skäl:

1. INLEDNING

(1) I förordning (EU) 2016/679 fastställs regler för överföring av personuppgifter från personuppgiftsansvariga eller personuppgiftsbiträden i Europeiska unionen till tredjeländer och internationella organisationer i den mån sådana överföringar omfattas av förordningens tillämpningsområde. Reglerna om internationella överföringar av uppgifter fastställs i kapitel V (artiklarna 44–50) i den förordningen. Flödet av personuppgifter till och från länder utanför Europeiska unionen är av avgörande betydelse för att utvidga den gränsöverskridande handeln och det internationella samarbetet, men skyddet av personuppgifter i unionen får inte undergrävas av överföringar till tredjeländer ([2]).

(2) Enligt artikel 45.3 i förordning (EU) 2016/679 får kommissionen genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer i ett tredjeland eller en internationell organisation säkerställer en adekvat skyddsnivå. Enligt detta villkor får överföring av personuppgifter till ett tredjeland ske utan ytterligare tillstånd enligt artikel 45.1 och skäl 103 i förordning (EU) 2016/679.

(3) Enligt artikel 45.2 i förordning (EU) 2016/679 måste antagandet av ett beslut om adekvat skyddsnivå grundas på en omfattande analys av tredjelandets rättsordning som omfattar både de regler som är tillämpliga på uppgiftsinförare och begränsningarna och skyddsåtgärderna när det gäller myndigheters tillgång till personuppgifter. I sin bedömning måste kommissionen avgöra om det berörda tredjelandet garanterar en skyddsnivå som ”i allt väsentligt är likvärdig” med den som säkerställs inom Europeiska unionen (skäl 104 i förordning (EU) 2016/679). Huruvida så är fallet ska bedömas mot unionens lagstiftning, särskilt förordning (EU) 2016/679, samt rättspraxis från Europeiska unionens domstol ([3]).

([1]) EUT L 119, 4.5.2016, s. 1.
([2]) Se skäl 101 i förordning (EU) 2016/679.
([3]) Se det senaste målet C-311/18, Facebook Ireland och Schrems (*Schrems II*), ECLI:EU:C:2020:559.

(4) Enligt Europeiska unionens domstol kräver detta inte att en identisk skyddsnivå uppnås ([4]). I synnerhet kan de medel som tredjelandet i fråga har till sitt förfogande för att skydda personuppgifter skilja sig från dem som används i unionen förutsatt att de i praktiken visar sig vara effektiva för att säkerställa en adekvat skyddsnivå ([5]). Standarden för en adekvat skyddsnivå kräver därför inte att unionens regler kopieras till punkt och pricka. Snarare gäller det att avgöra huruvida det utländska systemet som helhet erbjuder den höga skyddsnivå som krävs med avseende på innehållet i rätten till personlig integritet och genomförandet, tillsynen och verkställandet av dem i praktiken ([6]). Europeiska dataskyddsstyrelsens referensram för adekvat skyddsnivå, som syftar till att ytterligare förtydliga denna standard, ger också vägledning i detta avseende ([7]).

(5) Kommissionen har noggrant analyserat sydkoreansk lagstiftning och praxis. På grundval av de resultat som anges i skälen 8–208 drar kommissionen slutsatsen att Sydkorea säkerställer en adekvat skyddsnivå för personuppgifter som överförs från personuppgiftsansvariga eller personuppgiftsbiträden i unionen ([8]) till enheter (t.ex. fysiska eller juridiska personer, organisationer, offentliga institutioner) i Sydkorea som omfattas av lagen om skydd av personuppgifter (lag nr 10465 av den 29 mars 2011, senast ändrad genom lag nr 16930 av den 4 februari 2020). Detta inbegriper både personuppgiftsansvariga och personuppgiftsbiträden (som kallas ”uppdragstagare” ([9])) i den mening som avses i förordning (EU) 2016/679. Beslutet om adekvat skyddsnivå omfattar inte religiösa organisationers behandling av personuppgifter för missionsverksamhet och politiska partiers nominering av kandidater, eller behandling av personlig kreditinformation enligt lagen om kreditinformation som utförs av personuppgiftsansvariga under tillsyn av kommittén för finanstjänster.

(6) I denna slutsats beaktas de ytterligare skyddsåtgärder som anges i meddelande nr 2021-5 (bilaga I) och den sydkoreanska regeringens officiella framställningar, utfästelser och åtaganden till kommissionen (bilaga II).

(7) Genom detta beslut får överföringar till personuppgiftsansvariga och personuppgiftsbiträden i Sydkorea äga rum utan ytterligare tillstånd. Detta påverkar inte den direkta tillämpningen av förordning (EU) 2016/679 på sådana enheter, när villkoren för förordningens territoriella tillämpningsområde som anges i artikel 3 är uppfyllda.

2. REGLER FÖR BEHANDLING AV PERSONUPPGIFTER

2.1 Det Sydkoreanska regelverket för skydd av personuppgifter

(8) Den ordning som styr rätten till personlig integritet och dataskydd i Sydkorea har sina rötter i den sydkoreanska författningen som fastslogs den 17 juli 1948. Även om rätten till skydd av personuppgifter inte uttryckligen anges i författningen erkänns den ändå som en grundläggande rättighet som härrör från de författningsenliga rättigheterna till mänsklig värdighet och strävan efter lycka (artikel 10), privatliv (artikel 17) och personlig integritet vid kommunikation (artikel 18). Detta har bekräftats av både högsta domstolen ([10]) och författningsdomstolen ([11]). Grundläggande rättigheter och friheter (däribland rätten till integritet) får endast får begränsas genom lag när det är nödvändigt för den nationella säkerheten eller för upprätthållandet av lag och ordning för den allmänna välfärden, och begränsningarna får inte påverka det väsentliga innehållet i friheten eller rätten (artikel 37.2).

([4]) Mål C-362/14, Maximilian Schrems/Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650, punkt 73.
([5]) Schrems-målet, punkt 74.
([6]) Se meddelandet från kommissionen till Europaparlamentet och rådet om utbyte och skydd av personuppgifter i en globaliserad värld (COM(2017) 7 final, 10.1.2017), avsnitt 3.1, s. 6–7.
([7]) Europeiska dataskyddsstyrelsen, Adequacy Referential, WP 254 rev. 01. Finns på följande länk: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) Detta beslut har betydelse för EES. Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Gemensamma EES-kommitténs beslut om införlivande av förordning (EU) 2016/679 i bilaga XI till EES-avtalet antogs av gemensamma EES-kommittén den 6 juli 2018 och trädde i kraft den 20 juli 2018. Förordningen omfattas således av det avtalet. I beslutet bör hänvisningar till EU och EU:s medlemsstater sålunda anses omfatta även EES-staterna.
([9]) Se avsnitt 2.2.3 i detta beslut.
([10]) Se t.ex. högsta domstolens beslut nr 2014Da77970 av den 15 oktober 2015 (en engelsk sammanfattning finns under ”Lawmaker’s disclosure of teachers’ trade union members case” på https://www.privacy.go.kr/eng/enforcement_01.do) och den rättspraxis som det hänvisas till i beslutet, bl.a. beslut nr 2012Da49933 av den 24 juli 2014.
([11]) Se särskilt författningsdomstolens beslut nr 99Hun-ma513 av den 26 maj 2005 (en engelsk sammanfattning finns på http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) och beslut nr 2014JHun-ma449 2013Hun-Ba68 (konsoliderad) av den 23 december 2015 (en engelsk sammanfattning finns under ”Change of resident registration number case” på https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Även om det på olika ställen i författningen hänvisas till sydkoreanska medborgares rättigheter har författningsdomstolen fastställt att även utländska medborgare har grundläggande rättigheter ([12]). Domstolen ansåg särskilt att skyddet av den personliga värdigheten och människovärdet samt rätten att sträva efter lycka är alla människors rättigheter och inte bara medborgarnas ([13]). Enligt de officiella framställningarna från den sydkoreanska regeringen ([14]) är det dessutom allmänt erkänt att grundläggande mänskliga rättigheter föreskrivs i artiklarna 12–22 i författningen (bl.a. integritetsskydd) ([15]). Även om det hittills inte finns någon rättspraxis som specifikt rör utländska medborgares rätt till integritet har denna rättighet sin grund i skyddet av mänsklig värdighet och strävan efter lycka, vilket stöder denna slutsats ([16]).

(10) Dessutom har Sydkorea antagit en rad lagar på dataskyddsområdet som innehåller skyddsåtgärder för alla individer, oavsett nationalitet ([17]). Vid tillämpning av detta beslut är följande lagar tillämpliga:

— Lagen om skydd av personuppgifter (PIPA), *personal information protection act)*.

— Lagen om användning och skydd av kreditinformation ([18]).

— Lagen om integritetsskydd inom kommunikation.

(11) PIPA utgör den allmänna rättsliga ramen för skydd av personuppgifter i Sydkorea. Den kompletteras av en genomförandedekret (presidentdekret nr 23169 av den 29 september 2011, senast ändrad genom presidentdekret nr 30892 av den 4 augusti 2020) (genomförandedekret till PIPA), som liksom PIPA är rättsligt bindande och verkställbart.

(12) Dessutom innehåller föreskrivande meddelanden som antagits av nämnden för skydd av personuppgifter (*nämnden*) ytterligare bestämmelser om tolkning och tillämpning av PIPA. På grundval av artikel 5 (statens förpliktelser) och artikel 14 i PIPA (Internationellt samarbete) antog nämnden för skydd av personuppgifter meddelande nr 2021-5 av den 1 september 2020 (i dess ändrade lydelse enligt nr 2021-1 av den 21 januari 2021 och meddelande nr 2021-5 av den 16 november 2021, meddelande nr 2021-5) om tolkning, tillämpning och verkställighet av vissa bestämmelser i PIPA. Detta meddelande innehåller förtydliganden som gäller all behandling av personuppgifter enligt PIPA samt ytterligare skyddsåtgärder för personuppgifter som överförs till Sydkorea på grundval av detta beslut. Meddelandet är rättsligt bindande för personuppgiftsansvariga och kan verkställas av både nämnden för skydd av personuppgifter och domstolarna ([19]). En överträdelse av reglerna i meddelandet innebär en överträdelse av de relevanta bestämmelserna i PIPA som de kompletterar. Innehållet i de kompletterande skyddsåtgärderna analyseras därför som en del av bedömningen av de relevanta artiklarna i PIPA. Slutligen ges ytterligare vägledning om PIPA och dess genomförandedekret, som präglar tillämpning och verkställande av dataskyddsreglerna i PIPA, i handboken och riktlinjerna för PIPA som antagits av nämnden för skydd av personuppgifter ([20]).

([12]) Författningsdomstolens beslut nr 93Hun-MA120 av den 29 december 1994.

([13]) Författningsdomstolens beslut nr 99HeonMa494 av den 29 november 2001.

([14]) Se avsnitt 1.1 i bilaga II.

([15]) Se även artikel 1 i lagen om skydd av personuppgifter som uttryckligen hänvisar till ”enskildas friheter och rättigheter”. Närmare bestämt anges att syftet med en sådan lag är ”att sörja för behandling och skydd av personuppgifter i syfte att skydda enskildas frihet och rättigheter och att ytterligare förverkliga enskildas värdighet och värde”. I artikel 5.1 i lagen om skydd av personuppgifter fastställs på samma sätt statens ansvar att ”utforma politiska åtgärder för att förebygga skadliga effekter av insamling som går utöver ändamålet, missbruk och felaktig användning av personuppgifter, genomgripande övervakning och förföljelse osv. samt att stärka människors värdighet och den personliga integriteten”.

([16]) Dessutom föreskrivs i artikel 6.2 i författningen att utländska medborgares ställning garanteras i enlighet med internationell rätt och internationella fördrag. Sydkorea har anslutit sig till flera internationella avtal som garanterar rätten till integritet, t.ex. den internationella konventionen om medborgerliga och politiska rättigheter (artikel 17), konventionen om rättigheter för personer med funktionsnedsättning (artikel 22) och konventionen om barnets rättigheter (artikel 16).

([17]) Detta inbegriper regler som är relevanta för skyddet av personuppgifter men som inte tillämpas i en situation där personuppgifter samlas in i unionen och överförs till Sydkorea enligt förordning (EU) 2016/679, t.ex. i lagen om skydd, användning osv. av lokaliseringsuppgifter.

([18]) Syftet med denna lag är att verka för en sund kreditinformationsverksamhet, främja effektivt utnyttjande och systematisk hantering av kreditinformation och skydda den personliga integriteten mot missbruk och felaktig användning av kreditinformation (artikel 1 i lagen).

([19]) T.ex. har sydkoreanska domstolar uttalat sig om efterlevnad av reglerande meddelanden i ett antal fall, bl.a. genom att ställa sydkoreanska personuppgiftsansvariga till ansvar för att överträtt ett meddelande (se t.ex. högsta domstolens beslut nr 2018Da219406 av den 25 oktober 2018 i vilket domstolen ålade en personuppgiftsansvarig att betala ersättning till enskilda för skador orsakade av en överträdelse av ”meddelande om standarden för åtgärder som garanterar säkerhet för personuppgifter”; se även högsta domstolens beslut nr 2018Da219352 av den 25 oktober 2018; högsta domstolens beslut nr 2011Da24555 av den 16 maj 2016; centrala distriktsdomstolen i Seoul, beslut nr 2014Gahap511956 av den 13 oktober 2016; centrala distriktsdomstolen i Seoul, beslut nr 2009Gahap43176 av den 26 januari 2010).

([20]) Artikel 12.1 i PIPA.

(13) I lagen om användning och skydd av kreditinformation (*Act on the Use and Protection of Credit Information*) fastställs dessutom särskilda regler som gäller både för ”vanliga” kommersiella operatörer och specialiserade enheter inom finanssektorn när de behandlar personlig kreditinformation, dvs. information som krävs för att fastställa parters kreditvärdighet i finansiella eller kommersiella transaktioner. Detta inbegriper särskilt namn, kontaktuppgifter, finansiella transaktioner, kreditbetyg, försäkringsstatus eller lånebalans när sådan information används för att fastställa en persons kreditvärdighet ([21]). Om sådan information däremot används för andra ändamål (t.ex. mänskliga resurser) tillämpas PIPA i sin helhet. När det gäller de särskilda bestämmelserna om dataskydd i lagen om användning och skydd av kreditinformation övervakas efterlevnaden delvis av nämnden för skydd av personuppgifter (för kommersiella organisationer, se artikel 45-3 i lagen om användning och skydd av kreditinformation) och delvis av kommittén för finanstjänster ([22]) (för finanssektorn, bl.a. kreditvärderingsinstitut, banker, försäkringsbolag, ömsesidiga sparbanker, specialiserade företag inom kreditfinansiering, företag som erbjuder finansieringstjänster, företag inom värdepappersfinansiering, kreditkassor osv., se artikel 45.1 i lagen om användning och skydd av kreditinformation och artikel 36-2 i genomförandedekreteten till lagen om användning och skydd av kreditinformation). I detta avseende är tillämpningsområdet för detta beslut begränsat till kommersiella operatörer som är föremål för tillsyn av nämnden för skydd av personuppgifter ([23]). De särskilda regler i lagen om användning och skydd av kreditinformation som är tillämpliga i detta sammanhang (de allmänna reglerna i PIPA tillämpas om särskilda regler saknas) beskrivs i avsnitt 2.3.11.

2.2 **Materiellt och personligt tillämpningsområde för PIPA**

(14) Om inte annat uttryckligen föreskrivs i andra rättsakter regleras skyddet av personuppgifter i PIPA (artikel 6). Dess materiella och personliga tillämpningsområde bestäms av de fastställda begreppen ”personuppgifter”, ”behandling” och ”personuppgiftsansvarig”.

2.2.1 *Definition av personuppgifter*

(15) I artikel 2.1 i PIPA definieras personuppgifter som uppgifter om en levande person som direkt identifierar personen, t.ex. hans eller hennes namn, nummer i folkbokföringsregistret eller avbild, eller som indirekt identifierar personen, dvs. där uppgifter som i sig inte kan identifiera en viss person enkelt kan kombineras med andra uppgifter. Huruvida informationen ”enkelt” kan kombineras beror på om en sådan kombination rimligtvis är sannolik med beaktande av möjligheten att erhålla andra uppgifter samt den tid, kostnad och teknik som krävs för att identifiera en person.

(16) Dessutom betraktas pseudonymiserade uppgifter (dvs. uppgifter som inte kan identifiera en viss person utan att användas eller kombineras med ytterligare uppgifter för att återställa dem till deras ursprungliga tillstånd) som personuppgifter enligt PIPA (artikel 2.1 c i PIPA). Omvänt utesluts uppgifter som är helt ”anonymiserade” från tillämpningsområdet för PIPA (artikel 58-2 i PIPA). Detta gäller för uppgifter som inte kan identifiera en viss person även om de kombineras med andra uppgifter, med beaktande av den tid, kostnad och teknik som rimligen krävs för identifiering.

(17) Detta motsvarar det materiella tillämpningsområdet för förordning (EU) 2016/679 och dess begrepp ”personuppgifter”, ”pseudonymisering” ([24]) och ”anonymiserad information” ([25]).

([21]) Artikel 2.1 i lagen om användning och skydd av kreditinformation.

([22]) Kommittén för finanstjänster är Sydkoreas tillsynsmyndighet för finanssektorn och i denna egenskap upprätthåller den även lagen om användning och skydd av kreditinformation.

([23]) Om detta skulle ändras i framtiden, t.ex. genom att utvidga nämndens behörighet till att omfatta all behandling av personlig kreditinformation inom ramen för lagen om användning och skydd av kreditinformation, skulle överväganden kunna göras om att ändra beslutet om adekvat skyddsnivå så att det även omfattar de enheter som för närvarande är föremål för tillsyn av kommittén för finanstjänster.

([24]) I PIPA betraktas ”pseudonymiserad behandling” som behandling med metoder som att delvis radera personuppgifter eller helt eller delvis ersätta personuppgifter på ett sådant sätt att ingen specifik person kan igenkännas utan ytterligare uppgifter (artikel 2.1–2.2 i PIPA). Detta motsvarar definitionen av pseudonymisering i artikel 4.5 i förordning (EU) 2016/679, där det hänvisas till ”behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person”.

([25]) I skäl 26 i förordning (EU) 2016/679 klargörs särskilt att förordningen inte är tillämplig på anonymiserade uppgifter, dvs. uppgifter som inte rör en identifierad eller identifierbar fysisk person. Detta beror i sin tur på alla medel som med rimlig sannolikhet kan komma att användas, antingen av den personuppgiftsansvarige eller av en annan person, för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om sådana medel med rimlig sannolikhet kan komma att användas måste man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen.

2.2.2 *Definition av behandling*

(18) Begreppet ”behandling” har getts en vid definition i PIPA där det omfattar ”insamling, generering, förening, sammankoppling, upptagning, lagring, bevarande, mervärdesbehandling, redigering, åtkomst, utmatning, rättelse, återvinning, användning, tillhandahållande och utlämnande, förstörelse av personuppgifter samt annan, liknande verksamhet” ([26]). Även om vissa bestämmelser i PIPA endast avser särskilda typer av behandling, såsom ”användning”, ”tillhandahållande” eller ”insamling” ([27]), tolkas begreppet ”användning” som att det omfattar alla typer av behandling förutom ”insamling” eller ”tillhandahållande (till tredje part)”. Denna vida tolkning av ”användning” säkerställer därmed att det inte finns några luckor i skyddet när det gäller specifik behandling. Begreppet behandling motsvarar därför samma begrepp som enligt förordning (EU) 2016/679.

2.2.3 *Personuppgiftsansvarig och "uppdragstagare"*

(19) PIPA är tillämplig på personuppgiftsansvariga. I likhet med förordning (EU) 2016/679 omfattar detta alla offentliga institutioner, juridiska personer, organisationer eller enskilda personer som direkt eller indirekt behandlar personuppgifter för att handha personuppgiftsregister som en del av sin verksamhet ([28]). I detta sammanhang avses med ”personuppgiftsregister” ”en personuppgift eller personuppgifter som ordnas eller organiseras på ett systematiskt sätt enligt en viss regel för enkel tillgång till personuppgifterna” (artikel 2.4 i PIPA) ([29]). Internt är den personuppgiftsansvarige skyldig att utbilda de personer som deltar i behandlingen under hans eller hennes ledning, t.ex. företagets tjänstemän eller anställda, och att utöva lämplig kontroll och tillsyn (artikel 28.1 i PIPA).

(20) Särskilda skyldigheter gäller när en personuppgiftsansvarig (*uppdragsgivaren*) lägger ut behandlingen av personuppgifter på tredje part (*uppdragstagaren*). I synnerhet måste uppdraget styras av ett rättsligt bindande arrangemang (vanligtvis ett avtal) ([30]) där det utkontrakterade arbetets omfattning fastställs, liksom ändamålet med behandlingen, de tekniska och administrativa skyddsåtgärder som ska tillämpas, den personuppgiftsansvariges tillsyn, skadeståndsansvar (t.ex. ersättning för skador som orsakats av brott mot avtalsförpliktelser) samt begränsningarna för eventuell underentreprenad ([31]) (artikel 26.1 och 26.2 i PIPA jämförd med artikel 28.1 i genomförandedekretet) ([32]).

(21) Personuppgiftsansvariga måste dessutom offentliggöra och kontinuerligt uppdatera uppgifter om utkontrakterat arbete och uppdragstagarens identitet eller, i den mån den utkontrakterade behandlingen avser direktmarknadsföring, direkt meddela relevant information till enskilda personer (artikel 26.2 och 26.3 i PIPA jämförd med artikel 28.2–28.5 i genomförandedekretet) ([33]).

(22) I enlighet med artikel 26.4 i PIPA jämförd med artikel 28.6 i genomförandedekretet är personuppgiftsansvariga dessutom skyldiga att ge uppdragstagaren ”utbildning” om nödvändiga säkerhetsåtgärder och att bl.a. genom kontroller övervaka huruvida uppdragstagaren fullgör alla den personuppgiftsansvariges skyldigheter enligt PIPA ([34]) samt enligt avtalet om utkontraktering. Om uppdragstagare orsakar skada på grund av en överträdelse av PIPA kommer deras agerande eller passivitet att tillskrivas den personuppgiftsansvarige när det gäller ansvarsfrågan, på samma sätt som när det gäller en anställd (artikel 26.6 i PIPA).

([26]) Artikel 2.2 i PIPA.
([27]) T.ex. avses i artiklarna 15–19 i PIPA endast insamling, användning och tillhandahållande av personuppgifter.
([28]) Artikel 2.5 i PIPA. Offentliga institutioner i den mening som avses i PIPA omfattar alla centrala förvaltningsavdelningar eller förvaltningsmyndigheter och därtill knutna organ, lokala myndigheter, skolor och lokala offentliga företag med statlig finansiering samt parlamentets och rättsväsendets förvaltningsorgan (inklusive författningsdomstolen) (artikel 2.6 i PIPA jämförd med artikel 2 i genomförandedekretet till PIPA).
([29]) Detta motsvarar det materiella tillämpningsområdet för förordning (EU) 2016/679. Enligt artikel 2.1 i förordning (EU) 2016/679 ska förordningen tillämpas på ”behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register”. I artikel 4 led 6 i förordning (EU) 2016/679 definieras ”register” som ”en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier”. I enlighet med detta förklaras i skäl 15 att skyddet för enskilda bör vara tillämpligt på ”både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.”
([30]) Se handboken för PIPA, kapitel III, avsnitt 2 om artikel 26 (s. 203–212), där det förklaras att artikel 26.1 i PIPA avser bindande arrangemang, såsom avtal eller liknande arrangemang.
([31]) Enligt artikel 26.5 i PIPA är det förbjudet för personuppgiftsbiträden att använda personuppgifter som ligger utanför det utkontrakterade arbetets tillämpningsområde, eller att lämna ut personuppgifter till en tredje part. Underlåtenhet att iaktta detta krav kan leda till straffrättsliga påföljder enligt artikel 71 led 2 i PIPA.
([32]) Underlåtenhet att uppfylla detta krav kan leda till böter, se artikel 75.4 led 4 i PIPA.
([33]) Underlåtenhet att uppfylla detta krav kan leda till böter, se artikel 75.2.1 och 75.4.5 i PIPA.
([34]) Se även artikel 26.7 i PIPA, enligt vilken artiklarna 15–25, 27–31, 33–38 och 50 i tillämpliga delar ska tillämpas på personuppgiftsbiträden.

(23) Även om olika begrepp för ”personuppgiftsansvariga” och ”personuppgiftsbiträden” därmed inte används i PIPA fastställs i reglerna om utkontraktering skyldigheter och skyddsåtgärder som i huvudsak motsvarar de som reglerar förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden enligt förordning (EU) 2016/679.

2.2.4 *Särskilda bestämmelser för leverantörer av informations- och kommunikationstjänster*

(24) PIPA är tillämplig på all behandling av personuppgifter som utförs av personuppgiftsansvariga, men vissa bestämmelser innehåller särskilda regler (som lex specialis) för ”leverantörer av informations- och kommunikationstjänster” vid behandling av ”användares” personuppgifter ([35]). Begreppet ”användare” omfattar enskilda personer som använder informations- och kommunikationstjänster (artikel 2.1.4 i lagen om främjande av användning av nätverk för information och kommunikation och om skydd av information, nätlagen). Detta kräver att personen antingen direkt använder telekommunikationstjänster som tillhandahålls av en sydkoreansk teleoperatör eller använder informationstjänster ([36]) som tillhandahålls kommersiellt (dvs. i vinstsyfte) av en enhet som i sin tur förlitar sig på tjänster som tillhandahålls av en teleoperatör som är licensierad/registrerad i Sydkorea ([37]). I båda fallen är den enhet som är bunden av de särskilda bestämmelserna i PIPA en enhet som erbjuder en onlinetjänst direkt till en enskild person (dvs. en användare).

(25) Omvänt gäller ett beslut om adekvat skyddsnivå uteslutande den skyddsnivå som ges för personuppgifter som överförs från en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen till en enhet i ett tredjeland (här: Sydkorea). I det senare fallet kommer enskilda inom unionen normalt endast att ha ett direkt förhållande till uppgiftsutföraren i unionen och inte till någon sydkoreansk leverantör av informations- och kommunikationstjänster ([38]). Därför kommer de särskilda bestämmelserna i PIPA i fråga om personuppgifter rörande användare av informations- och kommunikationstjänster endast i begränsade fall att tillämpas på personuppgifter som överförs enligt detta beslut.

2.2.5 *Undantag från vissa bestämmelser i PIPA*

(26) Enligt artikel 58.1 i PIPA är en del av PIPA (dvs. artiklarna 15–57) inte tillämplig när det gäller fyra kategorier av databehandling ([39]). Särskilt tillämpas inte de delar av PIPA som berör de särskilda grunderna för behandling, vissa skyldigheter avseende dataskydd, detaljerade regler för utövandet av enskildas rättigheter samt de regler som styr tvistlösning genom kommittén för tvistlösning avseende personuppgifter. Andra grundläggande bestämmelser i PIPA är fortfarande tillämpliga, särskilt de allmänna bestämmelserna om dataskyddsprinciper (artikel 3 i PIPA) – bl.a. principerna om laglighet, angivande av ändamål och ändamålsbegränsning, uppgiftsminimering, uppgifternas korrekthet och säkerhet – och enskildas rättigheter (tillgång, rättelse, radering och upphörande, se artikel 4 i PIPA). Genom artikel 58.4 i PIPA införs även särskilda skyldigheter avseende sådan behandling, nämligen när det gäller uppgiftsminimering, begränsad lagring av uppgifter, säkerhetsåtgärder och hantering av klagomål ([40]). Till följd av detta kan enskilda personer fortfarande inge ett klagomål till nämnden för skydd av personuppgifter om dessa principer och skyldigheter inte uppfylls, och nämnden för skydd av personuppgifter har befogenhet att vidta verkställighetsåtgärder i händelse av bristande efterlevnad.

([35]) Se särskilt artikel 18.2 och kapitel VI i PIPA.

([36]) Informationstjänster omfattar både tillhandahållande av information och förmedlingstjänster för tillhandahållande av information.

([37]) Se artikel 2.1.3 (jämförd med artikel 2.1 led 2 och 4) i nätlagen och artikel 2.6 och 2.8 i lagen om telekomoperatörer.

([38]) Om sydkoreanska leverantörer av informations- och kommunikationstjänster har ett direkt förhållande till enskilda personer i EU (genom att erbjuda onlinetjänster) kan detta leda till en direkt tillämpning av förordning (EU) 2016/679 i enlighet med artikel 3.2 a i samma förordning.

([39]) I artikel 58.2 i PIPA föreskrivs vidare att artiklarna 15, 22, 27.1–27.2, 34 och 37 inte ska tillämpas på personuppgifter som behandlas med hjälp av visuella anordningar för databehandling som installerats och drivs på öppna platser. Eftersom denna bestämmelse gäller användning av videoövervakning inom Sydkorea, dvs. direkt insamling av personuppgifter från enskilda personer i Sydkorea, är den inte relevant för detta beslut som omfattar överföring av personuppgifter från personuppgiftsansvariga/personuppgiftsbiträden i EU till enheter i Sydkorea. Enligt artikel 58.3 i PIPA tillämpas dessutom inte artikel 15 (insamling och användning av personuppgifter), artikel 30 (skyldighet att införa en allmän integritetspolicy) och artikel 31 (skyldighet att utse en dataskyddsansvarig) på personuppgifter som behandlas för att driva grupper eller vänskapsföreningar (t.ex. hobbyklubbar). Eftersom sådana grupper anses vara personliga till sin natur, utan anknytning till yrkesmässig eller kommersiell verksamhet, krävs ingen särskild rättslig grund (t.ex. de berörda personernas samtycke) för att samla in och använda deras uppgifter i detta sammanhang. Alla andra bestämmelser i PIPA (t.ex. uppgiftsminimering, ändamålsbegränsning, laglighet vid behandling, säkerhet och enskildas rättigheter) ska dock fortsatt tillämpas. Dessutom skulle behandling av personuppgifter utöver ändamålet att inrätta en umgängesförening inte omfattas av undantaget.

([40]) Närmare bestämt föreskrivs i artikel 58.4 i PIPA en skyldighet att behandla personuppgifter i den minsta mån som krävs för att uppnå det avsedda ändamålet, behandla dem under kortast möjliga tidsperiod och vidta nödvändiga åtgärder för en säker hantering och lämplig behandling av sådana personuppgifter. Det senare omfattar tekniska, administrativa och fysiska skyddsåtgärder samt åtgärder för att säkerställa lämplig behandling av enskilda klagomål.

(27) För det första omfattar det partiella undantaget personuppgifter som samlas in i enlighet med statistiklagen för att behandlas av offentliga institutioner. Enligt klargöranden från den sydkoreanska regeringen rör personuppgifter som behandlas i detta sammanhang vanligtvis sydkoreanska medborgare och inbegriper endast undantagsvis uppgifter om utlänningar, nämligen vad gäller statistik över inresa till och utresa ur landet eller utländska investeringar. Även i dessa fall överförs dock sådana uppgifter normalt inte från personuppgiftsansvariga eller personuppgiftsbiträden i unionen, utan samlas in direkt av myndigheter i Sydkorea ([41]). I likhet med vad som föreskrivs i skäl 162 i förordning (EU) 2016/679 är dessutom behandling av uppgifter enligt statistiklagen underkastat ett flertal villkor och garantier. I statistiklagen föreskrivs särskilt specifika skyldigheter för att t.ex. säkerställa noggrannhet, enhetlighet och opartiskhet, garantera enskilda personers konfidentialitet, skydda information från uppgiftslämnare vid statistiska förfrågningar (bl.a. i syfte att förhindra att sådan information används för något annat ändamål än att sammanställa statistik) samt ställa krav på sekretess för anställda ([42]). Myndigheter som behandlar statistik måste också agera i enlighet med bl.a. principerna om uppgiftsminimering, ändamålsbegränsning och säkerhet (artiklarna 3 och 58.4 i PIPA) och tillåta enskilda personer att utöva sina rättigheter (rätt till tillgång, rättelse, radering och upphörande, se artikel 4 i PIPA). Slutligen måste uppgifterna behandlas i anonymiserad eller pseudonymiserad form om detta gör det möjligt att uppfylla ändamålet med behandlingen (artikel 3.7 i PIPA).

(28) För det andra hänvisas i artikel 58.1 i PIPA till personuppgifter som samlas in eller begärs för analys av information som rör den nationella säkerheten. Omfattningen och konsekvenserna av detta partiella undantag beskrivs närmare i skäl 149.

(29) För det tredje gäller det partiella undantaget för tillfällig behandling av personuppgifter när detta är synnerligen angeläget på grund av orsaker kopplade till allmän säkerhet, däribland folkhälsan. Denna kategori tolkas strikt av nämnden för skydd av personuppgifter och har enligt den information som mottagits aldrig använts. Den gäller endast i nödsituationer som kräver omedelbara åtgärder, t.ex. för att spåra smittämnen, eller för att rädda och hjälpa offer för naturkatastrofer ([43]). Även i dessa situationer omfattar det partiella undantaget endast behandling av personuppgifter under en begränsad tidsperiod för att genomföra sådana åtgärder. Situationer där detta skulle kunna gälla för dataöverföringar som omfattas av detta beslut är ännu mer begränsade, med tanke på den låga sannolikheten för att personuppgifter som överförs från unionen till sydkoreanska operatörer skulle vara av den typ som skulle kunna göra den efterföljande behandlingen ”brådskande” vid sådana nödsituationer.

(30) Slutligen gäller det partiella undantaget personuppgifter som samlas in eller används av pressen, för religiösa organisationers missionärsverksamhet eller för politiska partiers nominering av kandidater. Undantaget gäller endast när personuppgifter behandlas av pressen, religiösa organisationer eller politiska partier för dessa specifika ändamål (dvs. journalistisk verksamhet, missionsarbete och nominering av politiska kandidater). Om dessa enheter behandlar personuppgifter för andra ändamål, t.ex. personaladministration eller intern förvaltning, tillämpas PIPA i full utsträckning.

(31) När det gäller pressens behandling av personuppgifter för journalistisk verksamhet föreskrivs en avvägning mellan yttrandefrihet och andra rättigheter (däribland rätten till integritet) i lagen om skiljeförfarande och rättsmedel för skador som orsakats av pressrapporter (*Act on Arbitration and Remedies, etc. for Damage Caused by Press Reports*, nedan kallad *presslagen*) ([44]). Det föreskrivs särskilt i artikel 5 i presslagen att pressen (dvs. alla programföretag, tidningar, tidskrifter eller tidningar på nätet), nyhetstjänster på internet eller multimediaföretag på internet inte får kränka enskilda personers privatliv. Om en kränkning av privatlivet ändå sker måste den åtgärdas snabbt i enlighet med de särskilda förfaranden som anges i lagen. I detta avseende föreskrivs i lagen ett antal rättigheter för enskilda personer som lider skada på grund av en pressrapport, t.ex. att en rättelse av ett falskt uttalande

([41]) I detta avseende föreskrivs i artikel 33 i statistiklagen att offentliga institutioner ska skydda information från uppgiftslämnare vid statistiska förfrågningar, bl.a. för att förhindra att sådan information används för något annat ändamål än att sammanställa statistik.
([42]) Artiklarna 2.2–2.3, 30.2, 33 och 34 i statistiklagen.
([43]) Handboken för PIPA, avsnitt om artikel 58.
([44]) I artikel 4 i presslagen föreskrivs t.ex. att pressrapporter ska vara opartiska och objektiva, ligga i allmänhetens intresse, respektera människans värde och värdighet, och att de varken får innehålla förtal av enskilda eller inkräkta på deras rättigheter, allmänna moral eller sociala etik.

offentliggörs, att en rättelse görs genom ett uttalande, eller en vidare rapport (när en pressrapport gäller anklagelser om brott och personen sedan frikänns) ([45]). Enskilda personers klagomål kan lösas direkt av presstjänsten (genom en ombudsman) ([46]), genom förlikning eller skiljeförfarande (inför en specialiserad presskommitté) ([47]) eller inför domstol. Enskilda personer kan också få ersättning när de drabbas av ekonomisk skada, kränkningar av personlighetsskyddet eller andra känslomässiga problem på grund av en olaglig handling som begås av pressen (genom uppsåt eller vårdslöshet) ([48]). Pressen är befriad från ansvar enligt lagen i den mån en pressrapport som inkräktar på en individs rättigheter inte strider mot sociala värden och offentliggörs antingen med den berörda personens samtycke eller på grund av allmänintresset (och det finns tillräckliga skäl att anse att rapporten är sanningsenlig) ([49]).

(32) Även om pressens behandling av personuppgifter för journalistisk verksamhet därför omfattas av särskilda skyddsåtgärder som följer av presslagen finns det inga sådana ytterligare skyddsåtgärder som ramar in religiösa organisationers och politiska partiers tillämpning av undantagen för behandling på ett sätt som är jämförbart med artiklarna 85, 89 och 91 i förordning (EU) 2016/679. Kommissionen anser därför att det är lämpligt att utesluta religiösa organisationer i den mån de behandlar personuppgifter för sin missionärsverksamhet och politiska partier i den mån de behandlar personuppgifter i samband med nomineringen av kandidater från detta besluts tillämpningsområde.

2.3 **Skyddsåtgärder, rättigheter och skyldigheter**

2.3.1 *Laglig och korrekt behandling*

(33) Personuppgifter bör behandlas på ett lagligt och korrekt sätt.

(34) Denna princip fastställs i artikel 3.1 och 3.2 i PIPA och förstärks genom artikel 59 i PIPA, enligt vilken behandling av personuppgifter ”med bedrägliga, otillbörliga eller orättmätiga metoder”, ”utan rättslig auktoritet” eller ”med överskridande av befogenhet” förbjuds ([50]). Dessa allmänna principer för laglig behandling beskrivs i artiklarna 15–19 i PIPA, där de olika rättsliga grunderna för behandling anges (insamling, användning och tillhandahållande till tredje part), samt under vilka omständigheter detta kan innebära att ändamålet förändras (artikel 18 i PIPA).

([45]) Artiklarna 15–17 i presslagen.

([46]) Varje presstjänst eller mediekanal måste ha en egen ombudsman för att förhindra och avhjälpa eventuella skador som pressen kan orsaka (t.ex. genom att rekommendera korrigering av pressrapporter som är falska eller skadar andras anseende), artikel 6 i presslagen.

([47]) Kommittén består av mellan 40 och 90 skiljemän som utsetts av ministern för kultur, idrott och turism bland personer som är domare, advokater, har varit verksamma inom nyhetsinsamling eller -rapportering i minst tio år eller som har sakkunskap vad gäller pressen. Skiljemän kan inte samtidigt vara offentliga tjänstemän, medlemmar i politiska partier eller journalister. Enligt artikel 8 i presslagen ska skiljemännen utföra sina uppgifter oberoende och får inte underkastas någon ledning eller några instruktioner i samband med dessa uppgifter. Dessutom finns särskilda regler för att förhindra intressekonflikter, t.ex. genom att enskilda skiljemän utesluts från hantering av enskilda fall om deras make, maka eller släktingar är parter i ärendet (artikel 10 i presslagen). Kommittén får hantera tvister genom förlikning eller skiljedomsförfarande, men får också fastställa rekommendationer för att avhjälpa överträdelser (avsnitt 5 i presslagen).

([48]) Artikel 30 i presslagen.

([49]) Artikel 5 i presslagen.

([50]) Enligt artikel 59 i PIPA förbjuds personer som ”behandlar eller har behandlat personuppgifter” att ”förvärva personuppgifter eller att erhålla samtycke till behandling av personuppgifter genom bedrägeri, otillbörliga eller orättmätiga metoder”, ”avslöja personuppgifter som förvärvats i samband med affärsverksamhet eller att tillhandahålla dem för tredje mans användning utan tillstånd” eller ”skada, förstöra, ändra, förfalska eller avslöja andras personuppgifter utan rättslig behörighet eller med överskridande av befogenhet”. En överträdelse av detta förbud kan leda till straffrättsliga påföljder, se artikel 71.5, 71.6 och artikel 72.2 i PIPA. Enligt artikel 70.2 i PIPA får dessutom en straffrättslig påföljd utdömas vid erhållande av personuppgifter som behandlats av tredje man genom bedrägeri eller andra otillbörliga eller orättmätiga medel eller metoder, eller vid tillhandahållande av sådana uppgifter till tredje man i vinstsyfte eller för orättmätiga ändamål, samt vid medverkan till eller organisation av sådana handlingar.

(35) Enligt artikel 15.1 i PIPA får personuppgiftsansvariga endast samla in personuppgifter (inom ramen för insamlingens ändamål) på ett begränsat antal rättsliga grunder. Dessa är 1) den registrerades samtycke ([51]) (led 1); 2) behovet att genomföra och fullgöra ett avtal med den registrerade (led 4); 3) ett särskilt rättsligt tillstånd eller behovet att fullgöra en rättslig skyldighet (led 2); en offentlig institutions behov ([52]) att utföra uppgifter inom ramen för sitt behörighetsområde; 4) ett uppenbart behov av att skydda den registrerades eller en tredje parts liv, kropp eller egendomsintressen mot överhängande fara (endast om den registrerade inte kan uttrycka sin avsikt eller om förhandsgodkännande inte kan erhållas) (led 5); 5) behovet att uppnå den personuppgiftsansvariges ”berättigade intresse” om det är ”uppenbart överordnat” den registrerades intressen (och endast om behandlingen har en ”väsentlig koppling” till det legitima intresset och inte går utöver vad som är rimligt) (led 6) ([53]). Dessa grunder för behandling är i huvudsak likvärdiga med dem som fastställs i artikel 6 i förordning (EU) 2016/679, däribland den grund för ”berättigat intresse” som motsvarar grunden ”berättigade intressen” i artikel 6.1 f i förordning (EU) 2016/679.

(36) När personuppgifter har samlats in får de användas inom ramen för ändamålet med insamlingen (artikel 15.1 i PIPA), eller ”inom ramen för det tillämpningsområde som rimligen kan hänföras till insamlingsändamålet”, med beaktande av eventuella nackdelar för den registrerade och förutsatt att nödvändiga säkerhetsåtgärder (t.ex. kryptering) har vidtagits (artikel 15.3 i PIPA). För att fastställa om ändamålet med användningen ”rimligen kan hänföras till” det ursprungliga ändamålet med insamlingen fastställs i genomförandedekretet särskilda kriterier som liknar dem i artikel 6.4 i förordning (EU) 2016/679. Den måste framför allt vara av avsevärd relevans för det ursprungliga ändamålet och den ytterligare användningen måste vara förutsägbar (t.ex. mot bakgrund av de omständigheter under vilka uppgifterna samlades in), och om möjligt måste uppgifterna pseudonymiseras ([54]). De specifika kriterier som personuppgiftsansvariga använder i denna bedömning ska offentliggöras i förväg i integritetspolicyn ([55]). Dessutom är den dataskyddsanvarige (se skäl 94) särskilt skyldig att granska om ytterligare användning sker inom dessa parametrar.

([51]) Samtycke måste ges fritt, vara informerat, specifikt och uttryckas på ett av flera sätt som fastställts i lag. Under alla omständigheter får samtycke inte erhållas genom bedrägeri eller otillbörliga eller på annat sätt orättfärdiga metoder (artikel 59.1 i PIPA). För det första har de registrerade enligt artikel 4 led 2 i PIPA rätt att ”samtycka eller inte” och ”att välja samtyckets omfattning” och bör informeras om detta (artiklarna 15.2, 16.2, 16.3, 17.2 och 18.3 i PIPA). Artikel 22.5 i PIPA innehåller ett ytterligare skydd genom att personuppgiftsansvariga förbjuds att neka tillhandahållande av varor eller tjänster om detta skulle kunna undergräva individens fria val vid beviljande av samtycke. Detta inbegriper situationer där endast vissa typer av behandling kräver samtycke (medan andra bygger på avtal) och omfattar även vidare behandling av personuppgifter som samlas in i samband med tillhandahållande av varor eller tjänster. För det andra måste personuppgiftsansvariga i enlighet med artiklarna 15.2, 17.2, 17.3 och 18.3 i PIPA vid begäran om samtycke tillhandahålla den registrerade ”närmare information” om uppgifterna i fråga (t.ex. att det rör sig om känsliga uppgifter, se artikel 17.2.2 a i genomförandedekretet till PIPA), ändamålet med behandlingen, lagringsperioden och eventuella mottagare av uppgifterna. Varje sådan begäran ska göras ”på ett tydligt igenkännligt sätt” som särskiljer frågor som kräver samtycke från andra frågor (artikel 22.1–22.4 i PIPA). För det tredje föreskrivs i artikel 17.1 led 1–6 i genomförandedekretet till PIPA de särskilda metoder genom vilka personuppgiftsansvariga ska erhålla samtycke, t.ex. skriftligt samtycke med den registrerades underskrift eller samtycke per e-post. Även om det inte finns någon uttryckligen föreskriven allmän rätt i PIPA enligt vilken enskilda personer kan dra tillbaka sitt samtycke har enskilda i stället rätt att begära att behandlingen av uppgifter relaterade till dem upphör. När den rätten används leder den till att behandlingen avbryts och att uppgifterna raderas (se skäl 78 om rätten till upphörande).

([52]) Enligt information från nämnden för skydd av personuppgifter får offentliga institutioner endast förlita sig på denna grund om behandling av personuppgifter är oundviklig, dvs. det måste vara omöjligt eller orimligt svårt för institutet att utföra sina uppgifter utan att behandla uppgifterna.

([53]) Genom artikel 39-3 i PIPA införs särskilda (striktare) skyldigheter för leverantörer av informations- och kommunikationstjänster när det gäller insamling och användning av användares personuppgifter. Där krävs särskilt att leverantören erhåller användarens samtycke efter att ha tillhandahållit information om syftet med insamlingen/användningen, vilka kategorier av personuppgifter som ska samlas in och under vilken tidperiod uppgifterna kommer att behandlas (artikel 39-3.1 i PIPA). Detsamma gäller när någon av dessa aspekter ändras. Underlåtenhet att inhämta samtycke för insamling av uppgifter är föremål för straffrättsliga påföljder (artikel 71.4–71.5 i PIPA). I undantagsfall får användares personuppgifter samlas in eller användas av leverantörer av information och kommunikation utan föregående samtycke. Detta är fallet 1) när det är uppenbart svårt att inhämta normalt samtycke för de personuppgifter som krävs för att fullgöra avtalet om tillhandahållande av informations- och kommunikationstjänster av ekonomiska och tekniska skäl (t.ex. när personuppgifter oundvikligen skapas i samband med utförandet av ett avtal, såsom faktureringsinformation, åtkomstregister och betalningsregister), 2) när det är nödvändigt för inbetalning av avgifter efter tillhandahållande av informations- och kommunikationstjänster, eller 3) om det är tillåtet enligt andra lagar (t.ex. artikel 21.1 led 6 i lagen om konsumentskydd i elektronisk handel, där det anges att näringsidkare får samla in personuppgifter om minderårigas vårdnadshavare för att bekräfta huruvida giltigt samtycke har erhållits för den underårigas räkning) (artikel 39-3.2 i PIPA). I samtliga fall får leverantörer av information och kommunikation inte vägra att tillhandahålla tjänster enbart på grund av att användaren inte tillhandahåller mer personlig information än vad som krävs (dvs. den information som är nödvändig för att utföra de väsentliga delarna av den berörda tjänsten), se artikel 39-3.3 i PIPA.

([54]) Se artikel 14-2 i genomförandedekretet till PIPA.

([55]) Artikel 14-2.2 i genomförandedekretet till PIPA.

(37) Liknande (men något strängare) regler gäller för tillhandahållande av uppgifter till tredje part. Enligt artikel 17.1 i PIPA är tillhandahållande av personuppgifter till en tredje part tillåtet efter samtycke ([56]) eller om det motsvarar ändamålet med insamlingen, i det fall uppgiftsinsamlingen grundas på någon av de rättsliga grunderna i artikel 15.1 led 2, 3 och 5 i PIPA. Detta utesluter särskilt all utlämning som grundar sig på den personuppgiftsansvariges ”berättigade intresse”. Utöver detta tillåts enligt artikel 17.4 i PIPA tillhandahållande till tredje part ”inom ramen för det tillämpningsområde som rimligen kan hänföras till insamlingsändamålet”, med beaktande av eventuella nackdelar för den registrerade och förutsatt att nödvändiga säkerhetsåtgärder (t.ex. kryptering) har vidtagits. Samma faktorer som beskrivs i skäl 36 måste beaktas för att bedöma om bestämmelsen ligger inom ramen för det tillämpningsområde som rimligen kan hänföras till insamlingsändamålet och samma skyddsåtgärder (dvs. när det gäller öppenhet genom integritetspolicyn och den dataskyddsansvariges medverkan) gäller.

(38) Om en sydkoreansk personuppgiftsansvarig tar emot personuppgifter från unionen betraktas det som ”insamling” i den mening som avses i artikel 15 i PIPA. I meddelande nr 2021-5 (avsnitt I i bilaga I till detta beslut) klargörs att det ändamål för vilket uppgifterna överfördes av den berörda EU-enheten utgör ändamålet med insamlingen för den sydkoreanska personuppgiftsansvarige. Till följd av detta är sydkoreanska personuppgiftsansvariga som tar emot personuppgifter från unionen i princip skyldiga att behandla sådana uppgifter inom ramen för ändamålet med överföringen, i enlighet med artikel 17 i PIPA.

(39) Särskilda begränsningar gäller om den personuppgiftsansvarige försöker använda personuppgifterna eller tillhandahålla dem till en tredje part för ett annat ändamål än insamlingsändamålet ([57]). Enligt artikel 18.2 i PIPA får en privat personuppgiftsansvarig undantagsvis ([58]) använda personuppgifter eller tillhandahålla dem till en tredje part för ett annat ändamål: 1) baserat på den registrerades ytterligare (dvs. separata) samtycke, 2) om detta tillåts enligt särskilda rättsliga bestämmelser, eller 3) om det föreligger ett uppenbart behov av att skydda den registrerades eller en tredje parts liv, kropp eller egendomsintressen mot överhängande fara (endast om den registrerade inte kan uttrycka sin avsikt eller om förhandsgodkännande inte kan erhållas) ([59]).

(40) Offentliga institutioner får också använda personuppgifter eller tillhandahålla dem till en tredje part för ett annat ändamål i vissa situationer. Detta omfattar fall där det annars skulle vara omöjligt för offentliga institutioner att fullgöra sina lagstadgade skyldigheter enligt lag, förutsatt att nämnden för skydd av personuppgifter ger sitt tillstånd. Dessutom får offentliga institutioner tillhandahålla personuppgifter till en annan myndighet eller domstol om detta är nödvändigt för utredning och lagföring av brott eller åtal, för att en domstol ska kunna utföra sina uppgifter i samband med pågående rättsliga förfaranden, eller för verkställighet av en straffrättslig påföljd eller ett beslut om omvårdnad eller vårdnad ([60]). De får även tillhandahålla personuppgifter till en utländsk regering eller internationell organisation för att uppfylla en rättslig skyldighet enligt ett fördrag eller en internationell konvention. I dessa fall måste de även uppfylla kraven för gränsöverskridande dataöverföringar (se skäl 90).

(41) Principerna om laglig och korrekt behandling tillämpas därför i den sydkoreanska rättsliga ramen på ett sätt som i huvudsak motsvarar förordning (EU) 2016/679 genom att behandling endast tillåts på grundval av legitima och klart definierade skäl. I alla nämnda fall är behandlingen dessutom endast tillåten om det är osannolikt att den ”otillbörligen överträder” den registrerades eller tredje mans intressen, vilket kräver en avvägning av intressen. Dessutom föreskrivs i artikel 18.5 i PIPA ytterligare skyddsåtgärder när den personuppgiftsansvarige tillhandahåller personuppgifter till en tredje part, vilket kan inbegripa en begäran om att begränsa syftet med och metoden för användning eller att införa särskilda säkerhetsåtgärder. Den tredje parten är i sin tur skyldig att genomföra de begärda åtgärderna.

([56]) Överträdelser av artikel 17.1.1 i PIPA kan leda till straffrättsliga påföljder (artikel 71.1 i PIPA).

([57]) Det ”avsedda ändamålet” är det ändamål för vilket uppgifterna samlades in. När uppgifterna exempelvis samlas in på grundval av den berörda personens samtycke är det avsedda ändamålet det som meddelas personen enligt artikel 15.2 i PIPA.

([58]) Se artikel 18.1 i PIPA. Överträdelser av artikel 18.1 och 18.2 kan leda till straffrättsliga påföljder (artikel 71.2 i PIPA).

([59]) Leverantörer av informations- och kommunikationstjänster får endast använda personuppgifter eller tillhandahålla dem till tredje part för ett annat ändamål än det ursprungliga på de grunder som anges i artikel 18.2 led 1 och 2 i PIPA (dvs. om ytterligare samtycke erhålls eller om särskilda bestämmelser föreskrivs i lag). Se artikel 18.2 i PIPA.

([60]) Med undantag för behandling som är nödvändig för utredning av brott, åtal och lagföring är offentliga institutioner som använder personuppgifter eller tillhandahåller den till en tredje part för ett annat ändamål än insamlingsändamålet (t.ex. om detta är uttryckligen tillåtet enligt lag eller nödvändigt för att fullgöra ett fördrag) skyldiga att offentliggöra de rättsliga grunderna för behandlingen, dess ändamål och räckvidd på sin webbplats eller i det officiella kungörelseorganet och föra register (artikel 18.4 i PIPA tillsammans med artikel 15 i genomförandedekretet till PIPA).

(42) Slutligen tillåts enligt artikel 28-2 i PIPA (ytterligare) behandling av pseudonymiserade uppgifter utan den berörda personens samtycke för statistik, vetenskaplig forskning ([61]) och arkivändamål i allmänhetens intresse, med förbehåll för särskilda skyddsåtgärder. I likhet med förordning (EU) 2016/679 ([62]) underlättas genom PIPA därför (ytterligare) behandling av personuppgifter för dessa ändamål inom en ram som tillhandahåller lämpliga mekanismer för att skydda enskilda personers rättigheter. I stället för att förlita sig på pseudonymisering som en möjlig skyddsåtgärd föreskrivs detta i PIPA som en förutsättning för att utföra viss behandling relaterad till statistik, vetenskaplig forskning och arkivändamål i allmänhetens intresse (t.ex. för att kunna behandla uppgifterna utan samtycke eller kombinera olika datauppsättningar).

(43) I PIPA föreskrivs dessutom ett antal särskilda skyddsåtgärder, särskilt när det gäller nödvändiga tekniska och organisatoriska åtgärder, dokumentation, begränsningar av datadelning och hantering av eventuella risker för återidentifiering. Kombinationen av de olika skyddsåtgärder som beskrivs i skälen 44–48 säkerställer att behandlingen av personuppgifter i detta sammanhang skyddas genom i huvudsak likvärdigt skydd som skulle krävas i enlighet med förordning (EU) 2016/679.

(44) För det första, och viktigast av allt, förbjuds i artikel 28-5.1 i PIPA behandling av pseudonymiserade uppgifter i syfte att identifiera en viss person. Om information som skulle kunna identifiera en person ändå genereras under behandlingen av pseudonymiserade uppgifter måste den personuppgiftsansvarige omedelbart avbryta behandlingen och förstöra sådan information (artikel 28-5.2 i PIPA). Underlåtenhet att följa dessa bestämmelser medför administrativa sanktionsavgifter och utgör ett brott ([63]). Detta innebär att det även i de situationer där det är *praktiskt* möjligt att återidentifiera personen är *rättsligt* förbjudet att utföra sådan återidentifiering.

(45) För det andra måste den personuppgiftsansvarige, när (ytterligare) behandling av pseudonymiserade uppgifter utförs för sådana ändamål, vidta särskilda tekniska, förvaltningsmässiga och fysiska åtgärder för att säkerställa informationssäkerheten (bl.a. åtskild lagring och hantering av de uppgifter som krävs för att återställa de pseudonymiserade uppgifterna till sitt ursprungliga tillstånd) ([64]). Dessutom måste de pseudonymiserade uppgifter som behandlas, ändamålet med behandlingen, användningshistoriken och eventuella mottagande tredje parter dokumenteras (artikel 29-5.2 i genomförandedekretet till PIPA).

(46) För det tredje och sista föreskrivs i PIPA särskilda skyddsåtgärder för att förhindra att tredje man kan identifiera personer i fall där uppgifterna delas. Vid tillhandahållande av pseudonymiserade uppgifter till en tredje part för statistik, vetenskaplig forskning eller arkivändamål i allmänhetens intresse gäller särskilt att personuppgiftsansvariga inte får bifoga uppgifter som kan användas för att identifiera en viss person (artikel 28-2.2 i PIPA) ([65]).

(47) Enligt PIPA tillåts sammanföring av pseudonymiserade uppgifter (som behandlas av olika personuppgiftsansvariga) för statistik, vetenskaplig forskning eller arkivändamål i allmänhetens intresse, men denna befogenhet förbehålls specialiserade institutioner som är utrustade med särskilda säkerhetsanordningar (artikel 28-3.1 i PIPA) ([66]). Vid ansökan om att sammanföra pseudonymiserade uppgifter måste den personuppgiftsansvarige lämna

([61]) Vetenskaplig forskning definieras i artikel 2.8 i PIPA som ”forskning som tillämpar vetenskapliga metoder, t.ex. teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning”. Dessa kategorier motsvarar dem som anges i skäl 159 i förordning (EU) 2016/679.

([62]) Se artiklarna 5.1 b och 89.1–89.2 samt skälen 50 och 157 i förordning (EU) 2016/679.

([63]) Se artiklarna 28-6.1, 71.4-3 och 75.2.4-4 i PIPA.

([64]) Artikel 28-4 i PIPA och artikel 29-5 i genomförandedekretet till PIPA. Underlåtenhet att uppfylla denna skyldighet är föremål för administrativa och straffrättsliga påföljder, se artiklarna 73.1 och 75.2.6 i PIPA.

([65]) Överträdelser av dessa bestämmelser kan leda till straffrättsliga påföljder (artikel 71.2 i PIPA). Nämnden för skydd av personuppgifter började omedelbart tillämpa dessa nya regler, t.ex. i sitt beslut av den 28 april 2021 där böter och korrigerande åtgärder ålades ett företag som bland andra överträdelser av PIPA inte uppfyllde kraven i artikel 28-2.2 i PIPA, se https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) För att utnämnas till en sådan specialiserad institution (ett ”expertorgan för kombination av uppgifter”) måste en ansökan lämnas in till nämnden för skydd av personuppgifter tillsammans med styrkande handlingar som bl.a. innehåller de hjälpmedel och den utrustning som installerats för att på ett säkert sätt kombinera pseudonymiserade uppgifter och som bekräftar att den sökande anställer minst tre heltidsanställda med kvalifikationer eller erfarenhet avseende skydd av personuppgifter (artikel 29-2.1–29-2.2 i genomförandedekretet till PIPA). Detaljerade krav, t.ex. när det gäller personalens kvalifikationer, tillgängliga hjälpmedel, säkerhetsåtgärder, interna riktlinjer och förfaranden samt finansiella krav anges i meddelande 2020-9 från nämnden för skydd av personuppgifter om kombination och utlämnande av pseudonymiserade uppgifter (förteckning I). En utnämning till expertorgan för kombination av uppgifter kan återkallas av nämnden för skydd av personuppgifter (efter en förhandling) på vissa grunder, t.ex. om organet inte längre uppfyller de säkerhetsnormer som krävs för utnämning, eller om en uppgiftsincident har inträffat i samband med att uppgifter har kombinerats (artikel 29-2.5–29-2.6 i genomförandedekretet till PIPA). Nämnden för skydd av personuppgifter måste offentliggöra varje utnämning (eller återkallande av utnämning) av ett expertorgan för kombination av uppgifter (artikel 29-2.7 i genomförandedekretet till PIPA).

dokumentation om bl.a. de uppgifter som ska kombineras, syftet med kombinationen samt de föreslagna säkerhetsåtgärderna för behandling av de kombinerade uppgifterna ([67]). För att kombinationen ska kunna göras måste den personuppgiftsansvarige sända de uppgifter som ska kombineras till den specialiserade institutionen och tillhandahålla en ”kombinationsnyckel” (dvs. den information som har använts för pseudonymisering) till Sydkoreas byrå för internet och säkerhet ([68]). Den senare genererar ”länkdata för kombinationsnycklar” (som gör det möjligt att koppla samman olika sökandens kombinationsnycklar och därmed kombinera datauppsättningarna) och tillhandahåller dem till den specialiserade institutionen ([69]).

(48) Den personuppgiftsansvarige som ansöker om en kombination får analysera de kombinerade uppgifterna i den specialiserade institutionens lokaler på en plats där särskilda tekniska, fysiska och administrativa säkerhetsåtgärder tillämpas (artikel 29-3 i genomförandedekretet till PIPA). Personuppgiftsansvariga som bidrar med en datauppsättning för en sådan kombination får endast använda de kombinerade uppgifterna utanför den specialiserade institutionen efter ytterligare pseudonymisering eller anonymisering av de kombinerade uppgifterna, och med institutionens godkännande (artikel 28-3.2 i PIPA) ([70]). När institutionen överväger om ett sådant godkännande ska beviljas eller inte kommer den att bedöma kopplingen mellan de kombinerade uppgifterna och ändamålet med behandlingen, och huruvida en särskild säkerhetsplan har utarbetats för användningen av sådana uppgifter ([71]). Export av de kombinerade uppgifterna utanför institutionen tillåts inte om de innehåller information som gör det möjligt att identifiera en enskild person ([72]). Slutligen övervakas den specialiserade institutionens kombination och utlämnande av pseudonymiserade uppgifter av nämnden för skydd av personuppgifter (artikel 29-4.3 i genomförandedekretet till PIPA).

2.3.2 *Behandling av särskilda kategorier av personuppgifter*

(49) Specifika skyddsåtgärder bör vidtas när ”särskilda kategorier” av uppgifter behandlas.

(50) PIPA innehåller särskilda regler för behandling av känsliga uppgifter ([73]), definierat som personuppgifter som avslöjar information om en enskild persons ideologi, övertygelse, inträde i eller utträde ur en fackförening eller ett politiskt parti, politiska åsikter, hälsa och sexualliv, samt andra personuppgifter som ”märkbart” kan hota den registrerades integritet och som förklarats vara känslig information enligt presidentdekret ([74]). Enligt förtydliganden från nämnden för skydd av personuppgifter tolkas sexualliv som att det även omfattar individens sexuella läggning eller preferenser ([75]). I artikel 18 i genomförandedekretet utvidgas dessutom definitionen av känsliga uppgifter till att omfatta ytterligare kategorier, särskilt DNA-information som erhållits genom genetisk testning och uppgifter som utgör belastningsregister. Den senaste ändringen av genomförandedekretet till PIPA har ytterligare breddat begreppet känsliga uppgifter genom att även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung och biometrisk information ([76]). Efter denna ändring är begreppet känsliga uppgifter enligt PIPA i huvudsak likvärdigt med det som anges i artikel 9 i förordning (EU) 2016/679.

(51) Enligt artikel 23.1 i PIPA och på samma sätt som enligt artikel 9.1 i förordning (EU) 2016/679 är behandling av känsliga uppgifter i allmänhet förbjuden, såvida inte ett av de angivna undantagen är tillämpligt ([77]). Dessa begränsar behandlingen till fall där den personuppgiftsansvarige underrättar den registrerade i enlighet med artiklarna 15 och 17 i PIPA, och erhåller separat samtycke (dvs. åtskilt från samtycke för behandling av andra personuppgifter) eller där behandlingen krävs eller tillåts enligt lag. Myndigheter får också behandla biometrisk information, DNA-information som förvärvats genom genetisk testning, personuppgifter som avslöjar ras eller

([67]) Artikel 8.1–8.2 i meddelande 2020-9 om kombination och utlämnande av pseudonymiserade uppgifter.
([68]) Artikel 2.3 och 2.6 och artikel 9.1 i meddelande 2020-9 om kombination och utlämnande av pseudonymiserade uppgifter.
([69]) Artikel 2.4 och artikel 9.2–9.3 i meddelande 2020-9 om kombination och utlämnande av pseudonymiserade uppgifter. Den specialiserade institutionen måste omedelbart förstöra länkdata för kombinationsnycklar efter kombination (artikel 9.4 i meddelandet).
([70]) Överträdelser av kraven för kombination av datauppsättningar kan leda till straffrättsliga påföljder (artikel 71.4-2 i PIPA). Se även artikel 29-2.4 i genomförandedekretet till PIPA.
([71]) Förfarandet för att godkänna utlämnande av kombinerade uppgifter anges i artikel 11 i meddelande 2020-9 om kombination och utlämnande av pseudonymiserade uppgifter. Den specialiserade institutionen måste särskilt inrätta en kommitté för granskning av detta utlämnande. Kommittén ska bestå av ledamöter med betydande kunskaper om och erfarenhet av dataskydd.
([72]) Artikel 29-2.4 i genomförandedekretet till PIPA och meddelande nr 2020-9, artikel 11.
([73]) Behovet av särskilt skydd för behandling av känsliga uppgifter, t.ex. uppgifter om hälsa eller sexuellt beteende, har också erkänts av den sydkoreanska författningsdomstolen, se författningsdomstolens beslut HunMa 1139 av den 31 maj 2007.
([74]) Artikel 23.1 i PIPA.
([75]) Se även handboken för PIPA, kapitel III, avsnitt 2 om artikel 23 (s. 157–164).
([76]) Dvs. personuppgifter som erhållits genom en särskild teknisk behandling av uppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga egenskaper i syfte att unikt identifiera personen i fråga.
([77]) Om dessa krav inte uppfylls kan det leda till sanktioner enligt artikel 71 led 3 i PIPA.

etniskt ursprung och uppgifter som utgör belastningsregister på sådana grunder som endast finns tillgängliga för dem (t.ex. när det är nödvändigt för utredning av brott eller när det krävs för att en domstol ska behandla ett ärende) ([78]). De rättsliga grunder som finns att tillgå för behandling av känsliga uppgifter är mer begränsade än för andra typer av personuppgifter och till och med mer restriktiva i sydkoreansk lagstiftning än enligt artikel 9.2 i förordning (EU) 2016/679.

(52) Dessutom understryks i artikel 23.2 i PIPA den särskilda betydelsen av att säkerställa lämplig säkerhet vid hantering av känsliga uppgifter så att de ”inte kan gå förlorade, stjälas, spridas, förfalskas, ändras eller skadas”. Om detta inte efterlevs kan det leda till sanktioner ([79]). Även om detta är ett allmänt krav enligt artikel 29 i PIPA klargörs i artikel 3.4 att säkerhetsnivån måste anpassas till den typ av personuppgifter som behandlas, vilket innebär att de särskilda riskerna vid behandling av känsliga uppgifter ska beaktas. Dessutom ska behandling av personuppgifter alltid utföras ”på ett sätt som minimerar risken för överträdelser” av den registrerades privatliv och om möjligt ”med anonymitet” (artikel 3.6 och 3.7 i PIPA). Dessa krav är särskilt relevanta när behandlingen gäller känsliga uppgifter.

2.3.3 *Ändamålsbegränsning*

(53) Personuppgifter ska samlas in för ett specifikt ändamål och på ett sätt som inte är oförenligt med ändamålet med behandlingen.

(54) Denna princip säkerställs genom artikel 3.1 och 3.2 i PIPA enligt vilken personuppgiftsansvariga ”tydligt och klart” ska ange ändamålet med behandlingen, behandla personuppgifter på ett lämpligt sätt i enlighet med ändamålet och inte använda dem utöver detta ändamål. Den allmänna principen om ändamålsbegränsning bekräftas också i artiklarna 15.1, 18.1, 19, och för personuppgiftsbiträden (så kallade ”uppdragstagare”) i artikel 26.1 led 1, 26.5 och 26.7 i PIPA. I synnerhet får personuppgifter i princip endast användas och tillhandahållas tredje man inom ramen för det ändamål för vilket de samlades in (artiklarna 15.1 och 17.1 led 2). Behandling för ett förenligt ändamål, dvs. ”inom ramen för det tillämpningsområde som rimligen kan hänföras till insamlingsändamålet”, får endast ske om det inte inverkar negativt på de registrerade och om nödvändiga säkerhetsåtgärder (t.ex. kryptering) antas (artiklarna 15.3 och 17.4 i PIPA). För att fastställa om ytterligare behandling är för ett förenligt ändamål förtecknas i genomförandedekretet till PIPA särskilda kriterier som liknar dem som anges i artikel 6.4 i förordning (EU) 2016/679, se skäl 36.

(55) Som framgår av förklaringen i skäl 38 är ändamålet med insamlingen när det gäller sydkoreanska personuppgiftsansvariga som tar emot personuppgifter från unionen det ändamål för vilket uppgifterna överförs. En personuppgiftsansvarig får endast ändra ändamålet i undantagsfall, i specifika (uppräknade) fall (artikel 18.2 led 1–3 i PIPA, se även skäl 39). I den mån en ändring av ändamålet är tillåten enligt lag måste sådana lagar i sin tur respektera den grundläggande rätten till integritet och dataskydd, samt principerna om nödvändighet och proportionalitet som fastställs i den sydkoreanska författningen. Dessutom föreskrivs i artikel 18.2 och 18.5 i PIPA ytterligare skyddsåtgärder, särskilt kravet att en sådan ändring av ändamålet inte får ”inkräkta på den registrerades intressen på ett otillbörligt sätt”, vilket således alltid kräver en avvägning av intressen. Detta ger en skyddsnivå som i huvudsak motsvarar den som anges i artikel 5.1 led b och artikel 6 jämförd med skäl 50 i förordning (EU) 2016/679.

2.3.4 *Uppgifternas korrekthet och uppgiftsminimering*

(56) Personuppgifter bör vara korrekta och vid behov hållas uppdaterade. De bör också vara adekvata, relevanta och begränsade till vad som krävs när det gäller de ändamål för vilka de behandlas.

([78]) Enligt artikel 18 i genomförandedekretet till PIPA är de kategorier av uppgifter som förtecknas däri undantagna från bestämmelserna i artikel 23.1 i lagen när de behandlas av en offentlig institution i enlighet med artikel 18.2 led 5–9 i PIPA.

([79]) Se artiklarna 73 led 1 och 75.2 led 6 i PIPA.

(57) Principen om korrekthet erkänns på samma sätt i artikel 3.3 i PIPA enligt vilken personuppgifter ska vara ”adekvata, fullständiga och uppdaterade i den utsträckning som krävs när det gäller de ändamål” för vilka uppgifterna behandlas. Uppgiftsminimering krävs enligt artiklarna 3.1, 3.6 och 16.1 i PIPA, där det föreskrivs att den personuppgiftsansvarige (endast) ska samla in personuppgifter ”i den minsta mån som krävs” för det avsedda ändamålet och att den personuppgiftsansvarige har bevisbördan i detta avseende. Om det är möjligt att uppfylla ändamålet med insamlingen genom att behandla uppgifter i anonymiserad form bör personuppgiftsansvariga sträva efter att göra detta (artikel 3.7 i PIPA).

2.3.5 *Begränsad lagring*

(58) Uppgifter ska i princip inte lagras under längre tid än vad som krävs för de ändamål för vilka personuppgifterna behandlas.

(59) Principen om lagringsbegränsning föreskrivs på liknande sätt i artikel 21.1 i PIPA ([80]), enligt vilken den personuppgiftsansvarige ska ”förstöra” ([81]) personuppgifter utan dröjsmål när ändamålet med behandlingen har uppnåtts eller när lagringsperioden har löpt ut (beroende på vilket som infaller först), såvida inte ytterligare lagring krävs enligt lag ([82]). I det senare fallet ska relevanta personuppgifter ”lagras och hanteras åtskilt från andra personuppgifter” (artikel 21.3 i PIPA).

(60) Artikel 21.1 i PIPA tillämpas inte när pseudonymiserade uppgifter behandlas för statistik, vetenskaplig forskning eller arkivändamål i allmänhetens intresse ([83]). För att säkerställa principen om begränsad lagring av uppgifter även i detta fall krävs enligt meddelande 2021-5 att personuppgiftsansvariga anonymiserar uppgifterna i enlighet med artikel 58-2 i PIPA om uppgifterna inte har förstörts när det särskilda ändamålet med behandlingen har uppfyllts ([84]).

2.3.6 *Datasäkerhet*

(61) Personuppgifter bör behandlas på ett sätt som säkerställer att säkerheten garanteras, vilket inbegriper skydd mot obehörig eller otillåten behandling och mot oavsiktlig förlust, förstöring eller skada. I detta syfte bör näringsidkare vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från eventuella hot. Dessa åtgärder bör bedömas med beaktande av den senaste utvecklingen, relaterade kostnader och behandlingens art, omfattning, sammanhang och syfte samt riskerna för enskilda personers rättigheter.

(62) En liknande säkerhetsprincip fastställs i artikel 3.4 i PIPA där det föreskrivs att personuppgiftsansvariga ska ”hantera personuppgifter säkert i enlighet med personuppgifternas behandlingsmetod, typ osv., med beaktande av risken för överträdelse av de registrerades rättigheter och hur allvarliga de relevanta riskerna är”. Den personuppgiftsansvarige ska dessutom ”behandla personuppgifter på ett sätt som minimerar risken för kränkning av den registrerades integritet” och i detta sammanhang sträva efter att behandla personuppgifter anonymt eller i pseudonymiserad form, om möjligt (artikel 3.6 och 3.7 i PIPA).

(63) Dessa allmänna krav beskrivs närmare i artikel 29 i PIPA, enligt vilken varje personuppgiftsansvarig ”ska vidta sådana tekniska, förvaltningsmässiga och fysiska åtgärder (som att upprätta en intern förvaltningsplan och bevara inloggningsregister osv.) som krävs för att garantera säkerheten såsom anges i presidentdekret, så att personuppgifterna inte går förlorade, stjäls, sprids, förfalskas, ändras eller skadas”. I artikel 30.1 i genomförandedekretet

([80]) Artikel 8 (jämförd med artikel 8-2 i genomförandedekretet), artikel 11 (jämförd med artikel 12.2 i genomförandedekretet).

([81]) Om metoder för att förstöra personuppgifter, se artikel 16 i genomförandedekretet till PIPA. I artikel 21.2 i PIPA klargörs att detta ska omfatta ”nödvändiga åtgärder för att förhindra återvinning och återupprättande”.

([82]) Underlåtenhet att uppfylla dessa krav kan leda till straffrättsliga påföljder (artikel 73.1–73.2 i PIPA). Enligt artikel 39-6 i PIPA ska leverantörer av informations- och kommunikationstjänster radera personuppgifter avseende användare som under minst ett års tid inte har använt de erbjudna informations- och kommunikationstjänsterna (såvida inte ytterligare lagring krävs enligt lag eller på begäran av den enskilde). Enskilda personer ska underrättas om den planerade raderingen av deras uppgifter 30 dagar innan tidsfristen på ett år löper ut (artikel 39-6.2 i PIPA och artikel 48-5.3 i genomförandedekretet till PIPA). Om ytterligare lagring krävs enligt lag måste de lagrade uppgifterna förvaras åtskilt från andra uppgifter om användarna och får endast användas eller utlämnas i enlighet med den lagen (artikel 48-5.1–48-5.2 i genomförandedekretet till PIPA).

([83]) Artikel 28-7 i PIPA.

([84]) Meddelande 2021-5 (bilaga I), avsnitt 4.

till PIPA anges dessa åtgärder genom hänvisning till 1) utarbetande och genomförande av en intern förvaltningsplan för säker behandling av personuppgifter, 2) tillträdeskontroller och -begränsningar, 3) införande av krypteringsteknik för säker lagring och överföring av personuppgifter, 4) inloggningsregister, 5) säkerhetsprogram och 6) fysiska åtgärder, t.ex. ett säkert lagrings- eller låsningssystem ([85]).

(64) Dessutom gäller särskilda skyldigheter om en uppgiftsincident inträffar (artikel 34 i PIPA jämförd med artiklarna 39 och 40 i genomförandedekretet till PIPA) ([86]). Den personuppgiftsansvarige är särskilt skyldig att utan dröjsmål underrätta påverkade registrerade om incidenten ([87]), däribland information om (obligatoriska) motåtgärder som den personuppgiftsansvarige har vidtagit och vad de registrerade kan göra för att minimera risken för skada (artikel 34.1 och 34.2 i PIPA) ([88]). Om uppgiftsincidenten berör minst 1 000 registrerade ska den personuppgiftsansvarige utan dröjsmål också rapportera uppgiftsincidenten och de motåtgärder som vidtagits till nämnden för skydd av personuppgifter och Sydkoreas byrå för internet och säkerhet, som kan tillhandahålla tekniskt bistånd (artikel 34.3 i PIPA jämförd med artikel 39 i genomförandedekretet till PIPA). Personuppgiftsansvariga är ansvariga för skada till följd av uppgiftsincidenter, i enlighet med bestämmelserna i civillagen om skadeståndsansvar (se även avsnitt 2.5 om rättslig prövning) ([89]).

(65) För att uppfylla sina säkerhetsförpliktelser måste den personuppgiftsansvarige biträdas av en dataskyddsansvarig, vars uppgifter bl.a. är att bygga upp ett internt kontrollsystem ”för att förhindra spridning, missbruk och felaktig användning av personuppgifter” (artikel 31.2 led 4 i PIPA). Den personuppgiftsansvarige är dessutom skyldig att utföra ”lämplig kontroll och tillsyn” av personal som behandlar personuppgifter, bl.a. vad gäller säker hantering. Detta omfattar nödvändig utbildning av anställda (artikel 28.1 och 28.2 i PIPA). Slutligen måste den personuppgiftsansvarige vid underentreprenad införa krav på bl.a. ”uppdragstagaren” när det gäller säker hantering av personuppgifter (”tekniska och förvaltningsmässiga skyddsåtgärder”) och övervaka hur dessa efterlevs med hjälp av kontroller (artikel 26.1 och 26.4 i PIPA jämförd med artikel 28.1 led 3 och 4 samt 28.6 i genomförandedekretet till PIPA).

2.3.7 *Öppenhet*

(66) De registrerade bör underrättas om de viktigaste dragen i behandlingen av deras personuppgifter.

([85]) När det gäller leverantörer av informations- och kommunikationstjänster som behandlar personuppgifter föreskrivs i artikel 39-5 i PIPA uttryckligen att antalet personer som hanterar användares personuppgifter ska begränsas till ett minimum. Leverantörer av informations- och kommunikationstjänster ska dessutom säkerställa att användarnas personuppgifter inte exponeras för allmänheten via informations- och kommunikationsnätet (artikel 39-10.1 i PIPA). Exponerade uppgifter måste raderas eller blockeras på begäran av nämnden för skydd av personuppgifter (artikel 39-10.2 i PIPA). Mer allmänt omfattas leverantörer av informations- och kommunikationstjänster (och tredje parter som tar emot användares personuppgifter) av ytterligare säkerhetskrav, som anges i artikel 48-2 i genomförandedekretet till PIPA, t.ex. utarbetande och genomförande av en intern förvaltningsplan med avseende på säkerhetsåtgärder, åtgärder för att säkerställa tillträdeskontroll, kryptering, användning av programvara för att upptäcka skadlig programvara osv.

([86]) Dessutom finns det ett allmänt förbud mot att skada, förstöra, ändra, förfalska eller läcka personuppgifter utan rättslig behörighet, se artikel 59 led 3 i PIPA.

([87]) Kravet på att underrätta personen är inte tillämpligt i den mån som en uppgiftsincident sker med avseende på pseudonymiserade uppgifter som behandlas för statistik, vetenskaplig forskning eller arkivändamål i allmänhetens intresse (artikel 28-7 i PIPA, enligt vilken ett undantag tillåts från artiklarna 34.1 och 39-4 i PIPA). För att säkerställa individuell underrättelse skulle den berörda personuppgiftsansvarige vara tvungen att identifiera personer från den pseudonymiserade datauppsättningen, vilket är uttryckligen förbjudet enligt artikel 28-5 i PIPA. Det allmänna kravet på underrättelse om uppgiftsincidenter (till nämnden för skydd av personuppgifter) fortsätter dock att gälla.

([88]) Kraven gällande underrättelsen, bl.a. tidpunkt och möjligheten att underrättelsen sker stegvis specificeras närmare i artikel 40 i genomförandedekretet till PIPA. Striktare regler gäller för leverantörer av informations- och kommunikationstjänster som är skyldiga att underrätta den registrerade och nämnden för skydd av personuppgifter inom 24 timmar efter det att de fått kännedom om att personuppgifter har förlorats, stulits eller läckt ut (artikel 39-4.1 i PIPA). Denna underrättelse måste innehålla uppgifter om de personuppgifter som har läckt ut, den tidpunkt då detta inträffade, de åtgärder som kan vidtas av användaren, beredskapsåtgärder som vidtagits av leverantören och kontaktuppgifter för den avdelning till vilken användaren kan ställa frågor (artikel 39-4.1.1–39-4.1.5 i PIPA). Om det finns ett motiverat skäl, t.ex. att man inte har användarens kontaktuppgifter, får andra underrättelsesätt användas, t.ex. genom att göra informationen tillgänglig för allmänheten på en webbplats (artikel 39-4.1 i PIPA jämförd med artikel 48-4.4 ff. i genomförandedekretet till PIPA). I sådana fall måste nämnden för skydd av personuppgifter informeras om skälen till detta (artikel 34-4.3 i PIPA).

([89]) Se t.ex. högsta domstolens beslut nr 2011Da59834, 2011Da59858 och 2011Da59841 av den 26 december 2012. En engelsk sammanfattning finns på http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Detta garanteras på olika sätt i det sydkoreanska systemet. Förutom rätten till information enligt artikel 4 led 1 (i allmänhet) och artikel 20.1 i PIPA (för personuppgifter som samlas in från tredje part), samt rätten till tillgång enligt artikel 35 i PIPA, innehåller PIPA ett allmänt öppenhetskrav när det gäller ändamålet med behandlingen (artikel 3.1 i PIPA) och särskilda öppenhetskrav om behandlingen grundas på samtycke (artiklarna 15.2, 17.2 och 18.3 i PIPA) ([90]). Dessutom krävs enligt artikel 20.2 i PIPA att vissa personuppgiftsansvariga – där behandlingen överskrider vissa tröskelvärden ([91]) – underrättar den registrerade vars personuppgifter de har mottagit från en tredje part om informationskällan, ändamålet med behandlingen och den registrerades rätt att begära att behandlingen upphör, såvida inte en sådan underrättelse visar sig vara omöjlig på grund av att kontaktuppgifter saknas. Undantag gäller för vissa personuppgiftsregister som innehas av myndigheter, särskilt sådana som innehåller uppgifter som behandlas för ändamål som rör den nationella säkerheten, andra särskilt viktiga (”allvarliga”) nationella intressen eller brottsbekämpande ändamål, eller när underrättelse sannolikt kan skada en annan persons liv eller kropp, eller otillbörligt skadar en annan persons äganderätt och andra intressen, dock endast när de berörda offentliga eller privata intressena är ”uppenbart överordnade” (artikel 20.4 i PIPA). Detta kräver en avvägning av intressen.

(68) Dessutom föreskrivs i artikel 3.5 i PIPA att personuppgiftsansvariga ska offentliggöra sin integritetspolicy (och andra frågor som rör behandling av personuppgifter). Detta krav specificeras närmare i artikel 30 i PIPA jämförd med artikel 31 i genomförandedekretet till PIPA. Enligt dessa bestämmelser måste den allmänna integritetspolicyn bl.a. omfatta 1) de typer av personuppgifter som behandlas, 2) ändamålet med behandlingen, 3) lagringsperioden, 4) huruvida personuppgifter tillhandahålls en tredje part ([92]), 5) eventuell underentreprenad, 6) information om den registrerades rättigheter och hur de ska utövas och 7) kontaktinformation (däribland den dataskyddsansvariges namn eller den interna avdelning som ansvarar för att säkerställa efterlevnaden av dataskyddet och hantering av klagomål). Integritetspolicyn måste göras tillgänglig för allmänheten på ett sådant sätt att registrerade ”lätt kan känna igen den” (artikel 30.2 i PIPA) ([93]) och måste uppdateras kontinuerligt (artikel 31.2 i genomförandedekretet till PIPA).

(69) Offentliga institutioner omfattas av en ytterligare skyldighet att registrera information hos nämnden för skydd av personuppgifter, särskilt följande: 1) den offentliga institutionens namn, 2) grunderna för och ändamålen med behandlingen av personuppgiftsregistret, 3) information om de personuppgifter som registreras, 4) behandlingsmetoden, 5) lagringstiden, 6) antalet registrerade vars personuppgifter lagras, 7) avdelningen som hanterar registrerades begäranden och 8) mottagare av personuppgifter om uppgifter tillhandahålls rutinmässigt eller upprepade gånger (artikel 32-1 i PIPA) ([94]). Registrerade personuppgiftsregister offentliggörs av nämnden för skydd av personuppgifter och offentliga institutioner måste hänvisa till dem i sin integritetspolicy (artiklarna 30.1 och 32.4 i PIPA).

(70) För att öka öppenheten för registrerade i unionen vars personuppgifter överförs till Sydkorea på grundval av detta beslut införs ytterligare krav på öppenhet i avsnitt 3 i och 3 ii i meddelande 2021-5 (bilaga I). För det första ska sydkoreanska personuppgiftsansvariga när de tar emot personuppgifter från unionen på grundval av detta beslut utan onödigt dröjsmål (och under alla omständigheter senast en månad efter överföringen) underrätta de berörda registrerade om namn och kontaktuppgifter för de enheter som överför och tar emot uppgifterna, de personuppgifter (eller kategorier av personuppgifter) som överförts, den sydkoreanska personuppgiftsansvariges ändamål med insamlingen, lagringstiden och de rättigheter som är tillgängliga enligt PIPA. För det andra måste de registrerade underrättas om bl.a. följande när personuppgifter som mottagits från unionen på grundval av detta

([90]) När personuppgifter behandlas med en enskild persons samtycke måste den personuppgiftsansvarige särskilt informera personen om ändamålet med behandlingen, vilka uppgifter som ska behandlas, mottagaren av uppgifterna, den tid under vilken personuppgifter lagras och används samt om att personen har rätt att neka samtycke (och eventuella nackdelar som kan uppstå till följd av detta).

([91]) Enligt artikel 15-2.1 i genomförandedekretet till PIPA gäller detta personuppgiftsansvariga som behandlar känsliga uppgifter om minst 50 000 registrerade, eller ”normala” personuppgifter om minst en miljon registrerade. I artikel 15-2.2 i genomförandedekretet till PIPA fastställs formerna för och tidpunkten för underrättelse, och i artikel 15-2.3 anges kravet på viss dokumentation avseende detta. Dessutom gäller särskilda regler för vissa kategorier av leverantörer av informations- och kommunikationstjänster (de som genererade intäkter på minst 10 miljarder won under det föregående året, eller de som lagrar/hanterar personuppgifter för minst en miljon användare per dag i genomsnitt under tre månader före utgången av föregående år). De är skyldiga att regelbundet underrätta användarna om hur deras personuppgifter har använts, såvida detta inte visar sig vara omöjligt på grund av att kontaktinformation saknas (artikel 39-8 i PIPA och artikel 48-6 i genomförandedekretet till PIPA).

([92]) Enligt den information som den sydkoreanska regeringen har lämnat innebär detta en skyldighet att förteckna mottagaren eller mottagarna separat i integritetspolicyn.

([93]) Ytterligare bestämmelser fastställs i artikel 31.3 i genomförandedekretet till PIPA.

([94]) Registreringskravet gäller inte för vissa typer av personuppgiftsregister, till exempel sådana som registrerar frågor som rör nationell säkerhet, diplomatiska hemligheter, brottsutredningar, åtal, bestraffning, utredningar av brott med anknytning till beskattning eller ärenden som uteslutande rör intern arbetsutövning (artikel 32.2 i PIPA).

beslut tillhandahålls tredje part: mottagaren, de personuppgifter (eller kategorier av personuppgifter) som ska tillhandahållas, det land till vilket uppgifterna översänds (om tillämpligt) samt de rättigheter som är tillgängliga enligt PIPA ([95]). Meddelandet säkerställer därmed att enskilda personer i EU fortsatt informeras om de specifika personuppgiftsansvariga som behandlar deras uppgifter och kan utöva sina rättigheter gentemot de berörda enheterna.

(71) I avsnitt 3 iii i meddelande (bilaga I) tillåts vissa begränsade och kvalificerade undantag från dessa ytterligare krav på öppenhet som i huvudsak motsvarar dem som föreskrivs i förordning (EU) 2016/679. I synnerhet krävs inte att registrerade i unionen underrättas 1) om och så länge som det är nödvändigt att begränsa underrättelsen av vissa skäl relaterade till allmänintresset (t.ex. om uppgifterna behandlas för ändamål som rör nationell säkerhet eller pågående brottsutredningar), i den mån dessa mål av allmänt intresse är uppenbart överordnade den registrerades rättigheter, 2) om den registrerade redan förfogar över informationen, 3) om och så länge som underrättelsen sannolikt skulle skada den enskildes eller en annan persons liv eller kropp, eller utgöra en otillbörlig överträdelse av en annan persons egendomsintressen, om dessa rättigheter eller intressen är uppenbart överordnade den registrerades rättigheter, eller 4) om det inte finns några kontaktuppgifter för de berörda personerna, eller om det skulle krävas en oproportionerlig ansträngning för att underrätta dem. Vid bedömningen av om det är möjligt att kontakta den registrerade eller om detta innebär alltför stora ansträngningar ska hänsyn tas till möjligheten att samarbeta med uppgiftsutföraren i unionen.

(72) Reglerna i skälen 67–71 säkerställer därför en skyddsnivå när det gäller öppenhet som i huvudsak motsvarar den som föreskrivs i förordning (EU) 2016/679.

2.3.8 *Enskildas rättigheter*

(73) De registrerade bör ha vissa rättigheter som kan göras gällande mot den personuppgiftsansvariga eller personuppgiftsbiträdet, särskilt rätten till tillgång till uppgifter, rätten till rättelse, rätten att invända mot behandlingen och rätten att få uppgifter raderade. Samtidigt kan sådana rättigheter vara föremål för begränsningar i den mån sådana begränsningar är nödvändiga och proportionerliga för att skydda viktiga mål av allmänt intresse.

(74) Enligt artikel 3.5 I PIPA ska den personuppgiftsansvarige garantera registrerade de rättigheter som anges i artikel 4 i PIPA och som specificeras närmare i artiklarna 35–37, 39 och 39-2 i PIPA.

(75) För det första har enskilda personer rätt till information och tillgång. När den personuppgiftsansvarige har samlat in personuppgifter från en tredje part (vilket alltid kommer att vara fallet när uppgifterna överförs från unionen) har registrerade i allmänhet rätt att få information om 1) källan till de personuppgifter som samlats in (dvs. den överförande parten), 2) ändamålet med behandlingen och 3) det faktum att den registrerade har rätt att begära att behandlingen upphör (artikel 20.1 i PIPA). Begränsade undantag gäller, nämligen om en sådan underrättelse sannolikt skulle skada en annan persons liv eller kropp, eller ”orättfärdigt skada en annan persons äganderätt och andra intressen”, men endast om dessa tredje parters intressen är ”uttryckligen överordnade” den registrerades rättigheter (artikel 20.4 led 2 i PIPA).

(76) Dessutom ger artikel 35.1 och 35.3 i PIPA jämförd med artikel 41.4 i genomförandedekretet till PIPA registrerade personer rätt att få tillgång till sina personuppgifter ([96]). Rätten till tillgång omfattar bekräftelse på behandlingen, information om vilken typ av uppgifter som behandlats, ändamålet med behandlingen, lagringstiden samt varje

([95]) Meddelande 2021-5, avsnitt 3 ii (bilaga I).

([96]) Enligt artikel 35.3 i PIPA jämförd med artikel 42.2 i genomförandedekretet till PIPA får den personuppgiftsansvarige skjuta upp tillgången baserat på ”goda skäl” (dvs. på motiverade grunder, t.ex. om det behövs mer tid för att bedöma om tillgång kan ges), men ska underrätta den registrerade om detta inom tio dagar och lämna information om hur detta beslut kan överklagas. Så snart som grunderna för uppskovet inte längre föreligger måste tillgång beviljas.

utlämnande till tredje part och tillhandahållande av en kopia av de personuppgifter som behandlas (artikel 4 led 3 i PIPA jämförd med artikel 41.1 i genomförandedekretet till PIPA) ([97]). Tillgången får begränsas (delvis tillgång) ([98]) eller nekas endast om detta föreskrivs i lag ([99]), om det sannolikt skulle orsaka skada på en tredje parts liv eller kropp eller en omotiverad kränkning av en annan persons äganderätt eller andra intressen (artikel 35.4 i PIPA) ([100]). Det senare innebär att en avvägning bör göras mellan den enskilda personens konstitutionellt skyddade rättigheter och friheter å ena sidan, och andra personers sådana å andra sidan. Om tillgång begränsas eller nekas måste den personuppgiftsansvarige underrätta den registrerade om skälen till detta och hur beslutet kan överklagas (artiklarna 41.5 och 42.2 i genomförandedekretet till PIPA).

(77) För det andra har registrerade rätt till rättelse eller radering ([101]) av sina personuppgifter, ”om inte annat uttryckligen anges i annan lagstiftning” (artikel 36.1 och 36.2 i PIPA) ([102]). Efter att ha mottagit en begäran ska den personuppgiftsansvarige utan dröjsmål utreda frågan, vidta nödvändiga åtgärder ([103]) och underrätta den registrerade om detta inom tio dagar. Om begäran inte kan beviljas omfattar detta krav på underrättelse skälen till avslaget och hur man kan överklaga (se artikel 36.4 i PIPA jämförd med artikel 43.3 i genomförandedekretet till PIPA) ([104]).

(78) Slutligen har registrerade rätt till att behandlingen av deras personuppgifter upphör utan dröjsmål ([105]), såvida inte ett av de uppräknade undantagen är tillämpligt (artikel 37.1 och 37.2 i PIPA) ([106]). Den personuppgiftsansvarige får neka en sådan begäran 1) om detta uttryckligen tillåts enligt lag eller är nödvändigt (”oundvikligt”) för att uppfylla rättsliga skyldigheter, 2) om upphörande sannolikt skulle orsaka skada på en tredje parts liv eller kropp, eller en omotiverad kränkning av en annan persons äganderätt och andra intressen, 3) om det skulle vara omöjligt för en offentlig institution att fullgöra sina uppgifter enligt lag utan att behandla uppgifterna, eller 4) om den registrerade underlåter att uttryckligen häva det underliggande avtalet med den personuppgiftsansvariga även om det inte skulle vara praktiskt möjligt att genomföra avtalet utan sådan behandling av uppgifter. I detta fall måste den personuppgiftsansvarige utan dröjsmål underrätta den registrerade om skälen till avslaget och hur man kan överklaga (artikel 37.2 i PIPA jämförd med artikel 44.2 i genomförandedekretet till PIPA). Enligt artikel 37.4 i PIPA måste den personuppgiftsansvarige utan dröjsmål ”vidta nödvändiga åtgärder, inklusive förstöring av relevanta personuppgifter” för att uppfylla kraven i begäran om upphörande ([107]).

(79) Rätten till upphörande gäller också när personuppgifter används för direkt marknadsföring, dvs. för att främja försäljning av varor eller tjänster, eller för att försöka få till stånd köp av dessa. Sådan ytterligare behandling kräver dessutom i allmänhet den registrerades specifika (ytterligare) samtycke (se artikel 15.1 led 1, artikel 17.2 led 1 i PIPA) ([108]). När den personuppgiftsansvarige begär detta samtycke måste den registrerade i synnerhet informeras om hur uppgifterna avses att användas för direkt marknadsföring (dvs. det faktum att han eller hon

([97]) Tillgång till personuppgifter som behandlas av en offentlig institution kan erhållas direkt från institutionen eller indirekt genom att en begäran lämnas in till nämnden för skydd av personuppgifter, som utan dröjsmål ska vidarebefordra begäran (artikel 35.2 i PIPA och artikel 41.3 i genomförandedekretet till PIPA).

([98]) Enligt artikel 42.1 i genomförandedekretet till PIPA är den personuppgiftsansvarige skyldig att bevilja delvis tillgång när åtminstone en del av uppgifterna inte omfattas av skälen för avslag.

([99]) En sådan lag måste i sin tur respektera den grundläggande rätten till integritet och dataskydd, samt principerna om nödvändighet och proportionalitet som fastställs i den sydkoreanska författningen.

([100]) Dessutom får offentliga institutioner vägra att bevilja tillgång om detta skulle orsaka allvarliga svårigheter när vissa uppgifter utförs, bl.a. pågående revisioner eller införande, uppbörd eller återbetalning av skatter (artikel 35.4 i PIPA).

([101]) I detta fall måste den personuppgiftsansvarige vidta åtgärder för att förhindra att personuppgifterna återställs, se artikel 36.3 i PIPA.

([102]) Sådana lagar måste uppfylla kraven i författningen om att en grundläggande rättighet endast får begränsas när det är nödvändigt för den nationella säkerheten eller för upprätthållandet av lag och ordning för medborgarnas välfärd, och får inte påverka det väsentliga innehållet i friheten eller rätten (artikel 37.2 i författningen).

([103]) I artikel 43.2 i genomförandedekretet till PIPA föreskrivs ett särskilt förfarande om den personuppgiftsansvarige behandlar personuppgiftsregister som tillhandahållits av en annan personuppgiftsansvarig.

([104]) Underlåtenhet att vidta nödvändiga åtgärder för att rätta eller radera personuppgifter och kontinuerlig användning eller tillhandahållande av dessa uppgifter till en tredje part kan leda till straffrättsliga påföljder (artikel 73.2 i PIPA).

([105]) I enlighet med artikel 44.2 i PIPA ska den personuppgiftsansvarige informera den registrerade om att behandlingen har upphört inom tio dagar från mottagandet av begäran.

([106]) När det gäller offentliga institutioner får rätten till behandlingens upphörande utövas med avseende på uppgifter i personuppgiftsregister (artikel 37 jämförd med artikel 32 i PIPA). En sådan registrering krävs inte i ett begränsat antal situationer, t.ex. om personuppgiftsregistret rör nationell säkerhet, brottsutredningar, diplomatiska förbindelser osv. (artikel 32.2 i PIPA).

([107]) Underlåtenhet att upphöra med behandlingen kan leda till straffrättsliga påföljder (artikel 73.3 i PIPA).

([108]) Kommittén för tvistlösning (se skäl 133) har behandlat ett flertal ärenden där enskilda personer framförde klagomål angående användning av deras uppgifter för direkt marknadsföring utan samtycke, vilket bl.a. ledde till att berörd personuppgiftsansvarig betalade ut ersättning och raderade personuppgifter (se t.ex. kommittén för tvistlösning 20R10-024(2020.11.18), 20R08-015 (2020.8.28), 20R07-031(2020.9.1)).

kan komma att kontaktas vid marknadsföring av varor eller tjänster eller värvning för köp av dessa) på ett ”tydligt och igenkännligt sätt” (artikel 22.2 och 22.4 i PIPA jämförd med artikel 17.2 led 1 i genomförandedekretet till PIPA).

(80) För att underlätta utövandet av enskildas rättigheter måste den personuppgiftsansvarige inrätta särskilda förfaranden och offentliggöra dem (artikel 38.4 i PIPA) ([109]). Detta inbegriper förfaranden för att göra invändningar mot avslag på en begäran (artikel 38.5 i PIPA). Den personuppgiftsansvarige ska säkerställa att förfarandet för utövande av rättigheter är användarvänligt med avseende på de registrerade och inte svårare än förfarandet för insamling av personuppgifter. Detta inbegriper även skyldigheten att lämna information om förfarandet på den egna webbplatsen (artiklarna 41.2, 43.1 och 44.1 i genomförandedekretet till PIPA) ([110]). Enskilda personer kan ge en företrädare tillstånd att lämna in en sådan begäran (artikel 38.1 i PIPA jämförd med artikel 45 i genomförandedekretet till PIPA). Den personuppgiftsansvarige har rätt att ta ut en avgift (och vid begäran om att skicka kopior av personuppgifter även porto) men beloppet ska fastställas ”inom de faktiska kostnaderna för behandlingen av [begäran]”. Ingen avgift (eller porto) får tas ut om den personuppgiftsansvarige har orsakat begäran (artikel 38.3 i PIPA jämförd med artikel 47 i genomförandedekretet till PIPA).

(81) PIPA och genomförandedekretet saknar allmänna bestämmelser avseende beslut som påverkar den registrerade och uteslutande grundar sig på automatisk behandling av personuppgifter. Vad gäller personuppgifter som samlats in i unionen kommer dock de beslut som bygger på automatisk insamling normalt att fattas av den personuppgiftsansvarige i unionen (som har en direkt förbindelse med berörd registrerad) och omfattas därför av förordning (EU) 2016/679 ([111]). Detta inbegriper fall av överföringar i vilka behandlingen sköts av en utländsk (t. ex. sydkoreansk) näringsidkare i en funktion som agent (personuppgiftsbiträde) på uppdrag av den personuppgiftsansvarige i unionen (eller som underentreprenör på uppdrag av unionens personuppgiftsbiträde, som tagit emot uppgifterna från en personuppgiftsansvarig i unionen som samlat in dem) som sedan fattar beslut på denna grundval. Avsaknaden av särskilda regler om automatiserat beslutsfattande i PIPA kommer därför sannolikt inte att påverka omfattningen av skyddet av personuppgifter som överförs enligt detta beslut.

(82) Som ett undantag är bestämmelserna om öppenhet på begäran (artikel 20) och enskildas rättigheter (artiklarna 35–37) samt kravet på individuell underrättelse för leverantörer av informations- och kommunikationstjänster (artikel 39-8 i PIPA) inte tillämpliga på pseudonymiserade uppgifter när de behandlas för ändamål som rör statistik, vetenskaplig forskning eller arkivändamål i allmänhetens intresse (artikel 28-7 i PIPA) ([112]). I linje med artikel 11.2 (med skäl 57) i förordning (EU) 2016/679 motiveras detta med att den personuppgiftsansvarige för att säkerställa öppenhet eller bevilja individuella rättigheter skulle behöva identifiera om några (och om så är fallet vilka) uppgifter är kopplade till den enskilda person som lämnar in begäran, vilket är uttryckligen förbjudet enligt PIPA (artikel 28-5.1 i PIPA). Om en sådan återidentifiering upphäver pseudonymiseringen av hela (den pseudonymiserade) datauppsättningen skulle detta dessutom innebära att alla de berörda individernas personuppgifter utsätts för ökade risker. Medan det i förordning (EU) 2016/679 hänvisas till situationer där återidentifiering är praktiskt taget omöjlig, tillämpas en strängare strategi i PIPA genom att återidentifiering uttryckligen förbjuds i alla situationer där pseudonymiserade uppgifter behandlas.

(83) Det sydkoreanska systemet, såsom det beskrivs i skälen 74–82, innehåller därför regler om registrerade personers rättigheter som ger en skyddsnivå som i huvudsak motsvarar den som fastställs i förordning (EU) 2016/679.

([109]) Se även artikel 30.1 led 5 i PIPA om integritetspolicyn, som bl.a. ska omfatta information om den enskilda personens rättigheter och hur de kan utövas.

([110]) Se även artikel 39-7.2 avseende leverantörer av informations- och kommunikationstjänster.

([111]) I de undantagsfall i vilka den sydkoreanska näringsidkaren omvänt har en direkt relation till den registrerade i EU, kommer detta normalt att vara en följd av att näringsidkaren har inriktat sig på den berörde enskilde i Europeiska unionen genom att erbjuda vederbörande varor eller tjänster eller övervakat vederbörandes beteende. I detta fall skulle den sydkoreanska näringsidkaren själv omfattas av tillämpningsområdet för förordning (EU) 2016/679 (artikel 3.2) och måste således direkt efterleva EU:s dataskyddslag.

([112]) Se även meddelande 2021-5 där det bekräftas att avsnitt 3 i PIPA (inklusive artikel 28-7) endast tillämpas när pseudonymiserade uppgifter behandlas för vetenskaplig forskning, statistik eller arkivändamål i allmänhetens intresse, se avsnitt 4 i bilaga I till detta beslut.

2.3.9 *Vidare överföringar*

(84) Den erforderliga skyddsnivån för personuppgifter som överförs från unionen till personuppgiftsansvariga i Sydkorea får inte undergrävas av ytterligare överföring av personuppgifter till mottagare i ett tredjeland.

(85) Sådana ”vidare överföringar” utgör internationella överföringar från Sydkorea ur den sydkoreanska personuppgiftsansvariges perspektiv. I detta avseende görs i PIPA en åtskillnad mellan utkontraktering av behandling till en uppdragstagare (dvs. ett personuppgiftsbiträde) och tillhandahållande av personuppgifter till tredje part ([113]).

(86) För det första måste den sydkoreanska personuppgiftsansvarige vid utkontraktering av behandling av personuppgifter till en enhet i ett tredjeland se till att bestämmelserna i PIPA avseende utkontraktering efterlevs (artikel 26 i PIPA). Detta inbegriper införande av ett rättsligt bindande instrument genom vilket bl.a. uppdragstagarens behandling begränsas till det utkontrakterade arbetets ändamål, tekniska och administrativa skyddsåtgärder införs och underentreprenad begränsas (se artikel 26.1 i PIPA) tillsammans med en begränsning av offentliggörande av information om det utkontrakterade arbetet. Den personuppgiftsansvarige är dessutom skyldig att ge uppdragstagaren ”utbildning” om nödvändiga säkerhetsåtgärder och att bl.a. genom kontroller övervaka efterlevnaden av alla den personuppgiftsansvariges skyldigheter enligt PIPA ([114]) samt enligt avtalet om utkontraktering.

(87) Om uppdragstagaren orsakar skada genom att behandla personuppgifter i strid med PIPA kommer detta att tillskrivas den personuppgiftsansvarige när det gäller ansvarsfrågan, vilket skulle vara fallet med den personuppgiftsansvariges anställda (artikel 26.6 i PIPA). Den sydkoreanska personuppgiftsansvarige är därför fortsatt ansvarig för de personuppgifter som har utkontrakterats och måste säkerställa att det utomeuropeiska personuppgiftsbiträdet behandlar uppgifterna i enlighet med PIPA. Om uppdragstagaren behandlar uppgifterna i strid med PIPA kan Sydkoreas personuppgiftsansvarige hållas ansvarig för underlåtenhet att uppfylla sin skyldighet att säkerställa efterlevnad av PIPA, t.ex. genom sin övervakning av uppdragstagaren. De skyddsåtgärder som ingår i avtalet om utkontraktering och Sydkoreas personuppgiftsansvariges ansvar för uppdragstagarens verksamhet säkerställer kontinuitet i skyddet när behandling av personuppgifter utkontrakteras till enheter utanför Sydkorea.

(88) För det andra kan sydkoreanska personuppgiftsansvariga lämna ut personuppgifter till en tredje part utanför Sydkorea. Även om PIPA innehåller ett antal rättsliga grunder som möjliggör tillhandahållande till tredje part generellt sett måste den personuppgiftsansvarige om den tredje parten finns utanför Sydkorea i princip ([115]) erhålla den registrerades samtycke ([116]) efter att ha underrättat den registrerade om 1) typen av personuppgifter, 2) mottagaren av personuppgifterna, 3) ändamålet med överföringen, vilket innebär ändamålet med mottagarens behandling, 4) lagringstiden för mottagarens behandling samt 5) det faktum att den registrerade får vägra att ge sitt samtycke (artikel 17.2, 17.3 i PIPA). Enligt meddelande 2021-5, i avsnittet om öppenhet (se skäl 70), krävs att enskilda personer informeras om det tredjeland till vilket deras uppgifter kommer att lämnas. Detta säkerställer att registrerade i unionen kan fatta ett fullständigt informerat beslut om huruvida de samtycker till att uppgifterna lämnas ut till utlandet eller inte. Dessutom får den personuppgiftsansvarige inte ingå avtal med mottagande tredje part i strid med PIPA, vilket innebär att avtalet inte får innehålla skyldigheter som skulle strida mot de krav som ställs på den personuppgiftsansvarige enligt PIPA ([117]).

([113]) Särskilda regler gäller för leverantörer av informations- och kommunikationstjänster. I enlighet med artikel 39-12 i PIPA måste leverantörer av informations- och kommunikationstjänster i princip erhålla användarens samtycke för all överföring av personuppgifter till utlandet. Om personuppgifter överförs som en del av utkontraktering av behandling, även för lagring, krävs inget samtycke om de berörda personerna direkt eller genom ett lättillgängligt offentligt meddelande har informerats i förväg om 1) de uppgifter som ska överföras, 2) det land till vilket uppgifterna kommer att överföras (samt datum och metod för överföringen), 3) mottagarens namn och 4) ändamålet med mottagarens användning och lagring (artikel 39-12.3 i PIPA). Dessutom kommer i sådana fall de allmänna kraven för utkontraktering att gälla. För varje överföring måste särskilda skyddsåtgärder införas när det gäller säkerhet, hantering av klagomål och tvister samt andra åtgärder som är nödvändiga för att skydda användarnas uppgifter (artikel 48-10 i genomförandedekretet till PIPA).

([114]) Se även artikel 26.7 i PIPA, enligt vilken artiklarna 15–25, 27–31, 33–38 och 50 i tillämpliga delar ska tillämpas på personuppgiftsbiträden.

([115]) Om leverantörer av informations- och kommunikationstjänster tillhandahåller användares personuppgifter till tredje part kräver detta alltid användarens samtycke (artikel 39-12.2 i PIPA).

([116]) Såsom förklaras mer ingående i skäl 51 måste ett sådant samtycke vara frivilligt, informerat och specifikt för att vara giltigt.

([117]) Se även artikel 39-12.1 i PIPA avseende leverantörer av informations- och kommunikationstjänster.

(89) Utan den enskilda personens samtycke får personuppgifter tillhandahållas en tredje part (utomlands) om ändamålet med utlämnandet fortfarande är ”inom ramen för det tillämpningsområde som rimligen kan hänföras till insamlingsändamålet” (artikel 17.4 i PIPA, se skäl 36). Vid beslut om utlämnande av personuppgifter för ett ”närbesläktat” ändamål måste den personuppgiftsansvarige dock beakta huruvida utlämnandet av uppgifterna medför nackdelar för den enskilda personen och huruvida nödvändiga säkerhetsåtgärder (t.ex. kryptering) har vidtagits. Med tanke på att det tredjeland till vilket personuppgifter överförs eventuellt inte erbjuder skydd liknande dem som tillhandahålls enligt PIPA, erkänns det i avsnitt 2 i meddelande 2021-5 att sådana nackdelar kan uppstå och att de endast kan undvikas om den sydkoreanska personuppgiftsansvarige och den utomeuropeiska mottagaren säkerställer en skyddsnivå som motsvarar den i PIPA genom ett rättsligt bindande instrument (t.ex. ett avtal), även med avseende på de registrerades rättigheter.

(90) Särskilda regler gäller för offentliggörande som går utanför ändamålet, dvs. tillhandahållande av uppgifter till en tredje part för ett nytt (icke-närbesläktat) ändamål, vilket endast får ske på grundval av något av de skäl som anges i artikel 18.2 i PIPA, såsom beskrivs i skäl 39. Även under dessa förhållanden är dock tillhandahållande till tredje part endast tillåtet om det är osannolikt att det ”otillbörligt överträder” den registrerades eller tredje parts intressen, vilket kräver en avvägning av intressen. Dessutom måste den personuppgiftsansvarige enligt artikel 18.5 i PIPA tillämpa ytterligare skyddsåtgärder, vilket kan inbegripa en begäran till den tredje parten om att begränsa ändamålet med och metoden för behandlingen eller att införa särskilda säkerhetsåtgärder. Återigen, med tanke på att det tredjeland till vilket personuppgifter överförs eventuellt inte erbjuder skydd liknande dem som tillhandahålls enligt PIPA. erkänns det i avsnitt 2 i meddelande 2021-5 att ”otillbörlig överträdelse” av den enskilda personens eller tredje parts intressen kan uppstå och att det endast kan undvikas om den sydkoreanska personuppgiftsansvarige och den utomeuropeiska mottagaren säkerställer en skyddsnivå som motsvarar den i PIPA genom ett rättsligt bindande instrument (t.ex. ett avtal). Detta även med avseende på de registrerades rättigheter.

(91) Reglerna i skälen 86–90 säkerställer därmed kontinuitet i skyddet när personuppgifter överförs vidare (till en ”uppdragstagare” eller en tredje part) från Sydkorea på ett sätt som i huvudsak motsvarar vad som föreskrivs i förordning (EU) 2016/679.

2.3.10 *Ansvarsskyldighet*

(92) Enligt principen om ansvarsskyldighet är enheter som behandlar uppgifter skyldiga att införa lämpliga tekniska och organisatoriska åtgärder för att effektivt fullgöra sina skyldigheter att skydda uppgifter och kunna uppvisa sådan överensstämmelse, särskilt för den behöriga tillsynsmyndigheten.

(93) Enligt artikel 3.6 och 3.8 i PIPA ska den personuppgiftsansvarige behandla personuppgifter ”på ett sätt som minimerar risken för överträdelse” av den registrerades integritet och sträva efter att få den registrerades förtroende genom att iaktta och fullgöra de uppgifter och ansvarsområden som anges i PIPA och andra relaterade lagar. Detta inbegriper upprättandet av en intern förvaltningsplan (artikel 29 i PIPA) samt lämplig utbildning och övervakning av de anställda (artikel 28 i PIPA).

(94) För att säkerställa ansvarsskyldighet införs genom artikel 31 i PIPA jämförd med artikel 32 i genomförandedekretet till PIPA en skyldighet för personuppgiftsansvariga att utse en dataskyddsansvarig som ”på ett heltäckande sätt ansvarar för behandlingen av personuppgifter”. En dataskyddsansvarig har i synnerhet följande uppgifter: 1) upprätta och genomföra en plan för skydd av personuppgifter och utarbeta en integritetspolicy, 2) genomföra regelbundna undersökningar om status och praxis vid behandling av personuppgifter i syfte att förbättra eventuella brister, 3) hantera klagomål och kompensation, 4) inrätta ett internt kontrollsystem för att förhindra att personuppgifter röjs, missbrukas eller används felaktigt, 5) förbereda och genomföra ett utbildningsprogram, 6) skydda, kontrollera och hantera personuppgiftsregister och 7) förstöra personuppgifter när ändamålet med behandlingen har uppnåtts eller lagringstiden har löpt ut. Vid fullgörande av dessa uppgifter får den dataskyddsansvarige kontrollera tillståndet hos behandlingen av personuppgifter och tillhörande system och begära information om detta (artikel 31.3 i PIPA). Om den dataskyddsansvarige får kännedom om någon överträdelse av PIPA eller andra relevanta dataskyddslagar ska han eller hon omedelbart vidta korrigerande åtgärder och rapportera dessa åtgärder till den personuppgiftsansvariges ledning (”chef”) vid behov (artikel 31.4 i PIPA). Enligt artikel 31.5 i PIPA får den dataskyddsansvarige inte drabbas av omotiverade nackdelar till följd av utförandet av dessa uppgifter.

(95) Dessutom måste personuppgiftsansvariga proaktivt sträva efter att genomföra en konsekvensbedömning av inverkan på integritetsskyddet om användningen av personuppgiftsregister medför en risk för den personliga integriteten (artikel 33.8 i PIPA). På grundval av artikel 33.1 och 33.2 i PIPA jämförd med artiklarna 35, 36 och 38 i genomförandedekretet till PIPA kommer faktorer som de behandlade uppgifternas typ och beskaffenhet (särskilt huruvida de utgör känslig information), volym och lagringsperiod samt sannolikheten för uppgiftsincidenter att vara relevanta vid bedömningen av graden av risk för de registrerades rättigheter. Syftet med konsekvensbedömningen av inverkan på integritetsskyddet är att se till att riskfaktorerna avseende personlig integritet samt eventuella säkerhetsåtgärder eller andra motåtgärder analyseras, och att ange områden som behöver förbättras (se artikel 33.1 i PIPA jämförd med artikel 38 i genomförandedekretet till PIPA).

(96) Offentliga institutioner är skyldiga att genomföra en konsekvensbedömning vid behandling av vissa personuppgiftsregister som medför en större risk för eventuella kränkningar av integriteten (artikel 33.1 i PIPA). I enlighet med artikel 35 i genomförandedekretet till PIPA gäller detta bl.a. för register som innehåller känsliga uppgifter om minst 50 000 registrerade, register som kommer att matchas med andra register och som en följd av detta kommer att innehålla uppgifter om minst 500 000 registrerade eller register som innehåller uppgifter om minst en miljon registrerade. Resultatet av en konsekvensbedömning som utförs av en offentlig institution måste meddelas nämnden för skydd av personuppgifter (artikel 33.1 i PIPA), som får avge ett yttrande (artikel 33.3 i PIPA).

(97) Slutligen föreskrivs i artikel 13 i PIPA att nämnden för skydd av personuppgifter ska fastställa de riktlinjer som krävs för att främja och stödja ”självreglerande dataskyddsverksamhet” som utförs av personuppgiftsansvariga, bl. a. genom utbildning om dataskydd, främjande av och stöd till organisationer som arbetar med dataskydd och genom att hjälpa personuppgiftsansvariga att fastställa och genomföra självreglerande regler. Den ska dessutom införa och underlätta systemet för e-integritet. I detta avseende ges i artikel 32-2 i PIPA jämförd med artiklarna 34-2–34-8 i genomförandedekretet till PIPA möjligheten att intyga att en personuppgiftsansvarigs system för behandling och skydd av personuppgifter uppfyller kraven i PIPA. Enligt dessa regler kan en certifiering ([118]) beviljas (för en period på tre år) om den personuppgiftsansvarige uppfyller de certifieringskriterier som har fastställts av nämnden för skydd av personuppgifter, däribland inrättande av administrativa, tekniska och fysiska skyddsåtgärder för att skydda personuppgifter ([119]). Nämnden för skydd av personuppgifter måste minst en gång om året granska den personuppgiftsansvariges system som är relevanta för certifieringen för att upprätthålla dess effektivitet, vilket kan leda till att certifieringen återkallas (artikel 32.4 i PIPA jämförd med artikel 34-5 i genomförandedekretet till PIPA; så kallad uppföljningshantering).

(98) Inom den sydkoreanska ramen genomförs därför principen om ansvarsskyldighet på ett sätt som säkerställer en skyddsnivå som i huvudsak motsvarar den som fastställs i förordning (EU) 2016/679, bl.a. genom att tillhandahålla olika mekanismer för att säkerställa och påvisa överensstämmelse med PIPA.

2.3.11 *Särskilda regler för behandling av personlig kreditinformation*

(99) Så som beskrivs i skäl 13 fastställs i lagen om användning och skydd av kreditinformation särskilda regler för kommersiella operatörers behandling av personlig kreditinformation. Vid behandling av personlig kreditinformation måste de kommersiella operatörerna därför uppfylla de allmänna kraven i PIPA, såvida inte lagen om användning och skydd av kreditinformation innehåller mer specifika regler. Detta är t.ex. fallet när de behandlar uppgifter som rör ett kreditkort eller bankkonto i samband med en affärstransaktion med en enskild person. Som sektorslagstiftning för behandling av kreditinformation (både personlig och icke-personlig) införs genom lagen om användning och skydd av kreditinformation inte bara särskilda garantier för dataskydd (t.ex. i fråga om öppenhet och säkerhet), utan mer allmänt regleras där även de särskilda omständigheter under vilka personlig kreditinformation får behandlas. Detta återspeglas särskilt i de detaljerade kraven för användning, tillhandahållande av uppgifter till tredje part och lagring av sådana uppgifter.

(100) Liksom PIPA återspeglas i lagen om användning och skydd av kreditinformation principen om laglighet och proportionalitet. För det första, som ett allmänt krav, tillåts enligt artikel 15.1 i lagen om användning och skydd av kreditinformation endast insamling av personlig kreditinformation på rimliga och korrekta sätt och i den minsta mån som krävs för att tjäna ett bestämt syfte, i enlighet med artikel 3.1–3.2 i PIPA. För det andra regleras i lagen om användning och skydd av kreditinformation specifikt lagligheten i behandlingen av personlig kreditinformation genom att begränsa dess insamling, användning och tillhandahållande till tredje part, och denna behandling binds generellt sett till den berörda personens samtycke.

([118]) Om den personuppgiftsansvarige avser att hänvisa till eller främja certifieringen i sin affärsverksamhet får dessutom den dataskyddsmärkning som fastställts av nämnden för skydd av personuppgifter användas. Se artikel 34-7 i genomförandedekretet till PIPA.

([119]) Sedan november 2018 har systemet *Personal Information & Information Security Management System* (ISMS-P) utvecklats, som intygar att personuppgiftsansvariga har ett heltäckande ledningssystem.

(101) Personlig kreditinformation får samlas in på grundval av ett av de skäl som anges i PIPA eller på de särskilda grunder som anges i lagen om användning och skydd av kreditinformation. Eftersom artikel 45 i förordning (EU) 2016/679 förutsätter att en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen överför personuppgifter, vilket inte omfattar direkt insamling (t.ex. från en enskild person eller en webbplats) som utförs av en personuppgiftsansvarig i Sydkorea, är endast samtycke och de skäl som finns tillgängliga enligt PIPA relevanta för detta beslut. Dessa skäl omfattar i synnerhet scenarier där överföringen är nödvändig för att fullgöra ett avtal med den enskilde eller för den sydkoreanska personuppgiftsansvariges berättigade intressen (artikel 15.1 led 4 och 6 i PIPA) ([120]).

(102) Efter insamling kan personlig kreditinformation användas 1) för det ursprungliga ändamål för vilket den enskilda personen (direkt) tillhandahöll den ([121]), 2) för ett ändamål som är förenligt med det ursprungliga ändamålet med insamlingen ([122]), 3) för att fastställa om ett affärsförhållande som begärts av den enskilda personen ska upprättas eller upprätthållas ([123]), 4) för statistik, forskning och arkivändamål i allmänhetens intresse ([124]) om uppgifterna är pseudonymiserade ([125]), 5) om ytterligare samtycke erhålls, eller 6) i enlighet med lagen.

(103) Om en kommersiell operatör har för avsikt att lämna ut personlig kreditinformation till en tredje part måste denne inhämta den enskilda personens samtycke ([126]) efter att ha underrättat personen om uppgifterna, ändamålet med mottagarens behandling, vilka uppgifter som ska lämnas, mottagarens lagringsperiod och rätten att vägra samtycke (artikel 32.1 lagen om användning och skydd av kreditinformation och artikel 28.2 i genomförandedekretet till lagen om användning och skydd av kreditinformation) ([127]). Detta krav på samtycke gäller inte i särskilda situationer, nämligen när personlig kreditinformation lämnas ut i följande fall ([128]): 1) till en uppdragstagare vid utkontraktering ([129]), 2) till en tredje part vid företagsöverlåtelse, fission eller fusion, 3) för statistik, vetenskaplig forskning och arkivändamål i allmänhetens intresse, om uppgifterna är pseudonymiserade, 4) för ett ändamål som är förenligt med det ursprungliga ändamålet med insamlingen, 5) till en tredje part som använder uppgifterna för att inkassera en skuld som personen är skyldig ([130]), 6) för att följa ett domstolsbeslut, 7) till en åklagare eller tjänsteman vid kriminalpolisen i en nödsituation där den enskildes liv är i fara eller där han eller

([120]) Lagen om användning och skydd av kreditinformation innehåller också andra rättsliga grunder för insamling, dvs. när det krävs enligt lag, om uppgifterna offentliggörs av en offentlig institution i enlighet med lagstiftningen om informationsfrihet, eller om uppgifterna finns tillgängliga på ett socialt nätverk. För att den kommersiella operatören ska kunna förlita sig på det sista skälet måste den kunna visa att insamlingen ligger inom ramen för den registrerades samtycke, på grundval av en rimlig (”objektiv”) tolkning och med beaktande av uppgifternas art, avsikten och ändamålet med att göra dem tillgängliga på det sociala nätverket, om ändamålet med insamlingen är ”högst relevant” för detta ändamål osv. (artikel 13 i genomförandedekretet till lagen om användning och skydd av kreditinformation). Såsom förklaras i skäl 101 kommer dessa skäl i princip dock inte att vara relevanta i ett överföringsscenario.

([121]) När t.ex. kreditinformation genereras/tillhandahålls i samband med en affärstransaktion med den enskilda personen. Detta skäl kan dock inte åberopas för att använda personlig kreditinformation för direkt marknadsföring (se artikel 33.1 led 3 i lagen om användning och skydd av kreditinformation).

([122]) För att avgöra huruvida ändamålet med användningen är förenligt med det ursprungliga ändamålet med insamlingen måste följande faktorer beaktas: 1) förhållandet (”relevans”) mellan de två ändamålen, 2) hur uppgifterna samlades in, 3) användningens inverkan på den enskilda personen och 4) huruvida lämpliga säkerhetsåtgärder, t.ex. pseudonymisering, har genomförts (se artikel 32.6 led 9-4 i lagen om användning och skydd av kreditinformation).

([123]) En personuppgiftsansvarig kan t.ex. behöva beakta personlig kreditinformation som har mottagits från en enskild person för att kunna besluta huruvida lånets löptid ska förlängas för den personen.

([124]) Artikel 33 i lagen om användning och skydd av kreditinformation jämförd med artikel 32.6 led 9-2, 9-4 och 10 i lagen om användning och skydd av kreditinformation.

([125]) Pseudonymisering definieras enligt artikel 2.15 i lagen om användning och skydd av kreditinformation som behandling av personlig kreditinformation på ett sådant sätt att enskilda personer inte längre kan identifieras utifrån uppgifterna annat än i kombination med ytterligare information. Även om lagen om användning och skydd av kreditinformation innehåller särskilda skyddsåtgärder för behandling av pseudonymiserade uppgifter för statistik, vetenskaplig forskning och arkiveringsändamål i allmänhetens intresse (artikel 40-2 i lagen om användning och skydd av kreditinformation), är dessa regler inte tillämpliga på kommersiella organisationer. De senare omfattas i stället fortsatt av de särskilda kraven i avsnitt III i PIPA, som beskrivs i skälen 42–48. I artikel 40-3 i lagen om användning och skydd av kreditinformation undantas dessutom behandlingen av pseudonymiserad kreditinformation – när detta sker för statistik, vetenskaplig forskning eller arkiveringsändamål i allmänhetens intresse – från krav på öppenhet och enskildas rättigheter på ett sätt som liknar undantaget i artikel 28-7 i PIPA. Detta omfattas av skyddsåtgärderna i avsnitt III i PIPA, såsom beskrivs närmare i skälen 42–48.

([126]) Detta gäller inte om uppgifterna tillhandahålls en tredje part för att hålla personlig kreditinformation korrekt och uppdaterad, så länge som tillhandahållandet omfattas av det ursprungliga ändamålet med behandlingen (artikel 32.1 i lagen om användning och skydd av kreditinformation). Detta kan exempelvis inträffa när uppdaterad information tillhandahålls ett kreditvärderingsinstitut för att säkerställa att dess register är korrekta.

([127]) Om det är opraktiskt att tillhandahålla ovannämnda uppgifter kan det vara tillräckligt att hänvisa personen till tredje part för att få de uppgifter som begärs.

([128]) Med tanke på att utlämnande av personlig kreditinformation utomlands inte regleras i lagen om användning och skydd av kreditinformation måste sådana överföringar vara förenliga med de skyddsåtgärder för vidareöverföring som föreskrivs i avsnitt 2 i meddelande nr 2021-5.

([129]) Utkontraktering av behandling av personlig kreditinformation får endast ske på grundval av ett skriftligt avtal och i enlighet med kraven i artikel 26.1–26.3 och 26.5 i PIPA, såsom beskrivs i skäl 20 (artikel 17 i lagen om användning och skydd av kreditinformation och artikel 14 i genomförandedekretet till lagen om användning och skydd av kreditinformation). Uppdragstagaren får inte använda uppgifterna utöver ramen för de utkontrakterade tjänsterna, och det utkontrakterande företaget måste införa särskilda krav på säkerhet (t.ex. kryptering) och utbilda uppdragstagaren om hur man förebygger att kreditinformation går förlorad, stjäls, röjs, ändras eller äventyras.

([130]) Se även artikel 28.10 led 1, 2 och 6 i genomförandedekretet till lagen om användning och skydd av kreditinformation.

hon förväntas lida kroppsskada och där det inte finns tid att utfärda ett domstolsbeslut ([131]), 8) till behöriga skattemyndigheter för att följa skattelagstiftningen, eller 9) i enlighet med andra lagar. Om utlämning sker på grundval av ett av dessa skäl ska den registrerade underrättas i förväg (artikel 32.7 i lagen om användning och skydd av kreditinformation).

(104) I lagen om användning och skydd av kreditinformation regleras också uttryckligen hur länge personlig kreditinformation ska behandlas på grundval av ett av dessa skäl för användning eller tillhandahållande till tredje part efter det att affärsförbindelsen med den enskilda personen har upphört ([132]). Endast uppgifter som var nödvändiga för att upprätta eller bibehålla detta förhållande får lagras, med förbehåll för ytterligare skyddsåtgärder (de måste bevaras åtskilt från kreditinformation som rör enskilda personer med vilka ett affärsförhållande pågår, skyddas av särskilda säkerhetsåtgärder och endast vara tillgängliga för behöriga personer) ([133]). Alla andra uppgifter måste raderas (artikel 17-2.1 led 2 i genomförandedekretet till lagen om användning och skydd av kreditinformation). För att fastställa vilka uppgifter som var nödvändiga för affärsförbindelsen måste olika faktorer beaktas, bl.a. om det skulle ha varit möjligt att upprätta förhållandet utan uppgifterna och om de har en direkt relation till de varor eller tjänster som tillhandahållits den enskilda personen (artikel 17-2.2 i genomförandedekretet till lagen om användning och skydd av kreditinformation).

(105) Även i fall där personlig kreditinformation i princip kan bevaras även efter det att affärsförbindelsen har upphört måste den raderas inom tre månader efter det att det vidare ändamålet med behandlingen har uppnåtts ([134]), eller under alla omständigheter efter fem år (artikel 20-2 i lagen om användning och skydd av kreditinformation). I ett begränsat antal fall får personlig kreditinformation bevaras i mer än fem år, särskilt när det är nödvändigt för att fullgöra en rättslig förpliktelse, när det är nödvändigt för en enskild persons vitala intressen relaterade till liv, kropp eller egendom, för arkivering av pseudonymiserade uppgifter (som användes för vetenskaplig forskning, statistik eller arkivändamål i allmänhetens intresse) eller för försäkringsändamål (särskilt för försäkringsbetalningar eller för att förhindra försäkringsbedrägeri) ([135]). I dessa undantagsfall gäller särskilda skyddsåtgärder (t.ex. att den enskilda personen underrättas om fortsatt användning, att de lagrade uppgifterna skiljs från uppgifter som rör personer med vilka ett affärsförhållande fortfarande pågår, att åtkomsträtten begränsas, se artikel 17-2.1–17-2.2 i genomförandedekretet till lagen om användning och skydd av kreditinformation).

(106) I lagen om användning och skydd av kreditinformation specificeras även principerna om noggrannhet och uppgifternas kvalitet närmare genom att kräva att personlig kreditinformation ”registreras, ändras och hanteras” för att hålla uppgifterna korrekta och uppdaterade (artikel 18.1 i lagen om användning och skydd av kreditinformation och artikel 15.3 i genomförandedekretet till lagen om användning och skydd av kreditinformation) ([136]). När kommersiella operatörer tillhandahåller kreditinformation till vissa andra enheter (t.ex. kreditvärderingsinstitut) är de också särskilt skyldiga att kontrollera att uppgifterna är korrekta för att säkerställa att endast korrekta uppgifter registreras och hanteras av mottagaren (artikel 15.1 i genomförandedekretet till lagen om användning och skydd av kreditinformation jämförd med artikel 18.1 i lagen om användning och skydd av kreditinformation). Mer allmänt krävs enligt lagen om användning och skydd av kreditinformation att register förs över insamling, användning, utlämnande till tredje part och förstöring av personlig kreditinformation (artikel 20.2 i lagen om användning och skydd av kreditinformation) ([137]).

(107) Behandlingen av personlig kreditinformation omfattas dessutom av särskilda krav på datasäkerhet. Enligt lagen om användning och skydd av kreditinformation krävs framför allt att tekniska, fysiska och organisatoriska åtgärder vidtas för att förhindra obehörig åtkomst till datasystem samt för att förhindra att de uppgifter som behandlas ändras, förstörs eller utsätts för andra risker (detta görs t.ex. genom åtkomstkontroller, se artikel 19 i lagen om användning och skydd av kreditinformation och artikel 16 i genomförandedekretet till lagen om användning och skydd av kreditinformation). Vid utbyte av personlig kreditinformation med en tredje part måste dessutom ett avtal ingås som fastställer särskilda säkerhetsåtgärder (artikel 19.2 i lagen om användning och skydd av kreditinformation). Om en säkerhetsöverträdelse avseende personlig kreditinformation inträffar måste åtgärder vidtas för att minimera eventuell skada och de berörda personerna måste utan dröjsmål underrättas (artikel 39-4.1–39-4.2 i lagen om användning och skydd av kreditinformation). Dessutom måste nämnden för skydd av personuppgifter informeras om den underrättelse som lämnats till enskilda personer och de åtgärder som har genomförts (artikel 39-4.4 i lagen om användning och skydd av kreditinformation).

([131]) I så fall måste ett domstolsbeslut begäras utan dröjsmål. Om domstolsbeslutet inte utfärdas inom 36 timmar måste de mottagna uppgifterna raderas utan dröjsmål (artikel 32.6 led 6 i lagen om användning och skydd av kreditinformation).

([132]) T.ex. om en av parterna har utövat sin rätt till uppsägning på grund av att avtalsförpliktelser har fullgjorts osv., se artikel 17-2.5 i genomförandedekretet till lagen om användning och skydd av kreditinformation.

([133]) Artikel 20-2.1 i lagen om användning och skydd av kreditinformation och artikel 17-2.1 led 1 i genomförandedekretet till lagen om användning och skydd av kreditinformation.

([134]) Med denna tidsperiod tas hänsyn till att det ofta inte kommer att vara möjligt att utföra radering omedelbart eftersom det vanligtvis krävs vissa steg (t.ex. att uppgifterna som ska raderas skiljs från andra uppgifter och att raderingen utförs utan att informationssystemets stabilitet påverkas) som tar tid att genomföra.

([135]) Artikel 2-2.2 i lagen om användning och skydd av kreditinformation.

([136]) I artikel 18.2 i lagen om användning och skydd av kreditinformation och artikel 15.4 i genomförandedekretet till lagen om användning och skydd av kreditinformation fastställs mer specifika regler för denna dokumentationsplikt, t.ex. för uppgifter som kan missgynna en enskild person, exempelvis information om brottslighet och konkurs.

([137]) När det gäller andra mekanismer för ansvarsskyldighet krävs enligt lagen om användning och skydd av kreditinformation att vissa organisationer (t.ex. kooperativ och offentliga företag, se artikel 21.2 i genomförandedekretet till lagen om användning och skydd av kreditinformation) utser en ”förvaltare/bevakare av kreditinformation” som ansvarar för att övervaka efterlevnaden av lagen om användning och skydd av kreditinformation och utför den dataskyddsansvariges uppgifter enligt PIPA (artikel 20.3 och 20.4 i lagen om användning och skydd av kreditinformation).

(108) I lagen om användning och skydd av kreditinformation finns även särskilda insynskrav när det gäller att erhålla samtycke för användning eller tillhandahållande av personlig kreditinformation (artikel 32.4 och artikel 34-2 i lagen om användning och skydd av kreditinformation och artikel 30-3 i genomförandedekretet till lagen om användning och skydd av kreditinformation) och, mer allmänt, innan uppgifter lämnas till en tredje part (artikel 32.7 i lagen om användning och skydd av kreditinformation) ([138]). Dessutom har enskilda personer rätt att på begäran få information om användning och tillhandahållande av deras kreditinformation till tredje parter under de tre år som föregår begäran (inklusive ändamålet med och datumen för sådan användning eller sådant tillhandahållande) ([139]).

(109) Enligt lagen om användning och skydd av kreditinformation har enskilda personer också rätt att få tillgång till sin personliga kreditinformation (artikel 38.1 i lagen om användning och skydd av kreditinformation) och att få felaktiga uppgifter rättade (artikel 38.2–38.3 i lagen om användning och skydd av kreditinformation) ([140]). Utöver den allmänna rätten till radering enligt PIPA (se skäl 77) föreskrivs i lagen om användning och skydd av kreditinformation dessutom en särskild rätt till radering av personlig kreditinformation som har bevarats utöver de lagringsperioder som anges i skäl 104, dvs. fem år (för personlig kreditinformation som krävdes för att upprätta eller upprätthålla ett affärsförhållande) eller tre månader (för andra typer av personlig kreditinformation) ([141]). En begäran om radering kan undantagsvis avslås om ytterligare lagring är nödvändig på grund av de omständigheter som beskrivs i skäl 105. Om en enskild person begär radering, men ett av undantagen är tillämpligt, måste särskilda skyddsåtgärder tillämpas på den berörda kreditinformationen (artikel 38-3.3 i lagen om användning och skydd av kreditinformation och artikel 33-3 i genomförandedekretet till lagen om användning och skydd av kreditinformation). T.ex. måste uppgifterna hållas åtskilda från andra uppgifter, endast vara tillgängliga för behöriga och vara föremål för särskilda säkerhetsåtgärder.

(110) Utöver de rättigheter som nämns i skäl 109 garanteras genom lagen om användning och skydd av kreditinformation enskilda personers rätt att begära att en personuppgiftsansvarig inte ska kontakta dem för direkt marknadsföring (artikel 37.2 i lagen) och rätten till dataportabilitet. När det gäller den senare har enskilda personer enligt lagen om användning och skydd av kreditinformation rätt att begära att deras personliga kreditinformation överförs till dem själva eller till vissa tredje parter (t.ex. finansinstitut och kreditvärderingsföretag). Den personliga kreditinformationen måste behandlas och överföras till tredje part i ett format som kan behandlas av ett system för databehandling (t.ex. en dator).

(111) I den mån lagen om användning och skydd av kreditinformation innehåller särskilda regler jämfört med PIPA anser kommissionen därför att även dessa bestämmelser säkerställer en skyddsnivå som i huvudsak motsvarar den som ges enligt förordning (EU) 2016/679.

2.4 **Tillsyn och efterlevnad**

(112) För att säkerställa att en adekvat dataskyddsnivå garanteras i praktiken bör det finnas en oberoende tillsynsmyndighet med befogenhet att övervaka och verkställa efterlevnaden av dataskyddsbestämmelserna. Denna myndighet bör agera helt oavhängigt och opartiskt vid fullgörandet av sina skyldigheter och utövandet av sina befogenheter.

2.4.1 *Oberoende tillsyn*

(113) I Sydkorea är nämnden för skydd av personuppgifter den oberoende myndighet som övervakar och säkerställer att PIPA genomförs. Nämnden för skydd av personuppgifter består av en ordförande, en vice ordförande och sju ledamöter. Ordföranden och vice ordföranden utnämns av presidenten på rekommendation av premiärministern. Två av ledamöterna utnämns av presidenten på rekommendation av ordföranden och fem på rekommendation av parlamentet (av dessa utnämns två på rekommendation av det politiska parti som presidenten tillhör och tre på

([138]) Detta inbegriper ett allmänt krav på underrättelse (artikel 32.7 i lagen om användning och skydd av kreditinformation) och en särskild skyldighet avseende öppenhet när uppgifter som gör det möjligt att fastställa en persons kreditvärdighet tillhandahålls vissa enheter, såsom kreditvärderingsinstitut och företag som samlar in kreditinformation (artikel 35-3 i lagen om användning och skydd av kreditinformation och artikel 30-3 i genomförandedekretet till lagen om användning och skydd av kreditinformation), eller om ett affärsförhållande vägras eller avslutas på grundval av personlig kreditinformation som erhållits från en tredje part (artikel 36 i lagen om användning och skydd av kreditinformation och artikel 31 i genomförandedekretet till lagen om användning och skydd av kreditinformation).

([139]) Artikel 35 i lagen om användning och skydd av kreditinformation. Vissa kommersiella organisationer, t.ex. kooperativ och offentliga företag (artikel 21.2 i genomförandedekretet till lagen om användning och skydd av kreditinformation) omfattas av ytterligare krav på öppenhet, t.ex. offentliggörande av vissa uppgifter (artikel 31 i lagen om användning och skydd av kreditinformation) och information till enskilda personer om eventuell negativ påverkan på deras kreditbetyg när de deltar i finansiella transaktioner som medför kreditrisker (artikel 35-2 i lagen om användning och skydd av kreditinformation).

([140]) När det gäller villkoren och undantagen från rätten till tillgång och rättelse gäller reglerna i PIPA (som beskrivs i skälen 76–77). Dessutom fastställs närmare bestämmelser i artikel 38.4–38.8 i lagen om användning och skydd av kreditinformation och artikel 33 i genomförandedekretet till lagen om användning och skydd av kreditinformation. I synnerhet måste en kommersiell operatör som har rättat eller raderat felaktig kreditinformation underrätta den enskilda personen om detta. Dessutom ska varje tredje part till vilken uppgifterna lämnats under de föregående sex månaderna underrättas, och den berörda personen ska informeras om detta. Om en person inte är nöjd med hur en begäran om rättelse behandlats, kan han eller hon lämna in en begäran till nämnden för skydd av personuppgifter, som kontrollerar den personuppgiftsansvariges åtgärder och kan vidta korrigerande åtgärder.

([141]) Artikel 38-3 i lagen om användning och skydd av kreditinformation.

rekommendation av andra politiska partier (artikel 7-2.2 i PIPA), vilket motverkar partiskhet i utnämningsförfarandet) ([142]). Detta förfarande är i linje med de krav som tillämpas vid utnämning av ledamöter i dataskyddsmyndigheter i unionen (artikel 53.1 i förordning (EU) 2016/679). Dessutom måste ledamöter avstå från all vinstrelaterad verksamhet, politisk aktivitet och från att inneha positioner i den offentliga förvaltningen eller parlamentet (artiklarna 7-6 och 7-7.1 led 3 i PIPA) ([143]). Ledamöterna är också föremål för interna regler som förhindrar dem att delta i överläggningar vid eventuell intressekonflikt (artikel 7-11 i PIPA). Nämnden för skydd av personuppgifter biträds av ett sekretariat (artikel 7-13) och får inrätta underutskott (bestående av tre ledamöter) för att hantera mindre överträdelser och återkommande ärenden (artikel 7-12 i PIPA).

(114) Varje medlem i nämnden för skydd av personuppgifter utses för tre år och får återväljas en gång (artikel 7-4.1 i PIPA). Ledamöterna får endast avsättas under särskilda omständigheter, nämligen om de inte längre kan utföra sina uppgifter på grund av långvarig psykisk eller fysisk sjukdom, agerar i strid med lagen eller uppfyller någon av grunderna för att skiljas från sitt uppdrag ([144]) (artikel 7-5 i PIPA). Detta ger dem ett institutionellt skydd när de utövar sina uppdrag.

(115) Mer allmänt garanteras oberoendet inom nämnden för skydd av personuppgifter uttryckligen i artikel 7.1 i PIPA, och enligt artikel 7-5.2 i PIPA ska ledamöterna utföra sina uppgifter på ett oberoende sätt i enlighet med lagen och sitt samvete ([145]). De institutionella och förfarandemässiga skyddsåtgärder som beskrivs, även när det gäller utnämning och avsättning av dess ledamöter, säkerställer att nämnden för skydd av personuppgifter agerar fullständigt oberoende och utan yttre inflytande eller anvisningar. I egenskap av centralt förvaltningsorgan lägger nämnden för skydd av personuppgifter årligen fram ett förslag till egen budget (som granskas av finansministeriet som en del av den övergripande nationella budgeten innan den antas av parlamentet) och ansvarar för sin egen personalledning. För närvarande har nämnden en budget på omkring 35 miljoner euro och 154 anställda (däribland 40 specialister på informations- och kommunikationsteknik, 32 medarbetare med inriktning på utredningar och 40 juridiskt sakkunniga).

(116) Uppgifterna och befogenheterna för nämnden för skydd av personuppgifter anges huvudsakligen i artiklarna 7-8 och 7-9 samt i artiklarna 61–66 i PIPA ([146]). Framför allt omfattar nämndens arbetsuppgifter rådgivning om lagar och andra författningar om dataskydd, utveckling av strategier och riktlinjer för dataskydd, utredning av överträdelser av enskildas rättigheter, hantering av klagomål och medling av tvister, säkerställande av efterlevnad av PIPA, säkerställande av utbildning på och främjande av dataskyddsområdet samt utbyte och samarbete med dataskyddsmyndigheter i tredjeländer ([147]).

(117) På grundval av artikel 68 i PIPA jämförd med artikel 62 i genomförandedekretet till PIPA har vissa av uppgifterna för nämnden för skydd av personuppgifter delegerats till Sydkoreas byrå för internet och säkerhet, nämligen följande: 1) utbildning och pr-verksamhet, 2) utbildning av specialister och utarbetande av kriterier för konsekvensbedömningar av inverkan på integritetsskyddet, 3) handläggning av förfrågningar om att utse en så kallad institution för konsekvensbedömning av inverkan på integritetsskyddet, 4) hantering av förfrågningar

([142]) Endast personer som uppfyller följande kriterier får utses till ledamöter av nämnden för skydd av personuppgifter: högre offentliganställda tjänstemän med ansvar för personuppgiftsfrågor, före detta domare, allmänna åklagare eller advokater som har utövat yrket i minst tio år, tidigare chefer med erfarenhet av dataskydd som har tjänstgjort vid en offentlig institution eller organisation i mer än tre år, eller som har rekommenderats av en sådan institution eller organisation, Samt tidigare lektorer med yrkeskunskaper på området dataskydd som under minst fem år tjänstgjort vid en akademisk institution (artikel 7-2 i PIPA).

([143]) Se även artikel 4-2 i genomförandedekretet till PIPA.

([144]) Se artikel 7-7 i PIPA, enligt vilken icke-sydkoreanska medborgare och medlemmar i politiska partier inte får bli ledamöter i nämnden för skydd av personuppgifter. Detsamma gäller för personer som har varit föremål för vissa typer av straffrättsliga påföljder, som har avlägsnats från sin tjänst genom disciplinära åtgärder under de senaste fem åren osv. (artikel 7-7 i PIPA jämförd med artikel 33 i lagen om offentliga tjänstemän).

([145]) Även om det i artikel 7.2 i PIPA hänvisas till premiärministerns allmänna befogenhet att enligt artikel 18 i lagen om regeringens organisation upphäva eller återkalla ett olagligt eller omotiverat beslut från ett centralt förvaltningsorgan (med presidentens godkännande) beviljas ingen sådan befogenhet med avseende på utredande eller verkställande befogenheter som nämnden för skydd av personuppgifter har (se artikel 7.2 led 1 och 2 i PIPA). Enligt förklaringar som mottagits från den sydkoreanska regeringen är syftet med artikel 18 i lagen om regeringens organisation att ge premiärministern möjlighet att agera under exceptionella omständigheter, t.ex. för att medla i en tvist mellan olika statliga organ. Premiärministern har dock aldrig utnyttjat denna befogenhet sedan bestämmelsen antogs 1963.

([146]) När det är nödvändigt för att utföra de uppgifter som avses i artikel 7-9.1 i PIPA får nämnden för skydd av personuppgifter inhämta yttranden från berörda offentliga tjänstemän, experter på dataskydd, medborgarorganisationer och berörda näringsidkare. Dessutom kan nämnden för skydd av personuppgifter begära relevant material, utfärda rekommendationer om förbättringar och kontrollera om dessa genomförs (artikel 7-9.2–7-9.5 i PIPA).

([147]) Se även artikel 9 i PIPA (den treåriga huvudplanen för skydd av personuppgifter) artikel 12 i PIPA (standardriktlinjer för skydd av personuppgifter), artikel 13 i PIPA (riktlinjer för främjande och stöd av självreglering).

om indirekt tillgång till personuppgifter som innehas av myndigheter (artikel 35.2 i PIPA) och 5) uppgiften att begära in material och genomföra inspektioner avseende klagomål som mottagits via den så kallade integritetstjänsten. I samband med hanteringen av klagomål via integritetstjänsten vidarebefordrar Sydkoreas byrå för internet och säkerhet ärendet till nämnden för skydd av personuppgifter eller till åklagaren om den finner att en lagöverträdelse har ägt rum. Möjligheten att lämna in ett klagomål till integritetstjänsten hindrar inte enskilda personer från att direkt lämna in ett klagomål till nämnden för skydd av personuppgifter eller att vända sig till nämnden för skydd av personuppgifter om de anser att deras klagomål inte hanterades på ett tillfredsställande sätt av Sydkoreas byrå för internet och säkerhet.

2.4.2 *Verkställighet, inbegripet påföljder*

(118) För att säkerställa överensstämmelse med PIPA har lagstiftaren beviljat nämnden både utredande och verkställande befogenheter som sträcker sig från rekommendationer till administrativa sanktionsavgifter. Dessa befogenheter kompletteras dessutom av ett system med straffrättsliga påföljder.

(119) När det gäller utredande befogenheter får nämnden för skydd av personuppgifter, vid misstänkt eller anmäld överträdelse av PIPA eller om det är nödvändigt för att skydda den registrerades rättigheter mot överträdelser, utföra kontroller på plats och begära allt relevant material (t.ex. artiklar och handlingar) från personuppgiftsansvariga (artikel 63 i PIPA jämförd med artikel 60 i genomförandedekretet till PIPA) ([148]).

(120) När det gäller verkställighet får nämnden för skydd av personuppgifter enligt artikel 61.2 i PIPA ge råd till personuppgiftsansvariga om hur man kan förbättra nivån på skyddet av personuppgifter vid specifik behandling. Personuppgiftsansvariga måste göra ärliga ansträngningar för att genomföra sådana råd och är skyldiga att informera nämnden för skydd av personuppgifter om resultatet. Om det finns rimliga skäl att anta att en överträdelse av PIPA har inträffat och om underlåtenhet att vidta åtgärder sannolikt kommer att orsaka skada som är svår att avhjälpa, kan nämnden för skydd av personuppgifter dessutom vidta korrigerande åtgärder (artikel 64.1 i PIPA) ([149]). I avsnitt 5 i meddelande 2021-5 (bilaga I) klargörs med bindande verkan att dessa villkor är uppfyllda när det gäller överträdelser av bestämmelser i PIPA som skyddar enskilda personers rätt till integritet med avseende på personuppgifter ([150]). De åtgärder som nämnden för skydd av personuppgifter har befogenhet att vidta omfattar att beordra att det beteende som orsakat överträdelsen ska upphöra, att behandlingen av uppgifterna ska upphöra, eller andra nödvändiga åtgärder. Underlåtenhet att följa en korrigerande åtgärd kan leda till en påföljd där ett bötesbelopp på upp till 50 miljoner won åläggs (artikel 75.2 led 13 i PIPA).

(121) När det gäller vissa myndigheter (t.ex. parlamentet, centrala förvaltningsorgan, lokala organ och domstolarna) föreskrivs i artikel 64.4 i PIPA att nämnden för skydd av personuppgifter får ”rekommendera” någon av de korrigerande åtgärder som nämns i skäl 120 och att dessa myndigheter är skyldiga att följa en sådan rekommendation såvida inte extraordinära omständigheter föreligger. Enligt avsnitt 5 i meddelande 2021-5 avser detta extraordinära faktiska eller rättsliga omständigheter som nämnden för skydd av personuppgifter inte kände till när den lämnade sin rekommendation. Den berörda myndigheten får endast åberopa sådana extraordinära omständigheter om den tydligt visar att ingen överträdelse har ägt rum och nämnden för skydd av personuppgifter fastställer att så inte är fallet. I annat fall måste myndigheten följa nämndens rekommendation och ”vidta en korrigerande åtgärd, bl.a. att omedelbart avbryta åtgärden, och kompensera för skador i sådana undantagsfall där en olaglig handling ändå begåtts”.

(122) Nämnden får även begära att andra förvaltningsorgan med särskild kompetens enligt sektorslagstiftning (t.ex. hälsa, utbildning) genomför undersökningar – på egen hand eller tillsammans med nämnden – avseende (misstänkta) överträdelser av integritetsskyddet som begåtts av personuppgiftsansvariga inom de sektorer som ingår i organens behörighetsområde, samt att de vidtar korrigerande åtgärder (artikel 63.4–63.5 i PIPA). I dessa fall fastställer nämnden för skydd av personuppgifter skälen till undersökningen samt dess syfte och tillämpningsområde ([151]). Det berörda förvaltningsorganet måste i sin tur lämna in en plan för kontrollen till nämnden för skydd av personuppgifter och underrätta nämnden om dess resultat. Nämnden för skydd av personuppgifter kan rekommendera att en särskild korrigerande åtgärd vidtas, som den berörda myndigheten ska sträva efter att genomföra. Under alla omständigheter begränsar en sådan begäran inte den behörighet som nämnden för skydd av personuppgifter har att genomföra en egen undersökning eller ålägga påföljder.

([148]) Nämnden för skydd av personuppgifter har dessutom rätt till tillträde till den personuppgiftsansvariges lokaler för att kontrollera tillståndet hos affärsverksamheten, register, dokument osv. (artikel 63.2 i PIPA). Se även artikel 45-3 i lagen om användning och skydd av kreditinformation och artikel 36-4 i genomförandedekretet till lagen om användning och skydd av kreditinformation med avseende på befogenheterna för nämnden för skydd av personuppgifter enligt den lagen.

([149]) Se även artikel 45-4 i lagen om användning och skydd av kreditinformation med avseende på befogenheterna för nämnden för skydd av personuppgifter enligt den lagen.

([150]) I avsnitt 5 i meddelandet anges att ”betydande skäl att anse att en överträdelse med avseende på personuppgifter har ägt rum och att underlåtenhet att vidta åtgärder sannolikt kan orsaka skada som är svår att avhjälpa i den mening som avses i artikel 64.1 och 64.2 i PIPA avser en överträdelse av någon av de principer, rättigheter och skyldigheter som ingår i lagen för att skydda individers rätt till personuppgifter”. Detsamma gäller för befogenheterna för nämnden för skydd av personuppgifter enligt artikel 45-4 i lagen om användning och skydd av kreditinformation.

([151]) Artikel 60 i genomförandedekretet till PIPA.

(123) Utöver sina korrigerande befogenheter får nämnden ålägga administrativa sanktionsavgifter på mellan 10 och 50 miljoner won för överträdelser av olika krav i PIPA (artikel 75 i PIPA) ([152]). Detta inbegriper bl.a. bristande efterlevnad av kraven avseende laglighet i behandlingen, underlåtenhet att vidta nödvändiga säkerhetsåtgärder, underlåtenhet att underrätta registrerade i händelse av en uppgiftsincident, underlåtenhet att uppfylla kraven för underentreprenad, underlåtenhet att upprätta och offentliggöra en integritetspolicy, underlåtenhet att utse en dataskyddsansvarig eller underlåtenhet att agera på begäran av en registrerad som utövar sina individuella rättigheter samt vissa förfarandemässiga överträdelser (bristande samarbetsvilja vid en undersökning). Om samma personuppgiftsansvarig begår överträdelser mot flera bestämmelser i PIPA kan böter utfärdas för varje överträdelse, och antalet enskilda personer som påverkas kommer att beaktas när bötesnivån fastställs.

(124) Om det finns rimliga skäl för misstanke om överträdelse av PIPA eller andra ”lagar kopplade till dataskydd” får nämnden för skydd av personuppgifter dessutom inge en brottsanmälan till det behöriga utredningsorganet (t.ex. en åklagare, se artikel 65.1 i PIPA). Dessutom kan nämnden för skydd av personuppgifter råda den personuppgiftsansvarige att vidta disciplinära åtgärder mot den ansvariga personen (däribland ansvarig chef, se artikel 65.2 i PIPA). Efter att ha tagit emot ett sådant råd måste personuppgiftsansvariga följa det ([153]) och skriftligen underrätta nämnden för skydd av personuppgifter om resultatet (artikel 65 i PIPA jämförd med artikel 58 i genomförandedekretet till PIPA).

(125) När det gäller råd i enlighet med artikel 61, korrigerande åtgärder i enlighet med artikel 64, anklagelser eller råd avseende disciplinära åtgärder i enlighet med artikel 65 och åläggande av administrativa sanktionsavgifter i enlighet med artikel 75 i PIPA får nämnden för skydd av personuppgifter offentliggöra fakta (dvs. överträdelsen, den enhet som har överträtt lagen och införd åtgärd eller åtgärder) genom att lägga ut dem på sin webbplats eller i en allmän, landsomfattande dagstidning (artikel 66 i PIPA jämförd med artikel 61.1 i genomförandedekretet till PIPA) ([154]).

(126) Slutligen stöds efterlevnaden av kraven avseende dataskydd i PIPA (liksom andra ”lagar kopplade till dataskydd”) av ett system med straffrättsliga påföljder. I detta avseende innehåller artiklarna 70–73 i PIPA bestämmelser om påföljder som kan leda till antingen böter (mellan 20 och 100 miljoner won) eller fängelse (där den högsta påföljden är 2–10 år). Relevanta överträdelser omfattar bl.a. användning av personuppgifter eller tillhandahållande av sådana uppgifter till en tredje part utan nödvändigt samtycke, behandling av känsliga uppgifter i strid mot förbudet i artikel 23.1 i PIPA, bristande efterlevnad av tillämpliga säkerhetskrav som leder till att personuppgifterna går förlorade, stjäls, sprids, förfalskas, ändras eller skadas, underlåtenhet att vidta nödvändiga åtgärder för att rätta, radera eller upphöra med behandlingen av personuppgifter eller olaglig överföring av personuppgifter till ett tredjeland ([155]). Enligt artikel 74 i PIPA ska i vart och ett av dessa fall den personuppgiftsansvariges anställda, ombud eller representant liksom den personuppgiftsansvarige själv vara ansvariga ([156]).

(127) Utöver de straffrättsliga påföljder som föreskrivs i PIPA kan missbruk av personuppgifter också utgöra ett brott enligt strafflagen. Detta gäller särskilt överträdelser av sekretess för brev, handlingar eller elektroniska handlingar (artikel 316), utlämnande av uppgifter som omfattas av tystnadsplikt (artikel 317), bedrägeri genom användning av datorer (artikel 347-2) samt förskingring och trolöshet mot huvudman (artikel 355).

(128) Det sydkoreanska systemet kombinerar därför olika typer av sanktioner, från korrigerande åtgärder och administrativa sanktionsavgifter till straffrättsliga påföljder, som sannolikt har en särskilt stark avskräckande effekt på personuppgiftsansvariga och de personer som hanterar uppgifterna. Nämnden för skydd av personuppgifter

([152]) Dessutom kan nämnden för skydd av personuppgifter återkalla certifieringen i fall där system för behandling och skydd av personuppgifter som drivs av en personuppgiftsansvarig har certifierats som förenliga med PIPA, men faktiskt inte uppfyllt certifieringskriterierna enligt artikel 34-2.1 i genomförandedekretet till PIPA, eller om det föreligger en allvarlig överträdelse av en ”lag kopplad till skydd av [person]uppgifter” (artikel 32-2.3, 32-2.5 i PIPA). Nämnden för skydd av personuppgifter ska underrätta den personuppgiftsansvarige om ett sådant återkallande och ska offentligt tillkännage det, eller offentliggöra det på sin webbplats eller i det officiella kungörelseorganet (artikel 34-4 i genomförandedekretet till PIPA). Administrativa sanktionsavgifter (artikel 52 i lagen om användning och skydd av kreditinformation) och straffrättsliga påföljder (artikel 50 i lagen om användning och skydd av kreditinformation) anges också för överträdelser av lagen om användning och skydd av kreditinformation.

([153]) Enligt artikel 58.2 i genomförandedekretet till PIPA ska den personuppgiftsansvarige inkomma med en motiverad förklaring till nämnden för skydd av personuppgifter om särskilda omständigheter gör att det inte är ”praktiskt möjligt” att följa rådet.

([154]) Vid beslut om ett sådant offentliggörande ska nämnden för skydd av personuppgifter beakta överträdelsens innehåll och allvar, dess längd och frekvens samt dess konsekvenser (skadans omfattning). Den berörda enheten ska underrättas i förväg och ges möjlighet att försvara sig. Se artikel 61.2, 61.3 i genomförandedekretet till PIPA.

([155]) Se artikel 71 led 2 jämförd med artikel 18.1 i PIPA (underlåtenhet att uppfylla villkoren i artikel 17.3 i PIPA, som avses i artikel 18.1). Se även artikel 75.2 led 1 jämförd med artikel 17.2 i PIPA (underlåtenhet att tillhandahålla nödvändiga uppgifter till den berörda personen enligt artikel 17.2 i PIPA, som avses i artikel 17.3).

([156]) Dessutom möjliggör artikel 74-2 i PIPA förverkande av alla pengar, varor eller andra vinster som erhållits till följd av överträdelsen, eller – om förverkande är omöjligt – uppbörd av den förmån som erhållits på olagligt sätt.

började använda sina befogenheter omedelbart efter inrättandet 2020. Det framgår av nämndens årsrapport för 2021 att den redan har utfärdat ett antal rekommendationer, administrativa sanktionsavgifter och korrigerande åtgärder, både gentemot den offentliga sektorn (omkring 34 myndigheter) och privata aktörer (omkring 140 företag) ([157]). Bland uppmärksammade fall må nämnas ett företag som hade brutit mot olika bestämmelser i PIPA (bl.a. säkerhetskrav, krav på samtycke för utlämnande till tredje part och öppenhet) som i december 2020 ålades böter på 6,7 miljarder won ([158]) samt ett företag inom AI-teknik (som bl.a. gjort sig skyldigt till överträdelse av bestämmelserna om laglig behandling, särskilt samtycke och behandling av pseudonymiserad information) som i april 2021 ålades böter på 103,3 miljoner won ([159]). I augusti 2021 slutförde nämnden för skydd av personuppgifter ytterligare en undersökning av verksamheten vid tre företag, vilket ledde till korrigerande åtgärder och åläggande av bötesbelopp på upp till 6,47 miljarder won (bl.a. för att ha underlåtit att underrätta enskilda personer om utlämnande av personuppgifter till tredje part, däribland överföringar till tredje land) ([160]). Redan före den nyligen genomförda reformen visade Sydkorea goda resultat när det gäller verkställighet och de ansvariga myndigheterna använde sig av hela skalan av verkställighetsåtgärder, inklusive administrativa sanktionsavgifter, korrigerande åtgärder och ”namnuppgift och delning” när det gäller en rad olika personuppgiftsansvariga, däribland leverantörer av kommunikationstjänster (Sydkoreas kommunikationskommitté), samt kommersiella operatörer, finansinstitut, myndigheter, universitet och sjukhus (ministeriet för inrikesfrågor och säkerhet) ([161]). På grundval av detta drar kommissionen slutsatsen att det sydkoreanska systemet säkerställer en effektiv tillämpning av dataskyddsreglerna i praktiken, vilket garanterar en skyddsnivå som i huvudsak motsvarar den som fastställs i förordning (EU) 2016/679.

2.5 **Prövningsmöjligheter**

(129) För att säkerställa adekvat skydd, och i synnerhet tillämpningen av enskildas rättigheter, bör den registrerade erbjudas möjligheten till faktisk administrativ och rättslig prövning, däribland ersättning för skador.

(130) Det sydkoreanska systemet tillhandahåller enskilda personer olika mekanismer för att effektivt hävda sina rättigheter och erhålla (rättslig) prövning.

(131) Som ett första steg kan enskilda personer som anser att deras rättigheter eller intressen i fråga om dataskydd har kränkts vända sig till berörd personuppgiftsansvarig. Enligt artikel 30.1 led 5 i PIPA ska den personuppgiftsansvariges integritetspolicy bl.a. innehålla information om de registrerades rättigheter och hur de ska utövas. Den ska dessutom tillhandahålla kontaktuppgifter (t.ex. namn och telefonnummer till dataskyddsansvarig eller dataskyddsavdelningen) för att möjliggöra inlämning av klagomål. Inom ramen för den personuppgiftsansvariges organisation har den personuppgiftsansvarige i uppdrag att handlägga klagomål, vidta korrigerande åtgärder om integritetsskyddet överträds och hantera kompensation (artikel 31.2 led 3, 31.4 i PIPA). Det senare är relevant t.ex. vid en uppgiftsincident eftersom den personuppgiftsansvarige bl.a. måste informera den registrerade om en kontaktpunkt dit skador kan rapporteras (artikel 34.1 led 5 i PIPA).

(132) Dessutom erbjuds genom PIPA flera möjligheter till tvistlösning mellan enskilda personer och personuppgiftsansvariga. För det första får alla som anser att den personuppgiftsansvarige har kränkt deras rättigheter eller intressen avseende dataskydd anmäla sådana överträdelser direkt till nämnden för skydd av personuppgifter och/eller en av de specialiserade institutioner som utsetts av nämnden för att ta emot och hantera klagomål. Detta inbegriper Sydkoreas byrå för internet och säkerhet, som för detta ändamål driver en teletjänstcentral för personuppgifter (den så kallade *integritetstjänsten*) (artikel 62.1 och 62.2 i PIPA jämförd med artikel 59 i genomförandedekretet till PIPA). Integritetstjänsten undersöker och fastställer överträdelser, tillhandahåller rådgivning avseende behandling av personuppgifter (artikel 62.3 i PIPA) och får rapportera överträdelser till nämnden för

([157]) Se årsrapporten för 2021 för nämnden för skydd av personuppgifter, s. 50–55 (endast tillgänglig på koreanska) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Se (endast tillgänglig på koreanska) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Se (endast tillgänglig på koreanska) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Se (endast tillgänglig på koreanska) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Se t.ex. årsrapporten för 2020 (endast tillgänglig på koreanska) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 och exemplen på engelska som finns på https://www.privacy.go.kr/eng/enforcement_02.do.

skydd av personuppgifter (men kan inte själv vidta efterlevnadsåtgärder). Integritetstjänsten tar emot ett stort antal klagomål/begäranden (t.ex. 177 457 år 2020, 159 255 år 2019 och 164 497 år 2018) ([162]). Enligt information från nämnden för skydd av personuppgifter tog nämnden själv emot omkring 1 000 klagomål mellan augusti 2020 och augusti 2021. Som svar på ett klagomål får nämnden för skydd av personuppgifter utfärda en rekommendation om förbättringar, korrigerande åtgärder, en ”anklagelse” till det behöriga utredningsorganet (däribland en åklagare) eller råd om disciplinära åtgärder (se artiklarna 61, 64 och 65 i PIPA). Nämndens beslut (t.ex. en vägran att behandla ett klagomål eller ett avslag på ett klagomål i sak) kan bestridas enligt förvaltningsprocesslagen (*Administrative Litigation Act*) ([163]).

(133) För det andra kan de registrerade enligt artiklarna 40–50 i PIPA jämförda med artiklarna 48-14–57 i genomförandedekretet till PIPA begära en så kallad ”kommitté för tvistlösning”, bestående av företrädare som utsetts av ordföranden för nämnden för skydd av personuppgifter bland ledamöterna i nämndens styrelse och personer som utsetts bland vissa andra kvalificerade grupper på grundval av erfarenhet av dataskydd (se artikel 40.2, 40.3 och 40.7 i PIPA, artikel 48-14 i genomförandedekretet till PIPA) ([164]). Möjligheten att använda sig av medling inför kommittén för tvistlösning tillhandahåller ett alternativt tillvägagångssätt för att erhålla prövning, men begränsar inte den enskildes rätt att i stället vända sig till nämnden för skydd av personuppgifter eller domstolarna. För att pröva ärendet får kommittén begära att parterna i tvisten tillhandahåller nödvändigt material och/eller kalla berörda vittnen att inställa sig inför kommittén (artikel 45 i PIPA). När frågan har klargjorts förbereder kommittén ett utslag i form av ett medlingsförslag ([165]) som en majoritet av ledamöterna måste enas om. Medlingsförslag kan innefatta upphörande av överträdelsen, nödvändiga rättsmedel (däribland restitution eller ersättning) samt åtgärder som krävs för att förhindra att samma överträdelser eller liknande upprepas (artikel 47.1 i PIPA). Om båda parterna samtycker till medlingsutslaget får det samma verkan som en förlikning i domstol (artikel 47.5 i PIPA). Ingen av parterna hindras från att väcka talan vid domstol medan medlingen pågår, och om så sker kommer den senare att vilandeförklaras (se artikel 48.2 i PIPA) ([166]). Årliga uppgifter som publiceras av nämnden för skydd av personuppgifter visar att enskilda regelbundet utnyttjar medlingsförfarandet inför kommittén för tvistlösning, vilket ofta leder till ett framgångsrikt resultat. År 2020 behandlade kommittén t.ex. 126 fall varav 89 kunde lösas inför kommittén (i 77 fall hade parterna redan nått en överenskommelse innan medlingsprocessen avslutades och i 12 fall godtog parterna medlingsförslaget), vilket innebar en förlikningsgrad på 70,6 % ([167]). År 2019 behandlade kommittén 139 fall varav 92 kunde lösas, vilket innebar en förlikningsgrad på 62,2 %.

(134) Om minst 50 personer lider skada eller om deras dataskyddsrättigheter har kränkts på samma eller liknande sätt till följd av samma (typ av) incident ([168]), får dessutom en registrerad person eller en dataskyddsorganisation ansöka om kollektiv medling för en sådan gruppering. Andra registrerade kan ansöka om att ansluta sig till en sådan medling, som offentliggörs av kommittén för tvistlösning (artikel 49.1–49.3 i PIPA jämförd med artiklarna 52–54 i genomförandedekretet till PIPA) ([169]). Kommittén för tvistlösning får välja ut minst en person som bäst

([162]) Se årsrapporten för 2021 för nämnden för skydd av personuppgifter, s. 174. År 2020 handlade dessa klagomål t.ex. om insamling av uppgifter utan samtycke, underlåtenhet att iaktta krav avseende öppenhet, överträdelser av PIPA som begåtts av personuppgiftsbiträden, otillräckliga säkerhetsåtgärder, underlåtenhet att svara på begäranden från de registrerade samt allmänna förfrågningar.

([163]) I synnerhet får enskilda personer överklaga ett förvaltningsorgans utövande av eller vägran att utöva offentlig makt (artikel 2.1 led 1, artikel 3 led 1 i förvaltningsprocesslagen. Mer detaljerad information om förfarandemässiga aspekter, däribland villkoren för godkännande, finns i skäl 181.

([164]) Samtliga ledamöter har en fast mandatperiod och kan endast avsättas på skälig grund (se artiklarna 40.5 och 41 i PIPA). Dessutom innehåller artikel 42 i PIPA skyddsåtgärder mot intressekonflikter.

([165]) Se artikel 44 i PIPA. Dessutom kan den föreslå ett förslag till förlikning och rekommendera förlikning utan medling (se artikel 46 i PIPA).

([166]) Dessutom får kommittén avvisa medling om den anser det olämpligt att medla i tvisten på grund av dess art eller på grund av att ansökan om medling är oskälig (artikel 48 i PIPA).

([167]) Se årsrapporten för 2021 för nämnden för skydd av personuppgifter, s. 179–180. Dessa fall gällde bl.a. överträdelser av kravet att inhämta samtycke för insamling av uppgifter, principen om ändamålsbegränsning samt de registrerades rättigheter.

([168]) Se artikel 49.1 i PIPA enligt vilken de registrerade måste lida skada eller få sina rättigheter kränkta ”på ett identiskt eller liknande sätt”, och artikel 52 led 2 i genomförandedekretet till PIPA där det anges som villkor att ”[v]iktiga frågor angående incidenten är gemensamma, i sak eller rättsligt”.

([169]) Dessutom kan även icke-parter dra nytta av ett utslag vid kollektiv medling som godtas av den personuppgiftsansvarige, eftersom kommittén för tvistlösning kan råda den personuppgiftsansvarige att utarbeta och lämna in en kompensationsplan som (även) omfattar dem (artikel 49.5 i PIPA).

företräder det gemensamma intresset som representativ part (artikel 49.4 i PIPA). Om den personuppgiftsansvarige avvisar kollektiv medling eller inte godtar medlingsutslaget får vissa organisationer ([170]) ansöka om rättslig prövning genom grupptalan för att åtgärda överträdelsen (artiklarna 51–57 i PIPA).

(135) För det tredje har den registrerade rätt till lämplig prövning i ett ”snabbt och rättvist förfarande” om kränkningen av integriteten har medfört ”skada” för den enskilda personen (artikel 4 led 5 med artikel 39 i PIPA) ([171]). Den personuppgiftsansvarige kan avhända sig ansvar genom att bevisa avsaknad av uppsåt (”felaktig avsikt” eller vårdslöshet). Om den registrerade lider skada till följd av förlust, stöld, spridning, förfalskning, ändring eller skada av/på hans eller hennes personuppgifter, får domstolen besluta om ersättning upp till tre gånger den faktiska skadan, med beaktande av ett antal faktorer (artikel 39.3 och 39.4 i PIPA). Alternativt kan den registrerade begära en ”skälig” ersättning som inte överstiger 3 miljoner won (artikel 39-2.1 och 39-2.2 i PIPA). I enlighet med civillagen kan ersättning dessutom begäras från en person som ”orsakar förlust för en annan person eller vållar denne skada genom en olaglig handling, uppsåtligen eller av vårdslöshet” ([172]) eller från en person ”som vållar en annan person kroppsskada eller skadar dennes frihet eller ära, eller som har orsakat någon form av psykiskt lidande för en annan person” ([173]). Högsta domstolen har bekräftat att ett sådant skadeståndsansvar följer av överträdelser av dataskyddsregler ([174]). Om skadan har orsakats av en myndighets rättsstridiga agerande kan dessutom en begäran om ersättning lämnas in enligt lagen om statlig kompensation ([175]). Ett skadeståndsanspråk enligt lagen om statlig kompensation kan inges till ett specialiserat ”kompensationsråd” eller direkt till de sydkoreanska domstolarna ([176]). Statligt ansvar omfattar även icke-materiella skador (t.ex. psykiskt lidande) ([177]). Om offret är en utländsk medborgare tillämpas lagen om statlig kompensation under förutsättning att den medborgarens ursprungsland även säkerställer statlig kompensation för sydkoreanska medborgare ([178]).

(136) För det fjärde har högsta domstolen erkänt att enskilda personer har rätt att begära förbudsföreläggande för överträdelser av deras rättigheter enligt författningen, däribland rätten till skydd av personuppgifter ([179]). I detta sammanhang kan en domstol till exempel ålägga personuppgiftsansvariga att avbryta eller stoppa all olaglig verksamhet. Dataskyddsrättigheter kan dessutom upprätthållas genom civilrättsliga åtgärder, detta gäller även de rättigheter som skyddas genom PIPA. Högsta domstolen har erkänt denna horisontella tillämpning av det författningsmässiga integritetsskyddet på förhållanden mellan privata parter ([180]).

([170]) Det vill säga konsumentgrupper eller icke vinstdrivande icke-statliga organisationer av en viss storlek i fråga om medlemskap vars angivna syfte är dataskydd (dock när det gäller det sistnämnda med det ytterligare kravet att minst 100 registrerade personer som upplevt samma (typ av) överträdelse har ingett en begäran om rättslig prövning genom grupptalan). Se artikel 51 i PIPA.

([171]) I artiklarna 43–43-3 i lagen om användning och skydd av kreditinformation fastställs även skyldigheten att ersätta skador som orsakas av överträdelser av samma lag.

([172]) Artikel 750 i civillagen.

([173]) Artikel 751.1 i civillagen.

([174]) Se t.ex. högsta domstolens beslut nr 2015Da251539, 251546, 251553, 251560, 251577 av den 30 maj 2018. Dessutom bekräftade högsta domstolen att uppgiftsincidenter kan leda till skadestånd enligt civillagen, se högsta domstolens beslut nr 2011Da59834, 59858, 59841 av den 26 december 2012 (en engelsk sammanfattning finns på http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). I detta fall klargjorde högsta domstolen att för att bedöma huruvida känslomässigt lidande som drabbat en person kan anses utgöra en ersättningsbar skada bör flera faktorer beaktas, t.ex. typen av uppgifter som läckt ut och deras egenskaper, hur identifierbar den enskilde har blivit till följd av överträdelsen, tredje mans möjlighet att få tillgång till uppgifterna, i vilken utsträckning personuppgifterna spreds, huruvida detta ledde till ytterligare överträdelser av enskildas rättigheter, hur personuppgifterna hanterades och skyddades osv.

([175]) På grundval av lagen om statlig kompensation kan enskilda personer ansöka om ersättning för skador som offentliga tjänstemän åsamkar dem vid lagstridigt fullgörande av sina officiella arbetsuppgifter (artikel 2.1 i lagen).

([176]) Artiklarna 9 och 12 i lagen om statlig kompensation. Genom lagen inrättas distriktsråd (under ledning av vice åklagaren vid motsvarande åklagarmyndighet), ett centralråd (under ledning av vice justitieministern) och ett särskilt råd (under ledning av vice försvarsministern, ansvarigt för skador som orsakas av militär personal eller civilanställda inom militären). Skadeståndsanspråk hanteras i princip av distriktsrådet, som under vissa omständigheter måste vidarebefordra ärenden till det centrala eller särskilda rådet, t.ex. om skadeståndet överstiger ett visst belopp eller om en enskild person ansöker om ny granskning. Alla råd består av ledamöter som utses av justitieministern (t.ex. bland tjänstemän vid justitieministeriet, domstolar, advokater och personer med sakkunskap om statlig kompensation) och omfattas av särskilda regler om intressekonflikter (se artikel 7 i genomförandedekretet till lagen om statlig kompensation).

([177]) Se artikel 8 i lagen om statlig kompensation (som hänvisar till civillagen) och artikel 751 i civillagen.

([178]) Artikel 7 i lagen om statlig kompensation.

([179]) Högsta domstolens beslut nr 93Da40614 av den 12 april 1996 och beslut nr 2008Da42430 av den 2 september 2011 (en engelsk sammanfattning finns på https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord).

([180]) Se t.ex. högsta domstolens beslut nr 2008Da42430 av den 2 september 2011 (en engelsk sammanfattning finns på https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord).

(137) Slutligen kan enskilda personer inge en brottsanmälan i enlighet med straffprocesslagen (artikel 223) till en allmän åklagare eller en polistjänsteman inom kriminalpolisen ([181]).

(138) I det sydkoreanska systemet erbjuds sålunda olika möjligheter att erhålla prövning, från lättillgängliga och billiga alternativ (t.ex. genom att kontakta integritetstjänsten eller genom (kollektiv) medling) till administrativa (inför nämnden för skydd av personuppgifter) och rättsliga medel, vilket inbegriper möjligheten att erhålla ersättning för skador.

3. TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRS FRÅN EUROPEISKA UNIONEN AV MYNDIGHETER I SYDKOREA

(139) Kommissionen har också bedömt begränsningarna och skyddsåtgärderna, däribland den sydkoreanska lagstiftningens mekanismer för tillsyn och enskild prövning avseende Sydkoreanska myndigheters insamling och användning av personuppgifter som överförs till personuppgiftsansvariga i Sydkorea för att tillvarata allmänintresset, särskilt för straffrättsliga ändamål som rör brottsbekämpning och den nationella säkerheten (myndigheters tillgång till uppgifter). Den Sydkoreanska regeringen har försett kommissionen med officiella framställningar, utfästelser och åtaganden som undertecknats på högsta ministernivå och inom de högsta organen. Dessa ingår i bilaga II till detta beslut.

(140) Vid bedömningen av om villkoren för myndigheternas tillgång till uppgifter som överförs till Sydkorea enligt detta beslut uppfyller kriteriet om ”väsentlig likvärdighet” i enlighet med artikel 45.1 i förordning (EU) 2016/679 som den tolkats av Europeiska unionens domstol mot bakgrund av stadgan om de grundläggande rättigheterna, tog kommissionen särskilt hänsyn till följande kriterier.

(141) För det första ska varje begränsning av rätten till skydd av personuppgifter föreskrivas i lag och den rättsliga grund som möjliggör ett intrång i en sådan rättighet måste innehålla en definition av hur omfattande begränsningen är av utövandet av den berörda rättigheten ([182]).

(142) För det andra, för att uppfylla proportionalitetskravet, enligt vilket undantag från och begränsningar av skyddet av personuppgifter endast får tillämpas i den mån det är absolut nödvändigt i ett demokratiskt samhälle för att uppfylla särskilda mål av allmänintresse som motsvarar dem som erkänns av EU, ska det i lagstiftningen i det berörda tredjelandet, enligt vilken intrånget är tillåtet, fastställas klara och precisa regler för omfattningen och tillämpningen av åtgärderna i fråga och införas minimigarantier så att de personer vars uppgifter har överförts har tillräckliga garantier för att effektivt skydda sina personuppgifter mot risken för missbruk ([183]). Lagstiftningen måste särskilt ange under vilka omständigheter och på vilka villkor en åtgärd som föreskriver behandling av sådana uppgifter får antas ([184]) samt ställa krav på oberoende tillsyn för uppfyllandet av dessa krav ([185]).

(143) För det tredje måste denna lagstiftning och dess krav vara rättsligt bindande enligt nationell lagstiftning. Detta gäller först och främst myndigheterna i det berörda tredjelandet, men dessa rättsliga krav måste också vara verkställbara inför domstol mot dessa myndigheter ([186]). I synnerhet måste de registrerade ha möjlighet att väcka talan vid en oberoende och opartisk domstol för att få tillgång till sina personuppgifter eller för att få dessa uppgifter rättade eller raderade ([187]).

3.1 **Lagstiftning**

(144) De begränsningar och skyddsåtgärder som gäller för Sydkoreanska myndigheters insamling och efterföljande användning av personuppgifter följer av den övergripande konstitutionella ramen, särskilda lagar genom vilka deras verksamhet på områdena brottsbekämpning och nationell säkerhet regleras samt de regler som specifikt gäller för behandling av personuppgifter.

([181]) Såsom förklaras i skäl 127 kan missbruk av uppgifter utgöra ett brott enligt strafflagen.

([182]) Se Schrems II, punkterna 174–175 och där angiven rättspraxis. Se även, när det gäller tillgång för myndigheter i medlemsstaterna, mål C-623/17, Privacy International, ECLI:EU:C:2020:790, punkt 65 och de förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791, punkt 175.

([183]) Se Schrems II, punkterna 176 och 181, samt där angiven rättspraxis. Se även, när det gäller tillgång för medlemsstaternas myndigheter, Privacy International, punkt 68 och La Quadrature du Net m.fl., punkt 132.

([184]) Se Schrems II, punkt 176. Se även, när det gäller tillgång för medlemsstaternas myndigheter, Privacy International, punkt 68 och La Quadrature du Net m.fl., punkt 132.

([185]) Se Schrems II, punkt 179.

([186]) Se Schrems II, punkterna 181–182.

([187]) Se Schrems I, punkt 95, och Schrems II, punkt 194. I detta avseende har EU-domstolen särskilt betonat att efterlevnaden av artikel 47 i stadgan om de grundläggande rättigheterna, som garanterar rätten till ett effektivt rättsmedel inför en oavhängig och opartisk domstol, ”ingår i den skyddsnivå som krävs i unionen och [som] kommissionen måste slå fast innan den antar ett beslut om adekvat skyddsnivå enligt artikel 45.1 DSF” (Schrems II, punkt 186).

(145) För det första styrs sydkoreanska myndigheters tillgång till personuppgifter av allmänna principer om laglighet, nödvändighet och proportionalitet som följer av den sydkoreanska författningen ([188]). I författningen föreskrivs särskilt att grundläggande rättigheter och friheter (bl.a. rätten till integritet och rätten till post- och telehemlighet) ([189]) endast får begränsas genom lag och när det är nödvändigt för den nationella säkerheten eller för upprätthållande av lag och ordning för den allmänna välfärden. Sådana begränsningar får inte påverka rättens eller frihetens väsentliga innehåll. Med avseende särskilt på husrannsakan och beslag föreskrivs i författningen att en sådan endast får äga rum i enlighet med vad som stadgas i lag, på grundval av ett beslut utfärdat av en domare och med full respekt för rättssäkerheten ([190]). Slutligen kan enskilda personer åberopa sina rättigheter och friheter inför författningsdomstolen om de anser att dessa har kränkts i samband med myndighetsutövning ([191]). På samma sätt har enskilda personer som lidit skada på grund av en olaglig handling som begåtts av en offentlig tjänsteman i samband med tjänsteutövning rätt att begära rättvis ersättning ([192]).

(146) För det andra, vilket beskrivs närmare i avsnitten 3.2.1 och 3.3.1, återspeglas även de allmänna principer som nämns i skäl 145 i de särskilda lagar som reglerar befogenheterna för brottsbekämpande myndigheter och nationella säkerhetsmyndigheter. När det t.ex. gäller brottsutredningar föreskrivs i straffprocesslagen (*Criminal Procedure Act*) att obligatoriska åtgärder endast får vidtas om de uttryckligen föreskrivs i straffprocesslagen och i den minsta mån som krävs för att uppnå syftet med utredningen ([193]). På samma sätt förbjuds enligt artikel 3 i lagen om post- och telehemlighet (*Communications Privacy Protection Act*) tillgång till privat kommunikation, utom på grundval av lagen och med förbehåll för de begränsningar och skyddsåtgärder som anges däri. På området nationell säkerhet föreskrivs i lagen om den nationella underrättelsetjänsten (*NIS-lagen)(National Intelligence Service Act*) att all tillgång till kommunikations- eller lokaliseringsuppgifter måste vara förenlig med lagen och att missbruk av makt och lagöverträdelser ska omfattas av straffrättsliga påföljder ([194]).

(147) För det tredje omfattas myndigheters behandling av personuppgifter, även för brottsbekämpande ändamål och för ändamål som rör den nationella säkerheten, av dataskyddsregler enligt PIPA ([195]). Grundprincipen är enligt artikel 5.1 i PIPA att myndigheter ska utarbeta strategier för att förhindra ”missbruk och felaktig användning av personuppgifter, genomgripande övervakning och spårning osv. och att stärka människors värdighet och personliga integritet”. Dessutom måste alla personuppgiftsansvariga behandla personuppgifter på ett sätt som minimerar risken att den registrerades integritet kränks (artikel 3.6 i PIPA).

(148) Alla kraven i PIPA, som beskrivs närmare i avsnitt 2, gäller för behandling av personuppgifter för brottsbekämpande ändamål. Detta inbegriper grundläggande principer (t.ex. laglighet och korrekthet, ändamålsbegränsning, noggrannhet, uppgiftsminimering, begränsad lagring, säkerhet och öppenhet), skyldigheter (t.ex. när det gäller anmälan av uppgiftsincidenter och känsliga uppgifter) och rättigheter (tillgång, rättelse, radering och upphörande).

(149) Även om behandlingen av personuppgifter för ändamål som rör den nationella säkerheten omfattas av en mer begränsad uppsättning bestämmelser enligt PIPA gäller de grundläggande principerna samt reglerna om tillsyn, verkställighet och prövning ([196]). Närmare bestämt innehåller artiklarna 3 och 4 i PIPA allmänna principer för dataskydd (laglighet och korrekthet, ändamålsbegränsning, noggrannhet, uppgiftsminimering, säkerhet och öppenhet) och enskildas rättigheter (rätten att bli underrättad, rätten till tillgång och rätten till rättelse, radering och upphörande) ([197]). I artikel 4.5 i PIPA föreskrivs dessutom enskilda personers rätt till lämplig prövning genom ett skyndsamt och rättvist förfarande för skador som uppstår till följd av behandlingen av deras personuppgifter. Detta kompletteras av mer specifika skyldigheter att endast behandla personuppgifter i den minsta mån som

([188]) Se avsnitt 1.1 i bilaga II.
([189]) Artikel 37.2 i författningen.
([190]) Artiklarna 16 och 12.3 i författningen. I artikel 12.3 i författningen anges dessutom de undantagsfall då husrannsakan eller beslag kan äga rum utan domstolsbeslut (även om det fortfarande krävs ett domstolsbeslut i efterhand), dvs. om förövaren tas på bar gärning, eller för brott som leder till fängelse i minst tre år om det finns risk för att bevis kommer att förstöras eller att den misstänkte kommer att försvinna.
([191]) Artikel 68.1 i lagen om författningsdomstolen.
([192]) Artikel 29.1 i författningen.
([193]) Artikel 199.1 i straffprocesslagen. Mer allmänt ska myndigheter respektera misstänkta brottslingars och andra berörda personers grundläggande rättigheter när de utövar sina befogenheter enligt straffprocesslagen (artikel 198.2 i straffprocesslagen).
([194]) Artikel 14 i NIS-lagen.
([195]) Se avsnitt 1.2 i bilaga II.
([196]) Artikel 58.1 led 2 i PIPA. Se även avsnitt 6 i meddelande nr 2021-5 (bilaga I). Detta undantag från vissa bestämmelser i PIPA är endast tillämpligt när personuppgifter behandlas ”för ändamål som rör den nationella säkerheten”. När en sådan situation som rör den nationella säkerheten och som motiverar behandlingen av uppgifterna inte längre föreligger kan undantaget inte åberopas och alla krav i PIPA är tillämpliga.
([197]) Sådana rättigheter får endast inskränkas om det föreskrivs i lag i den utsträckning och så länge som det är nödvändigt och proportionerligt för att skydda ett viktigt mål av allmänt intresse, eller om beviljandet av rätten kan skada en tredje parts liv eller kropp, eller orsaka en omotiverad kränkning av en tredje parts äganderätt eller andra intressen. Se avsnitt 6 i meddelande nr 2021-5.

krävs för att uppnå det avsedda ändamålet och under kortast möjliga tidsperiod, att vidta nödvändiga åtgärder för att säkerställa säker datahantering och lämplig behandling (t.ex. tekniska, administrativa och fysiska skyddsåtgärder) samt att vidta åtgärder för lämplig hantering av enskilda klagomål ([198]). Slutligen gäller de allmänna principerna om laglighet, nödvändighet och proportionalitet enligt den sydkoreanska författningen (se skäl 145) även vid behandling av personuppgifter för ändamål som rör den nationella säkerheten.

(150) Dessa allmänna begränsningar och skyddsåtgärder kan åberopas av enskilda personer inför oberoende tillsynsorgan (t.ex. nämnden för skydd av personuppgifter och/eller den nationella människorättskommissionen, se skälen 177–178) och domstolar (se skälen 179–183) för att erhålla prövning.

3.2 **Sydkoreanska myndigheters tillgång till och användning av personuppgifter för brottsbekämpande ändamål**

(151) I Sydkoreas lagstiftning föreskrivs ett antal begränsningar av tillgången till och användningen av personuppgifter för brottsbekämpande ändamål, och den innehåller tillsyns- och prövningsmekanismer som är i linje med de krav som avses i skälen 141–143 i detta beslut. Villkoren för sådan tillgång och de garantier som gäller för utövandet av dessa befogenheter bedöms i detalj i följande avsnitt.

3.2.1 *Rättsliga grunder, begränsningar och skyddsåtgärder*

(152) Personuppgifter som behandlas av sydkoreanska personuppgiftsansvariga och som skulle överföras från unionen enligt detta beslut ([199]) får samlas in av de sydkoreanska myndigheterna för brottsbekämpande ändamål i samband med en husrannsakan eller ett beslag (på grundval av straffprocesslagen), genom tillgång till kommunikationsinformation (på grundval av lagen om post- och telehemlighet) eller genom att erhålla abonnentuppgifter genom en begäran om frivilligt utlämnande (på grundval av lagen om telekomoperatörer) ([200]).

3.2.1.1 Husrannsakan och beslag

(153) Enligt straffprocesslagen får husrannsakan eller beslag endast ske om en person misstänks för ett brott, det är nödvändigt för utredningen och ett samband har styrkts mellan utredningen och den person husrannsakan avser eller det föremål som ska kontrolleras eller beslagtas ([201]). Dessutom får husrannsakan eller beslag (liksom alla obligatoriska åtgärder) endast godkännas/genomföras i den minsta mån som krävs ([202]). Om husrannsakan avser en hårddisk eller annat datalagringsmedium, kommer i princip endast själva uppgifterna (kopierade eller utskrivna) att beslagtas i stället för hela mediet ([203]). Det senare får endast beslagtas om det anses vara praktiskt omöjligt att skriva ut eller kopiera de begärda uppgifterna separat, eller om det anses praktiskt ogenomförbart att på annat sätt uppnå syftet med genomsökningen ([204]). Genom straffprocesslagen fastställs därför tydliga och precisa regler för omfattningen och tillämpningen av dessa åtgärder, så att intrånget i enskilda personers rättigheter vid husrannsakan eller beslag begränsas till vad som är nödvändigt för en särskild brottsutredning och står i proportion till det eftersträvade syftet.

([198]) Artikel 58.4 i PIPA.

([199]) Se avsnitt 2.1 i bilaga II. Den sydkoreanska regeringens officiella framställning (avsnitt 2.1 i bilaga II) hänvisar också till möjligheten att samla in information om finansiella transaktioner i syfte att förhindra penningtvätt och finansiering av terrorism på grundval av lagen om rapportering och användning av specificerad information om finansiella transaktioner (*lagen om finansiella transaktioner*). I lagen om finansiella transaktioner åläggs upplysningsskyldigheter dock endast personuppgiftsansvariga som behandlar personlig kreditinformation i enlighet med lagen om användning och skydd av kreditinformation och som är föremål för tillsyn av kommissionen för finansiella tjänster (se skäl 13). Eftersom behandling av personlig kreditinformation som utförs av sådana personuppgiftsansvariga inte omfattas av detta beslut är lagen om finansiella transaktioner inte relevant för denna bedömning.

([200]) I artikel 3 i lagen om post- och telehemlighet nämns också lagen om militärdomstolen som en möjlig rättslig grund för insamling av kommunikationsuppgifter. I lagen om militärdomstolen regleras dock insamling av uppgifter om militär personal och den kan endast tillämpas på civila i ett begränsat antal fall (t.ex. kan förfaranden inledas vid en militär domstol om militär personal och civila skulle begå ett brott tillsammans, eller om en person begår ett brott mot militären; se artikel 2 i lagen om militärdomstolen). Lagen innehåller allmänna bestämmelser för husrannsakan och beslag som liknar dem som anges i straffprocesslagen (se t.ex. artiklarna 146–149 och 153–156 i lagen om militärdomstolen) och där föreskrivs t.ex. att postförsändelser endast får samlas in om det är nödvändigt för en utredning och på grundval av ett beslut från militärdomstolen. In den mån elektronisk kommunikation skulle samlas in på grundval av ovanstående lag gäller de begränsningar och skyddsåtgärder som anges i lagen om post- och telehemlighet. Se avsnitt 2.2.2 i bilaga II och fotnot 50.

([201]) Artikel 215.1 och 215.2 i straffprocesslagen. Se även artiklarna 106.1, 107 och 109 i straffprocesslagen, enligt vilka domstolar får göra husrannsakan och beslag så länge de berörda föremålen eller personerna anses vara kopplade till ett enskilt fall. Se avsnitt 2.2.1.2 i bilaga II.

([202]) Artikel 199.1 i straffprocesslagen.

([203]) Artikel 106.3 i straffprocesslagen.

([204]) Artikel 106.3 i straffprocesslagen.

(154) När det gäller rättssäkerhetsgarantier krävs enligt straffprocesslagen att ett domstolsbeslut inhämtas för att utföra husrannsakan eller beslag ([205]). Husrannsakan eller beslag utan domstolsbeslut tillåts endast i undantagsfall, nämligen om brådskande omständigheter föreligger ([206]), på plats när en misstänkt brottsling grips eller frihetsberövas ([207]) eller om ett föremål kasseras eller inges frivilligt av en misstänkt brottsling eller tredje man (av den berörda personen när det gäller personuppgifter) ([208]). Rättsstridiga husrannsakningar och beslag är föremål för straffrättsliga påföljder ([209]) och alla bevis som erhållits i strid med straffprocesslagen betraktas som otillåten bevisning ([210]). Slutligen måste de berörda personerna alltid underrättas om en husrannsakan eller ett beslag (däribland ett beslag av deras uppgifter) utan dröjsmål ([211]), vilket i sin tur kommer att underlätta utövandet av personens materiella rättigheter och rätten till prövning (se särskilt möjligheten att bestrida verkställigheten av ett beslut om beslag, se skäl 180).

3.2.1.2 Tillgång till kommunikationsinformation

(155) På grundval av lagen om post- och telehemlighet får de sydkoreanska brottsbekämpande myndigheterna vidta två typer av åtgärder ([212]): å ena sidan samla in ”uppgifter om kommunikationsbekräftelse” ([213]), vilket innefattar datum för telekommunikation, start- och sluttid, antal utgående och inkommande samtal samt den andra partens abonnentnummer, användningsfrekvens, loggfiler avseende användningen av telekommunikationstjänster och lokaliseringsuppgifter (t.ex. från sändningstorn där signaler tas emot), och å andra sidan ”kommunikationsbegränsande åtgärder”, vilket omfattar både insamling av innehållet i traditionell post och direkt avlyssning av innehållet i telekommunikationer ([214]).

(156) Tillgång till uppgifter om kommunikationsbekräftelse tillåts endast när det är nödvändigt för att genomföra en brottsutredning eller verkställa en dom ([215]), och på grundval av ett domstolsbeslut ([216]). I detta avseende krävs enligt lagen om post- och telehemlighet att detaljerad information anges både i ansökan om domstolsbeslutet (t. ex. skälen till begäran, förhållandet till den person åtgärderna avser/abonnenten och de nödvändiga uppgifterna) och i själva domstolsbeslutet (t.ex. åtgärdens syfte, den person åtgärden avser och åtgärdens tillämpningsområde) ([217]). Insamling utan domstolsbeslut får endast ske när det på grund av brådskande skäl

([205]) Artikel 215.1 och 215.2 i straffprocesslagen, artikel 113 i straffprocesslagen. När ett domstolsbeslut begärs måste den berörda myndigheten lägga fram handlingar som visar att en person är misstänkt för ett brott, att husrannsakan, inspektion eller beslag krävs och att det finns relevanta föremål som ska beslagtas (artikel 108.1 i förordningen om straffrättsligt förfarande). I domstolsbeslutet måste bl.a. anges den brottsmisstänktes namn och brottet, den plats, person eller föremål som ska genomsökas, eller föremål som ska beslagtas, datum för utfärdande och den faktiska tillämpningsperioden (artikel 114.1 jämförd med artikel 219 i straffprocesslagen). Se avsnitt 2.2.1.2 i bilaga II.

([206]) Dvs. när det är omöjligt att erhålla ett domstolsbeslut på grund av brådska på platsen för ett brott (artikel 216.3 i straffprocesslagen). I sådana fall måste ett domstolsbeslut erhållas i efterhand utan dröjsmål (artikel 216.3 i straffprocesslagen).

([207]) Artikel 216.1 och 216.2 i straffprocesslagen.

([208]) Artikel 218 i straffprocesslagen. Dessutom, såsom förklaras i avsnitt 2.2.1.2 i bilaga II, godtas frivilligt ingivna föremål endast som bevis i domstolsförfaranden om det är utom rimligt tvivel att offentliggörandet är frivilligt, vilket det är åklagarens uppgift att visa.

([209]) Artikel 321 i strafflagen.

([210]) Artikel 308-2 i straffprocesslagen. Dessutom kan den berörda personen (och hans eller hennes ombud) närvara när ett domstolsbeslut om husrannsakan eller beslag verkställs och kan därför även göra invändningar vid den tidpunkt då beslutet verkställs (artiklarna 121 och 219 i straffprocesslagen).

([211]) Artiklarna 121 och 122 i straffprocesslagen (med avseende på husrannsakan) och artikel 219 jämförd med artikel 106.4 i straffprocesslagen (med avseende på beslag).

([212]) Se även avsnitt 2.2.2.1 i bilaga II. Sådana åtgärder får vidtas med obligatorisk assistans från teleoperatörer efter att ha gett sådana operatörer ett skriftligt tillstånd från en domstol (artikel 9.2 i lagen om post- och telehemlighet). Operatörerna ska behålla detta tillstånd (artikel 15-2 i lagen om post- och telehemlighet och artikel 12 i genomförandedekretet till lagen om post- och telehemlighet). Leverantörer av telekommunikation får vägra att samarbeta om information som gäller den person åtgärderna riktas mot enligt domstolens skriftliga tillstånd (t.ex. den enskildes telefonnummer) är felaktig och under alla omständigheter förbjuds de att lämna ut lösenord som används för telekommunikation (artikel 9.4 i lagen om post- och telehemlighet).

([213]) Artikel 2.11 i lagen om post- och telehemlighet.

([214]) Se artikel 2.6 i lagen om post- och telehemlighet där det hänvisas till ”censur” (öppnande av post utan den berörda partens medgivande eller förvärv av kunskap om, registrering av eller undanhållande av innehåll på annat sätt) och artikel 2.7 i lagen om post- och telehemlighet där det hänvisas till ”avlyssning” (förvärv eller registrering av innehållet i telekommunikationer genom att lyssna på eller gemensamt läsa av ljud, ord, symboler eller bilder i kommunikationen med hjälp av elektronisk och mekanisk utrustning utan den berörda partens samtycke, eller genom att göra intrång i samband med kommunikationens överföring och mottagning).

([215]) Artikel 13.1 i lagen om post- och telehemlighet. Se även avsnitt 2.2.2.3 i bilaga II. Dessutom får uppgifter om spårning i realtid och kommunikationsbekräftelse avseende en viss basstation endast samlas in för utredning av allvarliga brott eller om det annars skulle vara svårt att förhindra att ett brott begås eller samla in bevis (artikel 13.2 i lagen om post- och telehemlighet). Detta återspeglar behovet av ytterligare skyddsåtgärder när det gäller åtgärder som gör synnerliga ingrepp i den personliga integriteten, i linje med proportionalitetsprincipen.

([216]) Artiklarna 13 och 6 i lagen om post- och telehemlighet.

([217]) Se artikel 13.3 och 13.9 jämförd med artikel 6.4 och 6.6 i lagen om post- och telehemlighet.

är omöjligt att erhålla domstolstillstånd, varvid domstolsbeslutet måste erhållas och meddelas telekommunikationsleverantören omedelbart efter att uppgifterna har begärts ([218]). Om domstolen vägrar att bevilja efterföljande tillstånd måste de insamlade uppgifterna förstöras ([219]).

(157) Vad gäller ytterligare skyddsåtgärder i samband med insamling av uppgifter om kommunikationsbekräftelse anges i lagen om post- och hemlighet särskilda krav på dokumentation och öppenhet ([220]). I synnerhet måste både brottsbekämpande myndigheter ([221]) och leverantörer av telekommunikation ([222]) föra register över begäranden och utlämnanden som gjorts. Dessutom måste brottsbekämpande myndigheter i princip underrätta enskilda personer om att deras uppgifter om kommunikationsbekräftelse har samlats in ([223]). En sådan underrättelse får endast skjutas upp i undantagsfall på grundval av ett tillstånd från chefen för en behörig åklagarmyndighet ([224]). Ett sådant tillstånd får endast beviljas om det är sannolikt att underrättelse kan 1) äventyra den nationella säkerheten, den allmänna säkerheten och ordningen, 2) orsaka dödsfall eller kroppsskada, 3) hindra rättvisa rättsliga förfaranden (t.ex. leda till att bevis förstörs eller vittnen hotas) eller 4) innebära förtal av den misstänkte, brottsoffer eller andra personer med anknytning till målet eller inkräkta på deras privatliv. I sådana fall ska underrättelse lämnas inom 30 dagar efter det att skälet eller skälen för uppskjutande av underrättelsen inte längre föreligger ([225]). När enskilda personer underrättas har de rätt att få information om skälen till att uppgifterna har samlats in ([226]).

(158) Strängare regler tillämpas för kommunikationsbegränsande åtgärder, som endast får användas om det finns betydande skäl att misstänka att vissa allvarliga brott som är särskilt förtecknade i lagen om post- och telehemlighet planeras, begås eller har begåtts ([227]). Dessutom får kommunikationsbegränsande åtgärder endast vidtas som en sista utväg och när det är svårt att på annat sätt förhindra att ett brott begås, gripa en brottsling eller samla in bevis ([228]). De måste omedelbart upphöra när de inte längre är nödvändiga, för att säkerställa att intrånget i kommunikationens integritet är så begränsad som möjligt ([229]). Information som erhållits på olaglig väg genom kommunikationsbegränsande åtgärder kommer inte att godtas som bevis i rättsliga eller disciplinära förfaranden ([230]).

(159) När det gäller rättssäkerhetsgarantier krävs enligt lagen om post- och telehemlighet att ett domstolsbeslut inhämtas för att genomföra kommunikationsbegränsande åtgärder ([231]). Återigen krävs enligt lagen om post- och telehemlighet att ansökan om ett domstolsbeslut och domstolsbeslutet i sig innehåller detaljerad information ([232]), däribland motiveringen till begäran samt den kommunikation som ska samlas in (som måste tillhöra den misstänkta person som är föremål för utredningen) ([233]). Sådana åtgärder får endast vidtas utan domstolsbeslut om det föreligger ett överhängande hot om organiserad brottslighet eller om ett annat allvarligt brott som direkt kan orsaka dödsfall eller allvarlig skada är nära förestående, och det föreligger en nödsituation som gör det

([218]) Artikel 13.2 i lagen om post- och telehemlighet.
([219]) Artikel 13.3 i lagen om post- och telehemlighet.
([220]) Se avsnitt 2.2.2.3 i bilaga II.
([221]) Artikel 13.5 och 13.6 i lagen om post- och telehemlighet.
([222]) Artikel 13.7 i lagen om post- och telehemlighet. Dessutom måste leverantörer av telekommunikation två gånger per år rapportera om utlämnande av uppgifter om kommunikationsbekräftelse till ministeriet för vetenskap och IKT.
([223]) Se artikel 13-3.7 jämförd med artikel 9-2 i lagen om post- och telehemlighet. I synnerhet måste enskilda personer underrättas inom 30 dagar efter det att ett beslut har fattats om att (inte) väcka åtal eller inom 30 dagar ett år efter det att ett beslut om att skjuta upp ett åtal har fattats (men underrättelsen måste under alla omständigheter ges inom 30 dagar ett år efter det att uppgifterna har samlats in), se artikel 13-3.1 i lagen om post- och telehemlighet.
([224]) Artikel 13-3.2–13-3.3 i lagen om post- och telehemlighet.
([225]) Artikel 13-3.4 i lagen om post- och telehemlighet.
([226]) Artikel 13-3.5 i lagen om post- och telehemlighet. På begäran av den enskilde ska en åklagare eller en tjänsteman inom kriminalpolisen skriftligen ange skälen till detta inom 30 dagar från mottagandet av begäran, såvida inte ett av undantagen för uppskjutande av underrättelse är tillämpligt (artikel 13-3.6 i lagen om post- och telehemlighet).
([227]) T.ex. uppror, narkotikarelaterade brott eller brott med sprängämnen, samt brott med anknytning till nationell säkerhet, diplomatiska förbindelser eller militära baser och installationer, se artikel 5.1 i lagen om post- och telehemlighet. Se även avsnitt 2.2.2.2 i bilaga II.
([228]) Artiklarna 3.2 och 5.1 i lagen om post- och telehemlighet.
([229]) Artikel 2 i genomförandedekretet till lagen om post- och telehemlighet.
([230]) Artikel 4 i lagen om post- och telehemlighet.
([231]) Artikel 6.1, 6.2 och 6.5–6.6 i lagen om post- och telehemlighet.
([232]) En ansökan om domstolsbeslut ska innehålla 1) väsentliga skäl (som vid första påseende framstår som befogade) till misstanke om att ett av de förtecknade brotten planeras, begås eller har begåtts samt eventuellt underlag, 2) de kommunikationsbegränsande åtgärderna samt deras mål, omfattning, syfte och faktiska tillämpningsperiod, 3) var åtgärderna skulle genomföras och hur de skulle genomföras (artikel 6.4 i lagen om post- och telehemlighet och artikel 4.1 i genomförandedekretet till lagen om post- och hemlighet). Domstolsbeslutet ska innehålla uppgifter om vilka typer av åtgärder som ska vidtas samt deras mål, omfattning, faktiska tillämpningsperiod, plats för genomförande och hur de ska genomföras (artikel 6.6 i lagen om post- och telehemlighet).
([233]) Målet för en kommunikationsbegränsande åtgärd måste vara specifika postförsändelser eller telekommunikationer som skickas eller tas emot av den misstänkte, eller postförsändelser eller telekommunikationer som skickas eller tas emot av den misstänkte under en bestämd tidsperiod (artikel 5.2 i lagen om post- och telehemlighet).

omöjligt att genomgå det ordinarie förfarandet ([234]). En ansökan om ett domstolsbeslut måste dock inges omedelbart efter det att åtgärden har vidtagits ([235]). Kommunikationsbegränsande åtgärder får endast vidtas under en period på högst två månader ([236]) och detta får endast förlängas med domstolens godkännande om villkoren för att genomföra åtgärderna fortfarande är uppfyllda ([237]). Den förlängda perioden får inte överstiga totalt ett år, eller tre år för vissa särskilt allvarliga brott (såsom brott med anknytning till uppror, utländsk aggression, nationell säkerhet) ([238]).

(160) I likhet med vad som är fallet för insamling av uppgifter om kommunikationsbekräftelse krävs enligt lagen om post- och telehemlighet att leverantörer av telekommunikation ([239]) och brottsbekämpande myndigheter ([240]) för register över genomförda åtgärder för kommunikationsbegränsning, och där föreskrivs att den berörda personen ska underrättas, vilket i undantagsfall kan skjutas upp om detta är nödvändigt av skäl som rör viktiga allmänna intressen ([241]).

(161) Slutligen är åsidosättande av flera av de begränsningar och skyddsåtgärder som anges i lagen om post- och telehemlighet (bl.a. skyldigheterna att erhålla ett domstolsbeslut, föra register och underrätta personen), både när det gäller insamling av uppgifter om kommunikationsbekräftelse och användning av kommunikationsbegränsande åtgärder, föremål för straffrättsliga påföljder ([242]).

(162) De brottsbekämpande myndigheternas befogenheter att samla in kommunikationsuppgifter på grundval av lagen om post- och telehemlighet (både innehållet i kommunikation och uppgifter om kommunikationsbekräftelse) begränsas därför genom tydliga och precisa regler och omfattas av ett antal skyddsåtgärder. Dessa skyddsåtgärder garanterar i synnerhet tillsyn av hur sådana åtgärder genomförs, både på förhand (genom förhandsgodkännande från domstol) och i efterhand (genom dokumentations- och rapporteringskrav), och underlättar enskilda personers tillgång till effektiva rättsmedel (genom att säkerställa att de informeras om insamlingen av deras uppgifter).

3.2.1.3 Begäran om frivilligt utlämnande av abonnentuppgifter

(163) Utöver att förlita sig på de obligatoriska åtgärder som beskrivs i skälen 153–162 får de sydkoreanska brottsbekämpande myndigheterna begära ”kommunikationsuppgifter” från leverantörer av telekommunikation på frivillig basis till stöd för en brottmålsprocess, utredning eller verkställighet av dom (artikel 83.3 i lagen om telekomoperatörer). Denna möjlighet finns endast med avseende på begränsade datauppsättningar, dvs. användarnas namn, nummer i folkbokföringsregistret, adress och telefonnummer, datum då användarna tecknar eller avslutar sitt abonnemang samt deras identifieringskoder (dvs. koder som används för att identifiera den rättmätiga användaren av datasystem eller kommunikationsnät) ([243]). Eftersom endast personer som direkt kontrakterar tjänster från en sydkoreansk telekommunikationsleverantör betraktas som ”användare” ([244]), skulle enskilda personer i EU vars uppgifter har överförts till Sydkorea normalt sett inte omfattas av denna kategori ([245]).

(164) Olika begränsningar gäller för sådan frivillig utlämning, både för den brottsbekämpande myndighetens utövande av sina befogenheter och för teleoperatörens respons. Ett allmänt krav är att de brottsbekämpande myndigheterna måste agera i enlighet med författningens principer om nödvändighet och proportionalitet (artiklarna 12.1 och 37.2 i författningen), även när de begär information på frivillig basis. Dessutom måste de följa PIPA, särskilt genom att endast samla in personuppgifter i den utsträckning som krävs för att uppnå ett legitimt ändamål, på ett sätt som minimerar inverkan på enskilda personers privatliv (t.ex. artikel 3.1 och 3.6 i PIPA). Närmare

([234]) Artikel 8.1 i lagen om post- och telehemlighet. Insamling av information i nödsituationer måste dock alltid ske i enlighet med ett ”uttalande om nödcensur/nödavlyssning” och den myndighet som utför insamlingen måste föra ett register över alla sådana nödåtgärder (artikel 8.4 i lagen om post- och telehemlighet).

([235]) Insamlingen måste upphöra omedelbart om det brottsbekämpande organet inte erhåller domstolstillstånd inom 36 timmar (artikel 8.2 i lagen om post- och telehemlighet), i vilket fall den insamlade informationen i princip kommer att förstöras såsom förklaras i avsnitt 2.2.2.2 i bilaga II. Domstolen måste också underrättas om nödåtgärderna har slutförts på så kort tid att behovet av tillstånd elimineras (t.ex. om den misstänkte grips omedelbart efter det att avlyssningen inletts, se artikel 8.5 i lagen om post- och telehemlighet). I sådana fall ska domstolen förses med information avseende syfte, mål, tillämpningsområde, tidsperiod, platsen för genomförandet och insamlingsmetod samt skälen för att inte ha lämnat in en begäran om domstolstillstånd (artikel 8.6–8.7 i lagen om post- och telehemlighet).

([236]) Artikel 6.7 i lagen om post- och telehemlighet. Om syftet med åtgärderna uppnås tidigare under denna period måste åtgärderna omedelbart upphöra.

([237]) Artikel 6.7–6.8 i lagen om post- och telehemlighet.

([238]) Artikel 6.8 i lagen om post- och telehemlighet.

([239]) Artikel 9.3 i lagen om post- och telehemlighet.

([240]) Artikel 18.1 i genomförandedekretet till lagen om post- och telehemlighet.

([241]) Åklagaren ska särskilt underrätta den enskilde inom 30 dagar från det att ett åtal väcks eller ett beslut utfärdas om att avstå från åtal eller gripande (artikel 9-2.1 i lagen om post- och telehemlighet). Underrättelsen får skjutas upp med godkännande från chefen för åklagarmyndigheten om det sannolikt skulle allvarligt äventyra den nationella säkerheten eller störa den allmänna säkerheten eller ordningen, eller om det sannolikt skulle leda till väsentlig skada på andras liv och kroppar (artikel 9.2.4–9.2.6 i lagen om post- och telehemlighet).

([242]) Artiklarna 16 och 17 i lagen om post- och telehemlighet.

([243]) Artikel 83.3 i lagen om telekomoperatörer. Se även avsnitt 2.2.3 i bilaga II.

([244]) Artikel 2.9 i lagen om telekomoperatörer.

([245]) Se även avsnitt 2.2.3 i bilaga II.

bestämt ska begäran om att erhålla kommunikationsuppgifter på grundval av lagen om telekomoperatörer göras skriftligen och däri ska skälen till begäran, länken till den relevanta användaren och de begärda uppgifternas omfattning anges ([246]).

(165) Leverantörer av telekommunikation behöver inte efterkomma begäran, men får göra det på frivillig basis och då endast i enlighet med PIPA. Detta innebär framför allt att de måste göra en avvägning mellan de olika intressen som står på spel och att de inte får tillhandahålla uppgifterna om detta sannolikt skulle inkräkta på enskilda individers eller tredje mans intressen på ett otillbörligt sätt ([247]). Detta skulle exempelvis vara fallet om det är uppenbart att den begärande myndigheten missbrukar sin auktoritet ([248]). Teleoperatörer måste föra register över uppgifter som lämnats ut enligt lagen om telekomoperatörer och två gånger per år rapportera till ministern för vetenskap och IKT ([249]).

(166) I enlighet med avsnitt 3 i meddelande nr 2021-5 (bilaga I) måste leverantörer av telekommunikation dessutom i princip underrätta den berörda personen när de frivilligt efterkommer en begäran ([250]). Detta kommer i sin tur att göra det möjligt för den enskilde att utöva sina rättigheter och erhålla prövning om hans eller hennes uppgifter röjs på ett olagligt sätt, antingen gentemot den personuppgiftsansvarige (t.ex. för att ha lämnat ut uppgifter i strid med PIPA eller för att ha efterkommit en begäran som var uppenbart oproportionerlig) eller mot den brottsbekämpande myndigheten (t.ex. för att ha agerat utöver vad som är nödvändigt och proportionerligt eller för att inte ha respekterat förfarandekraven i lagen om telekomoperatörer).

3.2.2 *Vidare användning av de insamlade uppgifterna*

(167) Behandling av personuppgifter som samlas in av de sydkoreanska brottsbekämpande myndigheterna omfattas av alla krav i PIPA, däribland ändamålsbegränsning (artikel 3.1–3.2 i PIPA), lagenlig användning och tillhandahållande till tredje part (artiklarna 15, 17 och 18 i PIPA), internationella överföringar (artiklarna 17 och 18 i PIPA jämförda med avsnitt 2 i meddelande nr 2021-5) ([251]), proportionalitet/dataminimering (artikel 3.1 och 3.6 i PIPA) och lagringsbegränsning (artikel 21 i PIPA) ([252]).

(168) När det gäller kommunikationsinnehåll som erhållits genom kommunikationsbegränsande åtgärder begränsas i lagen om post- och telehemlighet uttryckligen eventuell användning av sådant innehåll till utredning, lagföring eller förebyggande av allvarliga brott ([253]), disciplinära förfaranden för samma typ av brott, skadeståndsanspråk som väcks av en part i kommunikationen eller om detta uttryckligen tillåts enligt andra lagar ([254]). Dessutom får insamlat innehåll i telekommunikationer som överförs via internet endast lagras med godkännande från den domstol som godkände de kommunikationsbegränsande åtgärderna ([255]), i syfte att använda det för utredning, lagföring eller förebyggande av allvarliga brott ([256]). Mer allmänt förbjuds i lagen om post- och telehemlighet utlämnande av konfidentiell information som erhållits från kommunikationsbegränsande åtgärder och att sådan information används för att skada anseendet hos dem som var föremål för åtgärderna ([257]).

3.2.3 *Tillsyn*

(169) I Sydkorea övervakas de brottsbekämpande myndigheternas verksamhet av olika organ ([258]).

([246]) Artikel 83.4 i lagen om telekomoperatörer. Om det är omöjligt att lämna in en skriftlig begäran på grund av brådskande omständigheter ska den skriftliga begäran lämnas så snart som skälet till brådskan upphör (artikel 83.4 i lagen om telekomoperatörer).
([247]) Artikel 18.2 i PIPA.
([248]) Högsta domstolens beslut nr 2012Da105482 av den 10 mars 2016. Se även avsnitt 2.2.3 i bilaga II om detta beslut från högsta domstolen.
([249]) Artikel 83.5–83.6 i lagen om telekomoperatörer.
([250]) Begränsade och kvalificerade undantag gäller för detta krav, särskilt om och så länge som underrättelsen skulle äventyra en pågående brottsutredning eller sannolikt skulle skada en annan persons liv eller kropp, om dessa rättigheter eller intressen är uppenbart överordnade den registrerades rättigheter. Se avsnitt 3 iii.1 i meddelandet.
([251]) I synnerhet är sydkoreanska myndigheter skyldiga att genom ett rättsligt bindande instrument garantera en skyddsnivå som motsvarar PIPA, se även skäl 90.
([252]) Se även avsnitt 1.2 i bilaga II.
([253]) Se skäl 158.
([254]) Artikel 12 i lagen om post- och telehemlighet. Se avsnitt 2.2.2.2 i bilaga II.
([255]) Den åklagare eller polis som genomför de kommunikationsbegränsande åtgärderna måste välja ut den telekommunikation som ska lagras inom 14 dagar efter det att åtgärderna har upphört och begära godkännande från domstol (när det gäller en polistjänsteman ska ansökan göras hos en åklagare, som i sin tur vidarebefordrar ansökan till domstolen), se artikel 12-2.1 och 12-2.2 i lagen om post- och telehemlighet.
([256]) En ansökan om ett sådant tillstånd måste innehålla information om de kommunikationsbegränsande åtgärderna, en sammanfattning av åtgärdernas resultat, skälen till lagringen (tillsammans med underlag) och den telekommunikation som ska lagras (artikel 12-2.3 i lagen om post- och telehemlighet). Om ingen ansökan görs måste de insamlade uppgifterna raderas inom 14 dagar efter det att den kommunikationsbegränsande åtgärden har avslutats (artikel 12-2.5 i lagen om post- och telehemlighet) och inom sju dagar om ansökan avslås (artikel 12-2.5 i lagen om post- och telehemlighet). I båda fallen ska en rapport om raderingen inges inom sju dagar till den domstol som godkände insamlingen.
([257]) Artikel 11.2 i genomförandedekretet till lagen om post- och telehemlighet.
([258]) Se avsnitt 2.3 i bilaga II.

(170) För det första är polisen föremål för intern tillsyn av en generalinspektör ([259]) som utför laglighetskontroller, även när det gäller eventuella kränkningar av de mänskliga rättigheterna. Generalinspektörsämbetet inrättades för att genomföra lagen om revision av den offentliga sektorn, där inrättande av internt revisionsorgan uppmuntras och särskilda krav för deras sammansättning och uppgifter fastställs. I lagen föreskrivs särskilt att chefen för ett internt revisionsorgan ska utses utanför den berörda myndigheten (t.ex. tidigare domare, professorer) för en period på två till fem år ([260]), endast ska kunna avsättas av motiverade skäl (t.ex. om han eller hon inte kan utföra sina uppgifter av hälsoskäl eller är föremål för disciplinära åtgärder) ([261]) och ska garanteras oberoende i största möjliga utsträckning ([262]). Hindrande av internrevision är föremål för administrativa sanktionsavgifter ([263]). Revisionsrapporter (som kan innehålla rekommendationer, begäran om disciplinåtgärder och begäran om ersättning eller rättelse) överlämnas till chefen för den berörda myndigheten samt revisions- och kontrollstyrelsen (*Board of Audit and Inspection*) ([264]), och offentliggörs i allmänhet ([265]). Resultaten av genomförandet av rapporten måste också meddelas revisions- och kontrollstyrelsen ([266]) (se skäl 173 om revisions- och kontrollstyrelsens tillsynsroll och befogenheter).

(171) För det andra övervakar nämnden för skydd av personuppgifter att brottsbekämpande myndigheters behandling av personuppgifter följer PIPA och andra lagar som skyddar enskilda personers integritet, däribland lagar som reglerar insamlingen av (elektroniska) bevis för brottsbekämpande ändamål, såsom beskrivs i avsnitt 3.2.1 ([267]). Eftersom tillsyn av nämnden för skydd av personuppgifter utvidgas till att omfatta laglighet och korrekthet vid insamling och behandling av uppgifter (artikel 3.1 i PIPA), vilket åsidosätts om personuppgifter hämtas och används i strid med dessa lagar ([268]), får nämnden för skydd av personuppgifter även utreda och kontrollera efterlevnad av de begränsningar och skyddsåtgärder som anges i avsnitt 3.2.1 ([269]). Vid utövandet av denna tillsynsroll kan nämnden för skydd av personuppgifter utnyttja alla sina utredningsbefogenheter och korrigerande befogenheter, såsom beskrivs i detalj i avsnitt 2.4.2. Redan före den nyligen genomförda reformen av PIPA (dvs. i dess tidigare tillsynsroll för den offentliga sektorn) genomförde nämnden för skydd av personuppgifter flera tillsynsåtgärder avseende brottsbekämpande myndigheters behandling av personuppgifter, t.ex. i samband med förhör av misstänkta (ärende nr 2013-16 av den 26 augusti 2013), med avseende på underrättelse till enskilda om införandet av administrativa sanktionsavgifter (ärende nr 2015-02-04 av den 26 januari 2015, utbyte av uppgifter med andra myndigheter (ärende nr 2018-15-146 av den 9 juli 2018, ärende nr 2018-25-308 av den 10 december 2018, ärende nr 2019-02-015 av den 29 januari 2019), insamling av fingeravtryck eller fotografier (ärende nr 2019-17-273 av den 9 september 2019), användning av drönare (ärende nr 2020-01-004 av den 13 januari 2020). I dessa fall undersökte nämnden för skydd av personuppgifter efterlevnaden av flera bestämmelser i PIPA (t.ex. behandlingens lagenlighet, principerna om ändamålsbegränsning och uppgiftsminimering) men också relevanta bestämmelser i andra lagar, t.ex. straffprocesslagen, och utfärdade vid behov rekommendationer för att anpassa behandlingen till dataskyddskraven.

(172) För det tredje tillhandahålls oberoende tillsyn av den nationella människorättskommissionen ([270]), som kan utreda kränkningar av rätten till integritet och till sekretess vid korrespondens som en del av sitt allmänna mandat att skydda de grundläggande rättigheterna i artiklarna 10–22 i författningen. Den nationella människorättskommissionen består av elva ledamöter som måste uppfylla särskilda kvalifikationer ([271]) och utses av presidenten i enlighet med förfaranden som fastställts i lag. Särskilt gäller att fyra ledamöter utnämns efter nominering från parlamentet, fyra efter nominering från presidenten och tre efter nominering av högsta domstolens ordförande ([272]). Ordföranden utses av presidenten bland ledamöterna och måste bekräftas av parlamentet ([273]). Ledamöterna (däribland ordföranden) utses för en förnybar period på tre år och kan endast avsättas om de

([259]) Se avsnitt 2.3.1 i bilaga II. Se även https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) På samma sätt utses revisorer på grundval av de särskilda villkor som fastställs i lagen, se artiklarna 16 ff. i lagen om revisioner i den offentliga sektorn.
([261]) Artiklarna 8–11 i lagen om revisioner i den offentliga sektorn.
([262]) Artikel 7 i lagen om revisioner i den offentliga sektorn.
([263]) Artikel 41 i lagen om revisioner i den offentliga sektorn.
([264]) Artikel 23.1 i lagen om revisioner i den offentliga sektorn.
([265]) Artikel 26 i lagen om revisioner i den offentliga sektorn.
([266]) Artikel 23.3 i lagen om revisioner i den offentliga sektorn.
([267]) Se artikel 7-8.3, 7-8.4 och artikel 7-9.5 i PIPA.
([268]) Se meddelande från nämnden för skydd av personuppgifter nr 2021-5, avsnitt 6 (bilaga I).
([269]) Se även avsnitt 2.3.4 i bilaga II.
([270]) Artikel 1 i lagen om människorättskommissionen (*Human Rights Commission Act*, nedan kallad *NHRC-lagen*).
([271]) För att utses måste en ledamot 1) ha tjänstgjort i minst tio år vid ett universitet eller ett godkänt forskningsinstitut, åtminstone som biträdande professor, 2) ha tjänstgjort som domare, åklagare eller advokat i minst tio år, 3) ha varit verksam inom området mänskliga rättigheter i minst tio år (t.ex. för en ideell, icke-statlig organisation eller internationell organisation) eller 4) ha rekommenderats av grupper i det civila samhället (artikel 5.3 i NHRC-lagen). Efter att ha utsetts är den nationella människorättskommissionens ledamöter dessutom förbjudna att samtidigt inneha ett uppdrag i parlamentet, lokala råd eller något statligt eller lokalt myndighetsorgan (som offentlig tjänsteman), se artikel 10 i NHRC-lagen.
([272]) Artikel 5.1 och 5.2 i NHRC-lagen.
([273]) Artikel 5.5 i NHRC-lagen.

döms till fängelse eller inte längre kan utföra sina uppgifter på grund av långvarig bristande fysisk eller psykisk kapacitet (i vilket fall två tredjedelar av ledamöterna måste gå med på avskedandet) ([274]). Som en del av en undersökning får den nationella människorättskommissionen begära att relevant material lämnas in, att kontroller utförs och att enskilda personer kallas att vittna ([275]). När det gäller korrigerande befogenheter får den nationella människorättskommissionen utfärda (offentliga) rekommendationer för att förbättra eller korrigera särskilda politiska strategier och metoder. Myndigheter måste reagera på en sådan rekommendation med ett förslag till genomförandeplan ([276]). Om den berörda myndigheten underlåter att genomföra rekommendationer måste den informera människorättskommissionen om detta ([277]), som i sin tur kan underrätta parlamentet om denna underlåtenhet och/eller offentliggöra den. Enligt den officiella framställningen från den sydkoreanska regeringen (avsnitt 2.3.5 i bilaga II) följer de sydkoreanska myndigheterna i allmänhet den nationella människorättskommissionens rekommendationer och har ett starkt incitament att göra detta eftersom deras genomförande har bedömts vara en del av den allmänna, kontinuerliga utvärdering som genomförs under ledning av premiärministerns kansli. Årliga uppgifter om dess verksamhet visar att den nationella människorättskommissionen aktivt övervakar brottsbekämpande myndigheters verksamhet, antingen på grundval av enskilda framställningar eller genom undersökningar på eget initiativ ([278]).

(173) För det fjärde övervakar revisions- och kontrollstyrelsen myndighetsverksamheters laglighet i allmänhet och granskar statens inkomster och utgifter. Revisions- och kontrollstyrelsen övervakar även mer allmänt efterlevnad av myndigheternas skyldigheter i syfte att förbättra den offentliga förvaltningens verksamhet ([279]). Revisions- och kontrollstyrelsen är formellt inrättad under Sydkoreas president, men har en oberoende ställning när det gäller dess uppgifter ([280]). Dessutom beviljas den fullständigt oberoende när det gäller utnämning, avskedande och organisation av dess personal samt sammanställning av dess budget ([281]). Revisions- och kontrollstyrelsen består av en ordförande (utsedd av presidenten med parlamentets samtycke) ([282]) och sex ledamöter (utnämnda av presidenten på rekommendation av ordföranden) ([283]), som ska uppfylla de särskilda kvalifikationer som fastställs i lag ([284]) och endast får avsättas i händelse av riksrättsförfarande, frihetsstraff eller oförmåga att utföra sina uppgifter på grund av långvarig bristande psykisk eller fysisk kapacitet ([285]). Revisions- och kontrollstyrelsen utför en allmän revision på årsbasis, men kan också utföra särskilda revisioner i frågor av särskilt intresse. Revisions- och kontrollstyrelsen får begära in handlingar och begära att enskilda personer ska närvara i samband med en revision eller kontroll ([286]). Revisions- och kontrollstyrelsen får utfärda rekommendationer, begära disciplinära åtgärder eller inge en brottsanmälan ([287]).

(174) Slutligen utövar parlamentet tillsyn av myndigheter genom utredningar och kontroller ([288]) av deras verksamhet ([289]). Det får begära att handlingar lämnas ut, tvinga vittnen att framträda ([290]), rekommendera

([274]) Artiklarna 7.1 och 8 i NHRC-lagen.

([275]) Artikel 36 i NHRC-lagen. I enlighet med artikel 6.7 i lagen får inlämning av material eller föremål avslås om det skulle inverka menligt på statlig sekretess som skulle kunna ha en väsentlig inverkan på statens säkerhet eller diplomatiska förbindelser, eller utgöra ett allvarligt hinder för en brottsutredning eller pågående rättegång. I sådana fall får människorättskommissionen begära ytterligare information från chefen för det berörda organet (som med ärligt uppsåt måste efterkomma denna begäran) när så krävs för att kunna avgöra om vägran att lämna information är motiverad.

([276]) Artikel 25.1 och 25.3 i NHRC-lagen.

([277]) Artikel 25.4 i NHRC-lagen.

([278]) T.ex. mottog den nationella människorättskommissionen mellan 1 380 och 1 699 framställningar mot brottsbekämpande myndigheter per år mellan 2015 och 2019 och behandlade ett lika stort antal (t.ex. 1 546 klagomål mot polisen 2018 och 1 249 under 2019). Den nationella människorättskommissionen genomförde även flera utredningar på eget initiativ, vilket beskrivs närmare i den nationella människorättskommissionens årsrapport för 2018 (tillgänglig på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) och i årsrapporten för 2019 (tillgänglig på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Artiklarna 20 och 24 i lagen om revisions- och kontrollstyrelsen (*Act on the Board of Audit and Inspection*, nedan kallad *BAI-lagen*). Se avsnitt 2.3.2 i bilaga II.

([280]) Artikel 2.1 i BAI-lagen.

([281]) Artikel 2.2 i BAI-lagen.

([282]) Artikel 4.1 i BAI-lagen.

([283]) Artiklarna 5.1 och 6 i BAI-lagen.

([284]) T.ex. ha tjänstgjort som domare, allmän åklagare eller advokat i minst tio år, arbetat som offentlig tjänsteman eller professor eller ha haft en högre uppsatt tjänst vid ett universitet i minst åtta år, eller arbetat i minst tio år på ett börsnoterat aktiebolag eller vid en offentlig institution (varav minst fem år som verkställande direktör), se artikel 7 i BAI-lagen. Dessutom är ledamöter förbjudna att delta i politisk verksamhet och att samtidigt inneha uppdrag i parlamentet, förvaltningsorgan, organisationer som är föremål för revision och inspektion av revisions- och kontrollstyrelsen eller andra avlönade uppdrag eller befattningar (artikel 9 i BAI-lagen).

([285]) Artikel 8 i BAI-lagen.

([286]) Se t.ex. artikel 27 i BAI-lagen.

([287]) Artiklarna 24 och 31–35 i BAI-lagen.

([288]) Artikel 128 i lagen om parlamentet och artiklarna 2, 3 och 15 i lagen om kontroll och utredning av statsförvaltningen. Detta omfattar årliga inspektioner av offentliga angelägenheter som helhet, men även utredningar av specifika frågor.

([289]) Se avsnitt 2.2.3 i bilaga.

([290]) Artikel 10.1 i lagen om kontroll och utredning av statsförvaltningen. Se även artiklarna 128 och 129 i lagen om parlamentet.

korrigerande åtgärder (om den konstaterar att olaglig eller otillbörlig verksamhet har ägt rum) ([291]) och offentliggöra granskningsresultaten ([292]). Om parlamentet begär att korrigerande åtgärder ska vidtas – vilket t.ex. kan inbegripa beviljande av ersättning, disciplinära åtgärder eller förbättring av interna förfaranden – ska den berörda myndigheten agera utan dröjsmål och rapportera resultatet till parlamentet ([293]).

3.2.4 *Prövningsmöjligheter*

(175) I det sydkoreanska systemet erbjuds olika (rättsliga) möjligheter att erhålla prövning, däribland skadestånd.

(176) För det första ges enskilda personer enligt PIPA rätt till tillgång, rättelse, radering och upphörande när det gäller personuppgifter som behandlas för brottsbekämpande ändamål ([294]).

(177) För det andra kan enskilda personer använda sig av de olika prövningsmekanismer som erbjuds enligt PIPA om deras uppgifter har behandlats av en brottsbekämpande myndighet i strid med PIPA eller i strid med de begränsningar och skyddsåtgärder som styr insamlingen av personuppgifter i andra lagar (dvs. straffprocesslagen eller lagen om post- och telehemlighet, se skäl 171). I synnerhet kan enskilda personer lämna in ett klagomål till nämnden för skydd av personuppgifter (bl.a. via integritetstjänsten som drivs av Sydkoreas byrå för internet och säkerhet ([295])) eller kommittén för tvistlösning avseende personuppgifter ([296]). Dessa möjligheter till prövning omfattas inte av några ytterligare formkrav. På grundval av förvaltningsprocesslagen kan enskilda personer dessutom överklaga/bestrida nämndens beslut eller passivitet (se skäl 132).

(178) För det tredje kan en enskild individ ([297]) inge ett klagomål till den nationella människorättskommissionen avseende överträdelser av rätten till integritet och skydd av personuppgifter som begåtts av en sydkoreansk brottsbekämpande myndighet. Den nationella människorättskommissionen får rekommendera rättelse eller förbättring av relevanta stadgar, institutioner, riktlinjer eller praxis ([298]), eller genomförande av åtgärder såsom medling ([299]), upphörande av kränkningar av de mänskliga rättigheterna, skadestånd och åtgärder för att förhindra att samma eller liknande kränkningar upprepas ([300]). Enligt den officiella framställningen från den sydkoreanska regeringen (avsnitt 2.4.2 i bilaga II) kan detta även inbegripa radering av olagligt insamlade personuppgifter. Även om den nationella människorättskommissionen inte har befogenhet att fatta bindande beslut erbjuder den en mer informell och lättillgänglig prövningsväg till låg kostnad, särskilt eftersom det såsom förklaras i avsnitt 2.4.2 i bilaga II inte krävs att man påvisar någon skada för att klagomålet ska undersökas ([301]). Detta säkerställer att klagomål från enskilda avseende insamling av deras uppgifter kan undersökas även om en enskild person inte kan styrka att hans eller hennes uppgifter faktiskt har samlats in (t.ex. till följd av att underrättelse till den enskilda personen ännu inte har ägt rum). Den nationella människorättskommissionens årliga verksamhetsrapporter visar att enskilda personer också använder sig av denna väg i praktiken för att ifrågasätta brottsbekämpande myndigheters verksamhet, även när det gäller hantering av personuppgifter ([302]). Om en enskild person inte är nöjd med

([291]) Artikel 16.2 i lagen om kontroll och utredning av statsförvaltningen.
([292]) Artikel 12-2 i lagen om kontroll och utredning av statsförvaltningen.
([293]) Artikel 16.3 i lagen om kontroll och utredning av statsförvaltningen.
([294]) Denna rätt kan utövas direkt gentemot den behöriga myndigheten eller indirekt via nämnden för skydd av personuppgifter (artikel 35.2 i PIPA). Såsom beskrivs närmare i skälen 76–78 kommer undantag från dessa rättigheter endast att tillämpas när det är nödvändigt för att skydda viktiga (offentliga) intressen.
([295]) Artikel 62 i PIPA.
([296]) Artiklarna 40–50 i PIPA och artiklarna 48-2–57 i genomförandedekretet till PIPA. Se även avsnitt 2.4.1 i bilaga II.
([297]) Såsom förklaras i avsnitt 2.4.2 i bilaga II hänvisas i artikel 4 i lagen om den nationella kommissionen för mänskliga rättigheter till medborgare och utlänningar som är bosatta i Sydkorea, men begreppet ”bosatta” återspeglar snarare ett begrepp om jurisdiktion än territorium. Om en statlig institution i Sydkorea överträder grundläggande rättigheter tillhörande en utländsk medborgare utanför Sydkorea kan den personen inge ett klagomål till den nationella människorättskommissionen. Detta skulle vara fallet om de sydkoreanska myndigheterna har olaglig tillgång till personuppgifter som har överförts till Sydkorea avseende en utländsk medborgare. Se särskilt förklaringarna på https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Artikel 44 i NHRC-lagen.
([299]) En enskild person kan också begära att klagomålet ska lösas genom medling, se artikel 42 ff. i NRHC-lagen.
([300]) Artikel 42.4 i NHRC-lagen. Vidare får den nationella människorättskommissionen vidta brådskande åtgärder vid en pågående överträdelse som sannolikt kommer att orsaka skada som är svår att avhjälpa om den lämnas utan åtgärd, se artikel 48 i NHRC-lagen.
([301]) Ett klagomål måste i princip inges inom ett år från överträdelsen, men den nationella människorättskommissionen kan fortfarande besluta att utreda ett klagomål som inges efter den tidsperioden så länge preskriptionstiden enligt straffrätten eller civilrätten inte har löpt ut (artikel 32.1 led 4 i NHRC-lagen).
([302]) T.ex. har den nationella människorättskommissionen tidigare hanterat klagomål och utfärdat rekommendationer avseende olagliga beslag och en överträdelse av kravet att underrätta enskilda personer om beslag (se sidorna 80 och 91 i den nationella människorättskommissionens årsrapport för 2018 som finns på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), liksom olaglig behandling av personuppgifter utförd av polis, åklagarmyndighet och domstolar (se sidorna 157–158 i den nationella människorättskommissionens årsrapport för 2019 som finns på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, samt sida 76 i årsrapporten för 2019 som finns på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

resultatet av ett förfarande inför den nationella människorättskommissionen kan den nationella människorättskommissionens beslut (t.ex. ett beslut om att inte fortsätta undersöka ett klagomål ([303])) och rekommendationer överklagas vid de sydkoreanska domstolarna enligt förvaltningsprocesslagen (se skäl 181) ([304]). Dessutom kan ett förfarande inför den nationella människorättskommissionen ytterligare underlätta tillgången till domstolar, eftersom en enskild person skulle kunna söka vidare prövning gentemot den myndighet som olagligt behandlat hans eller hennes uppgifter. Detta på grundval av den nationella människorättskommissionens slutsatser och i enlighet med de förfaranden som beskrivs i skälen 181–183.

(179) Slutligen finns olika rättsmedel tillgängliga som gör det möjligt för enskilda att åberopa de begränsningar och skyddsåtgärder som beskrivs i avsnitt 3.2.1 för att erhålla prövning ([305]).

(180) När det gäller beslag (även av uppgifter) ges en möjlighet i straffprocesslagen att invända mot eller bestrida verkställigheten av ett domstolsbeslut med ett så kallat ”halvt klagomål”, genom att göra en framställning till den behöriga domstolen med en begäran om att upphäva eller ändra ett beslut som en åklagare eller polis har fattat ([306]).

(181) Mer allmänt kan enskilda personer begära prövning av myndigheters (däribland brottsbekämpande myndigheter) agerande ([307]) eller underlåtelse att agera ([308]) i enlighet med förvaltningsprocesslagen ([309]). Förvaltningsåtgärder anses vara "beslut som kan överklagas" om de direkt påverkar medborgerliga rättigheter och skyldigheter ([310]) och enligt bekräftelse från den sydkoreanska regeringen (avsnitt 2.4.3 i bilaga II) är detta fallet med åtgärder för att samla in personuppgifter, vare sig det sker direkt (t.ex. genom att övervaka kommunikation), genom bindande begäranden om utlämnande (t.ex. riktade till en tjänsteleverantör), eller begäranden om frivilligt samarbete. För att ett klagomål enligt förvaltningsprocesslagen ska kunna tas upp till prövning måste en enskild person ha ett rättsligt intresse av att driva talan ([311]). Enligt högsta domstolens rättspraxis tolkas ”rättsligt intresse” som ett ”rättsligt skyddat intresse”, dvs. ett direkt och specifikt intresse som skyddas av lagar och andra författningar som ligger till grund för förvaltningsbeslut (dvs. inte allmänhetens generella, indirekta och abstrakta intressen) ([312]). Enskilda personer har ett sådant rättsligt intresse vid överträdelse av begränsningar och skyddsåtgärder som är tillämpliga på insamlingen av deras personuppgifter för brottsbekämpande ändamål (enligt särskilda lagar eller PIPA). På grundval av förvaltningsprocesslagen kan en domstol besluta att upphäva eller ändra ett rättsstridigt beslut, avge ett yttrande om ogiltighet (dvs. ett konstaterande om att beslutet inte har någon rättslig verkan eller att det inte existerar i rättsordningen) eller utfärda ett konstaterande om att underlåtelse att agera är rättsstridigt ([313]). Parterna är bundna till en slutlig dom enligt förvaltningsprocesslagen ([314]).

([303]) Om den nationella människorättskommissionen t.ex. undantagsvis inte kan kontrollera visst material eller anläggningar på grund av att det rör sig om statshemligheter som skulle kunna ha en väsentlig inverkan på statens säkerhet eller diplomatiska förbindelser, eller om kontrollen skulle utgöra ett allvarligt hinder för en brottsutredning eller pågående rättegång, och om detta hindrar den nationella människorättskommissionen från att genomföra den undersökning som krävs för att bedöma framställningen, kommer den nationella människorättskommissionen i enlighet med artikel 39 i lagen om den nationella människorättskommissionen att underrätta personen om varför klagomålet avvisades. I detta fall skulle personen kunna överklaga den nationella människorättskommissionens beslut enligt förvaltningsprocesslagen.

([304]) Se t.ex. överdomstolen i Seoul, beslut nr 2007Nu27259 av den 18 april 2008, bekräftad genom högsta domstolens beslut nr 2008Du7854 av den 9 oktober 2008; överdomstolen i Seoul, beslut nr 2017Nu69382 av den 2 februari 2018.

([305]) Se avsnitt 2.4.3 i bilaga II.

([306]) Artikel 417 i straffprocesslagen jämförd med artikel 414.2 i straffprocesslagen. Se även högsta domstolens beslut nr 97Mo66 av den 29 september 1997.

([307]) I förvaltningsprocesslagen hänvisas till en ”bestämmelse”, dvs. utövande av eller vägran att utöva offentlig makt i ett visst fall.

([308]) Enligt förvaltningsprocesslagen avser detta ett förvaltningsorgans långvariga underlåtenhet att fatta ett visst beslut trots en rättslig förpliktelse att göra detta.

([309]) En administrativ prövning kan först inges till administrativa överklagandenämnder som inrättats av vissa myndigheter (t.ex. den nationella underrättelsetjänsten, den nationella människorättskommissionen) eller till den centrala administrativa överklagandenämnd som inrättats inom ramen för kommissionen för medborgerliga rättigheter och bekämpning av korruption (artikel 6 i lagen om administrativa överklaganden och artikel 18.1 i förvaltningsprocesslagen) som en mer informell möjlighet till prövning. Ett anspråk kan dock även inges direkt till de sydkoreanska domstolarna på grundval av förvaltningsprocesslagen.

([310]) Högsta domstolens beslut nr 98Du18435 av den 22 oktober 1999, högsta domstolens beslut nr 99Du1113 av den 8 september 2000 och högsta domstolens beslut nr 2010Du3541 av den 27 september 2012.

([311]) Artiklarna 12, 35 och 36 i förvaltningsprocesslagen. Dessutom ska en begäran om återkallande eller ändring av ett beslut och en begäran om att bekräfta att en underlåtelse att agera är rättsstridig lämnas in inom 90 dagar från den dag personen får kännedom om beslutet eller underlåtelsen och i princip senast ett år efter den dag då beslutet utfärdades eller underlåtelsen inträffade, såvida det inte finns välgrundade skäl (artiklarna 20 och 38.2 i förvaltningsprocesslagen). Begreppet ”välgrundade skäl” har tolkats i vidare bemärkelse av högsta domstolen och kräver en bedömning av huruvida det är socialt godtagbart att tillåta ett sent klagomål mot bakgrund av alla omständigheter i ärendet (högsta domstolens beslut nr 90Nu6521 av den 28 juni 1991). Som bekräftas av den sydkoreanska regeringen i avsnitt 2.4.3 i bilaga II omfattar detta t.ex. (men är inte begränsat till) skäl till förseningen som den berörda parten inte kan hållas ansvarig för (dvs. situationer som ligger utanför klagandens kontroll, t.ex. om han eller hon inte har underrättats om insamlingen av hans eller hennes personuppgifter) eller force majeure (t.ex. naturkatastrof, krig).

([312]) Högsta domstolens beslut nr 2006Du330 av den 26 mars 2006.

([313]) Artiklarna 2 och 4 i förvaltningsprocesslagen.

([314]) Artikel 30.1 i förvaltningsprocesslagen.

(182) Utöver att bestrida statliga åtgärder genom förvaltningsrättsliga tvister kan enskilda personer även inge ett författningsbesvär till författningsdomstolen om överträdelser av deras grundläggande rättigheter på grund av utövande eller underlåtenhet att utöva offentlig makt (med undantag av domstolsbeslut) ([315]). Om andra rättsmedel finns tillgängliga måste dessa först vara uttömda. Enligt författningsdomstolens rättspraxis kan utländska medborgare inge en författningsklagan i den mån deras grundläggande rättigheter erkänns i den sydkoreanska författningen (se förklaringarna i avsnitt 1.1) ([316]). Författningsdomstolen kan ogiltigförklara utövandet av den offentliga makt som orsakade överträdelsen eller bekräfta att en viss underlåtenhet att agera är författningsstridig ([317]). I så fall ska den berörda myndigheten vidta åtgärder för att rätta sig efter domstolens beslut.

(183) Dessutom kan enskilda personer få ersättning för skador vid de sydkoreanska domstolarna. Detta omfattar först och främst möjligheten att begära ersättning för brott mot PIPA som begåtts av brottsbekämpande myndigheter, i enlighet med artikel 39 (se även skäl 135). I allmänhet kan enskilda personer på grundval av lagen om statlig kompensation ansöka om ersättning för skador som offentliga tjänstemän åsamkat dem vid lagstridig myndighetsutövning (se även skäl 135) ([318]).

(184) De mekanismer som beskrivs i skäl 176–183 ger de registrerade effektiva administrativa och rättsliga medel som särskilt gör det möjligt för dem att tillvarata sina rättigheter, bl.a. rätten att få tillgång till sina personuppgifter eller att få dessa uppgifter rättade eller raderade.

3.3 **Sydkoreanska myndigheters åtkomst och användning för ändamål som rör den nationella säkerheten**

(185) Sydkoreas lagstiftning innehåller ett antal begränsningar och skyddsåtgärder avseende tillgången till och användningen av personuppgifter för ändamål som rör den nationella säkerheten, och den föreskriver tillsyns- och prövningsmekanismer som är i linje med de krav som avses i skälen 141–143 i detta beslut. Villkoren för sådan tillgång och de garantier som gäller för utövandet av dessa befogenheter bedöms i detalj i följande avsnitt.

3.3.1 *Rättsliga grunder, begränsningar och skyddsåtgärder*

(186) I Sydkorea tillåts åtkomst till personuppgifter för ändamål som rör den nationella säkerheten på grundval av lagen om integritetsskydd inom kommunikation, lagen om telekomoperatörer och lagen om åtgärder mot terrorism till skydd för medborgare och den allmänna säkerheten (*lagen mot terrorism*) (*Act on Anti-Terrorism for the Protection of Citizens and Public Security*) ([319]). Den nationella underrättelsetjänsten är huvudmyndighet ([320]) med behörighet på området nationell säkerhet ([321]). Vid insamling och användning av personuppgifter ska den

([315]) Artikel 68.1 i lagen om författningsdomstolen. En författningsklagan måste inges inom 90 dagar efter det att en person har fått kännedom om överträdelsen, och inom ett år efter det att den ägt rum. Såsom även förklaras i avsnitt 2.4.3 i bilaga II och med hänsyn till att förfarandet enligt förvaltningsprocesslagen är tillämpligt enligt lagen om författningsdomstolen enligt artikel 40 i lagen om författningsdomstolen kan ett klagomål fortfarande tas upp till prövning om det finns ”välgrundade skäl”, i den tolkning som anges i högsta domstolens rättspraxis som beskrivs i fotnot 312. Om andra rättsmedel först måste uttömmas ska en författningsklagan inges inom 30 dagar efter det slutliga beslutet om ett sådant rättsmedel (artikel 69 i lagen om författningsdomstolen).

([316]) Författningsdomstolens beslut nr 99HeonMa194 av den 29 november 2001.

([317]) Artikel 75.3 i lagen om författningsdomstolen.

([318]) Artikel 2.1 i lagen om statlig kompensation.

([319]) Se avsnitt 3.1 i bilaga II.

([320]) I undantagsfall får även polis och åklagare samla in personuppgifter för ändamål som rör den nationella säkerheten (se fotnot 327 och avsnitt 3.2.1.2 i bilaga II). Dessutom har Sydkoreas militära underrättelsetjänst (försvarets säkerhetskommando, som inrättats under försvarsministeriet) befogenheter på området nationell säkerhet. Som förklaras i avsnitt 3.1 i bilaga II ansvarar den emellertid endast för den militära underrättelsetjänsten och utför endast övervakning av civila när detta är nödvändigt för att utföra dess militära uppgifter. Framför allt kan den endast utreda militär personal, militärens civila anställda, personer i militär utbildning, personer i militärreserv eller rekryteringstjänst och krigsfångar (artikel 1 i lagen om militärdomstolen). Vid insamling av kommunikationsinformation för ändamål som rör den nationella säkerheten omfattas försvarets säkerhetskommando av de begränsningar och skyddsåtgärder som fastställs i lagen om post- och telehemlighet och genomförandedekretet till denna.

([321]) Den nationella underrättelsetjänstens uppdrag är att samla in, sammanställa och sprida information om andra länder (dvs. allmän information om tendenser och utveckling i förhållande till andra länder, eller statliga aktörers verksamhet); underrättelser avseende bekämpning av spionage (däribland militärt och industriellt spionage), terrorism och internationella brottssyndikat; underrättelser om vissa typer av brott som riktas mot allmän och nationell säkerhet (t.ex. inhemskt uppror, utländsk aggression) och underrättelser som rör uppgiften att säkerställa it-säkerhet och förebygga eller motverka cyberattacker och cyberhot (artikel 4.2 i NIS-lagen). Se även avsnitt 3.1 i bilaga II.

nationella underrättelsetjänsten följa relevanta rättsliga krav (däribland PIPA och lagen om post- och telehemlighet) ([322]) och allmänna riktlinjer som utarbetats av presidenten och granskats av parlamentet ([323]). Som en allmän princip måste den nationella underrättelsetjänsten upprätthålla politisk neutralitet och skydda individens frihet och rättigheter ([324]). Dessutom får anställda vid den nationella underrättelsetjänsten inte missbruka sina officiella befogenheter för att tvinga någon institution, organisation eller individ att göra något som de inte är skyldiga att göra (enligt lag) eller hindra någon från att utöva sina rättigheter ([325]).

3.3.1.1 Tillgång till kommunikationsinformation

(187) På grundval av lagen om post- och telehemlighet får de sydkoreanska myndigheterna ([326]) samla in uppgifter om kommunikationsbekräftelse (dvs. datum för telekommunikation, start- och sluttid för dessa, antal utgående och inkommande samtal samt den andra partens abonnentnummer, användningsfrekvens, loggfiler om användningen av telekommunikationstjänster och lokaliseringsuppgifter, se skäl 155) och kommunikationens innehåll (genom kommunikationsbegränsande åtgärder, se skäl 155) för ändamål som rör den nationella säkerheten (vilket fastställs genom den nationella underrättelsetjänstens uppdrag, se fotnot 322). Dessa befogenheter omfattar två typer av information: 1) kommunikation där en eller båda parter är sydkoreanska medborgare ([327]) och 2) kommunikation från a) länder som är fientliga mot Sydkorea, b) utländska organ, grupper eller medborgare som misstänks bedriva verksamhet riktad mot Sydkorea ([328]) eller c) medlemmar i grupper på Koreahalvön som i praktiken inte omfattas av Sydkoreas överhöghet samt paraplyorganisationer till dessa som är baserade i utlandet ([329]). Kommunikation från enskilda personer i EU som överförs från unionen till Sydkorea på grundval av detta beslut kan därför endast samlas in inom ramen för lagen om post- och telehemlighet för ändamål som rör den nationella säkerheten (med förbehåll för de villkor som anges i skälen 188–192) om de är antingen mellan en enskild person i EU och en sydkoreansk medborgare eller – om de uteslutande sker mellan icke-sydkoreanska medborgare – tillhör någon av de tre ovannämnda kategorierna 2 a), b) och c).

(188) I båda scenarier får insamling av uppgifter om kommunikationsbekräftelse endast ske i syfte att förebygga hot mot den nationella säkerheten ([330]), medan kommunikationsbegränsande åtgärder endast får vidtas om det föreligger en allvarlig risk för den nationella säkerheten och insamlingen är nödvändig för att förhindra den ([331]). Dessutom får åtkomst till kommunikationsinnehåll endast ske som en sista utväg, och ansträngningar måste göras för att minimera överträdelser av kommunikationens integritet ([332]) och därigenom säkerställa att det står i proportion till det eftersträvade ändamålet som rör den nationella säkerheten. Insamling av både kommunikationsinnehåll och uppgifter om kommunikationsbekräftelse får endast pågå i högst fyra månader och ska om det eftersträvade målet uppnås under tiden omedelbart upphöra ([333]). Om de relevanta villkoren fortfarande är uppfyllda får perioden förlängas med upp till fyra månader, med tillstånd från en domstol (för de åtgärder som beskrivs i skäl 189) eller presidenten (för de åtgärder som beskrivs i skäl 190) ([334]).

(189) Samma rättssäkerhetsgarantier gäller för insamling av uppgifter om kommunikationsbekräftelse och innehållet i kommunikation ([335]). Om minst en av de personer som är inblandade i kommunikationen är en sydkoreansk medborgare måste underrättelsetjänsten inge en skriftlig begäran till överåklagarmyndigheten, som i sin tur måste

([322]) Se även artiklarna 14, 22 och 23 i NIS-lagen.
([323]) Artikel 4.2 i NIS-lagen.
([324]) Artiklarna 3.1, 6.2, 11 och 21 i NIS-lagen. Se även reglerna om intressekonflikter, särskilt artiklarna 10 och 12 i NIS-lagen.
([325]) Artikel 13 i NIS-lagen.
([326]) Detta inbegriper underrättelsetjänsterna (dvs. den nationella underrättelsetjänsten och försvarets säkerhetskommando) samt polis/åklagare.
([327]) Artikel 7.1.1 i lagen om post- och telehemlighet.
([328]) Enligt den sydkoreanska regeringens förklaring i fotnot 244 i bilaga II avser detta verksamhet som hotar nationens existens och säkerhet, den demokratiska ordningen eller folkets överlevnad och frihet.
([329]) Artikel 7.1.2 i lagen om post- och telehemlighet.
([330]) Artikel 13-4 i lagen om post- och telehemlighet.
([331]) Artikel 7.1 i lagen om post- och telehemlighet.
([332]) Artikel 3.2 i lagen om post- och telehemlighet. Dessutom måste kommunikationsbegränsande åtgärder omedelbart upphöra när de inte längre är nödvändiga, så att överträdelser av den enskildes kommunikationshemligheter begränsas till ett minimum (artikel 2 i genomförandedekretet till lagen om post- och telehemlighet).
([333]) Artikel 7.2 i lagen om post- och telehemlighet.
([334]) Ansökan om tillstånd att utöka övervakningsåtgärderna ska göras skriftligen med angivande av skälen till att en utökning begärs. Ansökan ska även omfatta underlag (artikel 7.2 i lagen om post- och telehemlighet och artikel 5 i genomförandedekretet till lagen om post- och telehemlighet).
([335]) Se artikel 13-4.2 i lagen om post- och telehemlighet och artikel 37.4 i genomförandedekretet till lagen om post- och telehemlighet, enligt vilka de förfaranden som är tillämpliga på insamling av kommunikationsinnehåll även ska gälla för insamling av uppgifter om kommunikationsbekräftelse. Se även avsnitt 3.2.1.1.1 i bilaga II.

ansöka om ett domstolsbeslut från en chef vid en överdomstol ([336]). I lagen om post- och telehemlighet förtecknas den information som ska anges i begäran till åklagaren, ansökan om domstolsbeslut och själva domstolsbeslutet, vilket särskilt inbegriper motiveringen för begäran och de huvudsakliga skälen till misstanke, underlag samt information om den föreslagna åtgärdens syfte, mål (dvs. den eller de enskilda personer som berörs), omfattning och varaktighet ([337]). Insamling utan domstolsbeslut får endast ske om det rör sig om en konspirationshandling som hotar den nationella säkerheten och om det föreligger en nödsituation som gör det omöjligt att genomgå ovannämnda förfaranden ([338]). Även i detta fall måste dock en ansökan om ett domstolsbeslut inges omedelbart efter det att åtgärden har vidtagits ([339]). I lagen om post- och telehemlighet fastställs därför tydligt omfattningen och villkoren för dessa typer av insamling, och de underkastas särskilda (förfarandemässiga) skyddsåtgärder (bl.a. förhandsgodkännande från domstol), vilket säkerställer att användningen av sådana åtgärder begränsas till vad som är nödvändigt och proportionerligt. Kravet att tillhandahålla utförlig information i både ansökan om ett domstolsbeslut och i själva domstolsbeslutet utesluter dessutom urskillningslös tillgång.

(190) För kommunikation mellan icke-sydkoreanska medborgare som tillhör en av de tre särskilda kategorier som anges i skäl 187 ska en ansökan lämnas in till direktören för den nationella underrättelsetjänsten, som efter att ha granskat de föreslagna åtgärdernas lämplighet måste begära skriftligt förhandsgodkännande från Sydkoreas president ([340]). Underrättelsetjänstens ansökan ska innehålla samma utförliga information som en ansökan om domstolsbeslut (se skäl 189), framför allt vad avser motiveringen för begäran och de huvudsakliga skälen till misstanke, underlag och information om de föreslagna åtgärdernas syfte, berörd individ eller individer, omfattning och varaktighet ([341]). I nödsituationer ([342]) ska förhandsgodkännande inhämtas från den minister som den berörda underrättelsetjänsten sorterar under, även om underrättelsetjänsten måste ansöka om godkännande från presidenten omedelbart efter det att nödåtgärder har vidtagits ([343]). Även vad gäller insamling av kommunikation mellan uteslutande icke-sydkoreanska medborgare inskränker därför lagen om post- och telehemlighet användningen av detta till vad som är nödvändigt och proportionerligt genom att tydligt begränsa de kategorier av personer som kan bli föremål för sådana åtgärder och genom att fastställa detaljerade kriterier som underrättelsetjänster måste påvisa för att motivera en ansökan om insamling av information. Dessutom utesluter detta återigen möjligheten till urskillningslös tillgång. Även om det inte finns något oberoende förhandsgodkännande för sådana åtgärder garanteras oberoende tillsyn i efterhand genom framför allt nämnden för skydd av personuppgifter och den nationella människorättskommissionen (se t.ex. skälen 199–200).

(191) I lagen om post- och telehemlighet föreskrivs dessutom flera ytterligare skyddsåtgärder som bidrar till efterhandstillsyn och underlättar enskilda personers tillgång till effektiva rättsmedel. För det första föreskrivs olika dokumentations- och rapporteringskrav i lagen om post- och telehemlighet när det gäller alla typer av insamling för ändamål som rör den nationella säkerheten. Framför allt gäller att underrättelsetjänsterna när de begär samarbete med privata operatörer ska tillhandahålla domstolsbeslutet/tillståndet från presidenten eller en kopia av försättsbladet till ett uttalande om nödcensur, som den förpliktade enheten måste förvara i sina register ([344]). Om privata operatörer förpliktas att samarbeta ska både den begärande myndigheten och den berörda operatören föra

([336]) Artiklarna 6.5, 6.8 och 7.1.1 och 7.3 i lagen om post- och telehemlighet jämförda med artikel 7.3–7.4 i genomförandedekretet till lagen om post- och telehemlighet.

([337]) Se artiklarna 7.3 och 6.4 i lagen om post- och telehemlighet (för begäran från underrättelsetjänsten), artikel 4 i genomförandedekretet till lagen om post- och telehemlighet (för åklagarens ansökan) och artiklarna 7.3 och 6.6 i lagen om post- och telehemlighet (för domstolsbeslutet).

([338]) Artikel 8 i lagen om post- och telehemlighet.

([339]) Artiklarna 8.2 och 8.8 i lagen om post- och telehemlighet. Insamlingen måste upphöra omedelbart om domstolstillstånd inte erhålls inom 36 timmar efter det att åtgärderna har vidtagits. Om övervakningen slutförs inom en kort tid och domstolstillstånd utesluts ska chefen för den behöriga överåklagarmyndigheten skicka ett meddelande om nödåtgärd som utarbetats av underrättelsetjänsten till ordföranden för den behöriga domstolen, som på denna grund kan undersöka insamlingens lagenlighet (artikel 8.5 och 8.7 i lagen om post- och telehemlighet). I detta meddelande ska anges syfte, mål, tillämpningsområde, tidsperiod, platsen för genomförandet och övervakningsmetod, samt skälen för att inte ha lämnat in en begäran innan åtgärden genomfördes (artikel 8.6 i lagen om post- och telehemlighet). Mer allmänt får underrättelsetjänster endast vidta nödåtgärder i enlighet med ett ”uttalande om nödcensur/nödavlyssning” och måste föra ett register över sådana åtgärder (artikel 8.4 i lagen om post- och telehemlighet).

([340]) Artikel 8.1, 8.2 i genomförandedekretet till lagen om post- och telehemlighet.

([341]) Artikel 8.3 i genomförandedekretet till lagen om post- och telehemlighet jämförd med artikel 6.4 i lagen om post- och telehemlighet.

([342]) Dvs. när åtgärden gäller en konspirationshandling som hotar den nationella säkerheten och det inte finns tillräckligt med tid för att inhämta godkännande från presidenten, när underlåtenhet att vidta nödåtgärder kan skada den nationella säkerheten (artikel 8.8 i lagen om post- och telehemlighet).

([343]) Artikel 8.9 i lagen om post- och telehemlighet. Insamlingen måste upphöra omedelbart om tillstånd inte erhålls inom 36 timmar från den tidpunkt då ansökan gjordes.

([344]) Artikel 9.2 i lagen om post- och telehemlighet och artikel 12 i genomförandedekretet till lagen om post- och telehemlighet. Se artikel 13 i genomförandedekretet till lagen om post- och telehemlighet om möjligheten att förplikta postkontor och leverantörer av telekommunikationstjänster att samarbeta. Privata operatörer som ombeds lämna ut uppgifter får vägra att göra detta om domstolsbeslutet/tillståndet eller uttalandet om nödcensur avser fel identifierare (t.ex. ett telefonnummer som tillhör en annan person än den identifierade). Under alla omständigheter förbjuds de att lämna ut lösenord som används för telekommunikation (artikel 9.4 i lagen om post- och telehemlighet).

register över åtgärdernas föremål och syfte, samt datum för genomförandet ([345]). Underrättelsetjänsterna ska dessutom lämna rapporter om den information de har samlat in och övervakningens resultat till direktören för den nationella underrättelsetjänsten ([346]).

(192) För det andra måste enskilda personer underrättas om insamlingen av deras uppgifter (uppgifter om bekräftelse av kommunikation eller kommunikationsinnehåll) för ändamål som rör den nationella säkerheten om det gäller kommunikation där minst en av parterna är sydkoreansk medborgare ([347]). Denna underrättelse ska lämnas skriftligen inom 30 dagar från den dag då insamlingen avslutades (detta gäller även när uppgifter inhämtas i enlighet med nödförfarandet) och får endast skjutas upp om och så länge som den skulle äventyra den nationella säkerheten eller skada människors liv och fysiska säkerhet ([348]). Oberoende av en sådan underrättelse kan enskilda personer erhålla prövning på olika sätt, vilket förklaras närmare i avsnitt 3.3.4.

3.3.1.2 Insamling av uppgifter om misstänkta terrorister

(193) Enligt lagen mot terrorism får den nationella underrättelsetjänsten samla in uppgifter om misstänkta terrorister ([349]) i enlighet med de begränsningar och skyddsåtgärder som fastställs i andra lagar ([350]). I synnerhet får den nationella underrättelsetjänsten erhålla kommunikationsuppgifter (på grundval av lagen om post- och telehemlighet) och andra personuppgifter (genom en begäran om frivilligt utlämnande) ([351]). När det gäller insamling av kommunikationsinformation (dvs. kommunikationsinnehåll eller uppgifter om kommunikationsbekräftelse) gäller de begränsningar och skyddsåtgärder som beskrivs i avsnitt 3.3.1.1, däribland kravet på att erhålla ett domstolsbeslut. När det gäller ansökningar om frivilligt utlämnande av andra typer av personuppgifter om misstänkta terrorister måste den nationella underrättelsetjänsten uppfylla kraven i författningen och PIPA avseende nödvändighet och proportionalitet (se skäl 164) ([352]). Personuppgiftsansvariga som tar emot en sådan begäran kan samarbeta frivilligt enligt de villkor som fastställs i PIPA (t.ex. i enlighet med principen om uppgiftsminimering och genom att begränsa påverkan på den enskilda personens integritet) ([353]). I detta fall måste de också uppfylla kravet på att den berörda personen ska underrättas, som följer av meddelande nr 2021-5 (se skäl 166).

([345]) För kommunikationsbegränsande åtgärder måste sådana register bevaras i tre år, se artikel 9.3 i lagen om post- och telehemlighet och artikel 17.2 i genomförandedekretet till lagen om post- och telehemlighet. När det gäller uppgifter om kommunikationsbekräftelse ska underrättelsetjänster föra register över att en begäran om sådana uppgifter gjorts, liksom den skriftliga begäran och den institution som förlitat sig på den (artikel 13.5 och 13-4.3 i lagen om post- och telehemlighet). Leverantörer av telekommunikationstjänster måste bevara registren i sju år och rapportera två gånger per år till ministern för vetenskap och IKT om frekvensen för sådana upplysningar (artikel 9.3 i lagen om post- och telehemlighet jämförd med artikel 13.7 i lagen om post- och telehemlighet och artiklarna 37.4 och 39 i genomförandedekretet till lagen om post- och telehemlighet).

([346]) Artikel 18.3 i genomförandedekretet till lagen om post- och telehemlighet.

([347]) Artiklarna 9-2.3 och 13-4 i lagen om post- och telehemlighet. I underrättelsen ska följande anges: 1) det faktum att informationen har samlats in, 2) det verkställande organet och 3) genomförandeperioden.

([348]) Artikel 9-2.4 i lagen om post- och telehemlighet. I så fall ska underrättelse lämnas inom 30 dagar efter det att skälen för uppskovet inte längre föreligger, se artiklarna 13-4.2 och 9-2.6 i lagen om post- och telehemlighet.

([349]) Dvs. medlemmar i en terroristgrupp (som betecknats som sådan av Förenta nationerna, se artikel 2.2 i lagen mot terrorism), personer som främjar och sprider en terroristgrupps idéer eller taktik, samlar in eller bidrar till finansiering av terrorism eller deltar i annan verksamhet som förbereder, konspirerar, sprider eller uppmuntrar till terrorism, eller personer för vilka det finns starka skäl att misstänka att de har bedrivit sådan verksamhet (artikel 2.3 i lagen mot terrorism). *Terrorism* definieras i artikel 2.1 i lagen mot terrorism som ett agerande som utförs i syfte att hindra utövandet av befogenheter som vilar hos staten, en lokal myndighet eller en utländsk myndighet (däribland internationella organisationer), eller i syfte att tvinga dessa enheter att vidta åtgärder utan någon rättslig skyldighet att göra detta, eller för att hota allmänheten. Sådana handlingar kan t.ex. vara att döda, kidnappa eller ta en person som gisslan; kapa/beslagta, förstöra eller skada ett fartyg eller luftfartyg; använda biokemiska, explosiva eller brandfarliga vapen i syfte att orsaka dödsfall eller allvarlig skada på person eller egendom samt missbruk av nukleära eller radioaktiva material.

([350]) Artikel 9.1 och 9.3 i lagen mot terrorism.

([351]) I lagen mot terrorism hänvisas även till möjligheten att samla in uppgifter om inresa till och utresa från Sydkorea på grundval av immigrationslagen och tullagen, men dessa lagar föreskriver för närvarande inte någon sådan befogenhet (se avsnitt 3.2.2.1 i bilaga II). Under alla omständigheter skulle de i princip inte tillämpas på uppgifter som överförts på grundval av detta beslut, eftersom de normalt gäller uppgifter som samlas in direkt av de sydkoreanska myndigheterna (snarare än tillgång till uppgifter som tidigare överförts från unionen till sydkoreanska personuppgiftsansvariga). Dessutom anges i lagen mot terrorism lagen om finansiella transaktioner som rättslig grund för insamling av information om finansiella transaktioner. Såsom förklaras i fotnot 200 omfattas emellertid inte de typer av uppgifter som kan erhållas på grundval av denna lag av detta beslut. Slutligen föreskrivs det i lagen mot terrorism att den nationella underrättelsetjänsten kan samla in lokaliseringsuppgifter genom ickebindande begäranden. I sådana fall kan leverantörer av lokaliseringsuppgifter frivilligt lämna ut sådana uppgifter enligt de villkor som anges i PIPA (se skäl 193) och i lagen om lokaliseringsuppgifter. Såsom även förklaras i fotnot 17 skulle lokaliseringsuppgifter emellertid inte överföras från unionen till sydkoreanska personuppgiftsansvariga på grundval av detta beslut, utan snarare genereras inom Sydkorea.

([352]) Se avsnitt 3.2.2.2 i bilaga II.

([353]) Se artikel 58.4 i PIPA, enligt vilken personuppgifter ska behandlas i den minsta mån som krävs för att uppnå det avsedda ändamålet, och artikel 3.6 i PIPA där det föreskrivs att personuppgifter ska behandlas på ett sätt som minimerar risken för kränkning av den enskildes integritet. Se även artikel 59 led 2, 3 i PIPA enligt vilken personuppgiftsansvariga förbjuds att lämna ut personuppgifter till tredje part utan tillstånd.

3.3.1.3 Begäran om frivilligt utlämnande av abonnentuppgifter

(194) På grundval av lagen om telekomoperatörer får leverantörer av telekommunikation frivilligt lämna ut abonnentuppgifter (se skäl 163) på begäran av en underrättelsetjänst som har för avsikt att samla in sådana uppgifter för att förhindra ett hot mot den nationella säkerheten ([354]). När det gäller sådana begäranden från den nationella underrättelsetjänsten gäller samma begränsningar (som följer av författningen, PIPA och lagen om telekomoperatörer) som på området brottsbekämpning, såsom anges i skäl 164 ([355]). Leverantörer av telekommunikation är inte skyldiga att efterkomma begäran och kan endast göra det enligt de villkor som anges i PIPA (särskilt i enlighet med principen om uppgiftsminimering och genom att begränsa inverkan på den enskilda personens integritet, se även skäl 193). Samma krav avseende dokumentation och underrättelse till den berörda personen gäller som på det brottsbekämpande området (se skälen 165 och 166).

3.3.2 *Vidare användning av de insamlade uppgifterna*

(195) Behandling av personuppgifter som samlas in av sydkoreanska myndigheter för ändamål som rör den nationella säkerheten omfattas av principerna om ändamålsbegränsning (artikel 3.1–3.2 i PIPA), laglighet och korrekthet vid behandling (artikel 3.1 i PIPA), proportionalitet/uppgiftsminimering (artiklarna 3.1, 3.6 och 58 i PIPA), noggrannhet (artikel 3.3 i PIPA), öppenhet (artikel 3.5 i PIPA), säkerhet (artikel 58.4 i PIPA) och begränsad lagring (artikel 58.4 i PIPA) ([356]). Eventuellt utlämnande av personuppgifter till tredje part (däribland tredje land) kan endast ske i enlighet med dessa principer (i synnerhet ändamålsbegränsning och uppgiftsminimering) efter att ha utvärderat efterlevnaden av principerna om nödvändighet och proportionalitet (artikel 37.2 i författningen) och med beaktande av hur de berörda personernas rättigheter påverkas (artikel 3.6 i PIPA).

(196) När det gäller kommunikationsinnehåll och uppgifter om kommunikationsbekräftelse begränsas i lagen om post- och telehemlighet användningen av sådana uppgifter ytterligare till rättsliga förfaranden, om en part kopplad till kommunikationen förlitar sig på den i en skadeståndstalan, eller sådan användning som tillåts enligt andra lagar ([357]).

3.3.3 *Tillsyn*

(197) I Sydkorea övervakas de nationella säkerhetsmyndigheternas verksamhet av olika organ ([358]).

(198) För det första föreskrivs i lagen mot terrorism särskilda tillsynsmekanismer för terrorismbekämpning, däribland insamling av uppgifter om misstänkta terrorister. Särskilt när det gäller den verkställande makten övervakas terrorismbekämpning av kommissionen för terrorismbekämpning ([359]), som direktören för den nationella underrättelsetjänsten är skyldig att rapportera till avseende utredningar och spårning av misstänkta terrorister för att samla in uppgifter eller material som behövs för att bekämpa terrorism ([360]). Dessutom övervakar ombudet för skydd av de mänskliga rättigheterna specifikt efterlevnaden av de grundläggande rättigheterna vid terrorismbekämpning ([361]). Ombudet för skydd av de mänskliga rättigheterna utses av ordföranden för kommissionen för terrorismbekämpning bland personer som uppfyller de särskilda kvalifikationer som anges i genomförandedekretet till lagen mot terrorism ([362]) för en (förnybar) period på två år. Ombudet för skydd av de mänskliga rättigheterna kan endast avsättas från sitt uppdrag på särskilda, begränsade grunder och när starka skäl föreligger ([363]). Vid utövandet av sin tillsynsfunktion får ombudet för skydd av de mänskliga rättigheterna

([354]) Artikel 83.3 i lagen om telekomoperatörer.
([355]) Se även avsnitt 3.2.3 i bilaga II.
([356]) Se avsnitt 1.2 i bilaga II.
([357]) Artiklarna 5.1–5.2, 12 och 13-5 i lagen om post- och telehemlighet.
([358]) Se avsnitt 3.3 i bilaga II.
([359]) Artikel 5.3 i lagen mot terrorism. Kommissionen leds av premiärministern och består av flera ministrar och chefer för statliga organ, t.ex. utrikesministern, justitieministern, försvarsministern, ministern för inrikesfrågor och säkerhet, direktören för den nationella underrättelsetjänsten och rikspolischefen (artikel 3.1 i genomförandedekretet till lagen mot terrorism).
([360]) Artikel 9.4 i lagen mot terrorism.
([361]) Artikel 7 i lagen mot terrorism.
([362]) Dvs. vara advokat med minst tio års arbetslivserfarenhet, eller ha sakkunskap på området mänskliga rättigheter och tjänstgöra eller ha tjänstgjort (åtminstone) som biträdande professor i minst tio år, eller ha tjänstgjort som högre tjänsteman vid ett statligt organ eller en lokal myndighet, eller ha minst tio års arbetslivserfarenhet på området mänskliga rättigheter, t.ex. vid en icke-statlig organisation (artikel 7.1 i genomförandedekretet till lagen mot terrorism).
([363]) T.ex. om han eller hon åtalas i ett brottmål som rör ämbetets uppgifter eller röjer konfidentiella uppgifter, eller på grund av långvarig psykisk eller fysisk oförmåga (artikel 7.3 i genomförandedekretet till lagen mot terrorism).

utfärda allmänna rekommendationer för att förbättra skyddet av de mänskliga rättigheterna ([364]) och särskilda rekommendationer för korrigerande åtgärder om en kränkning av de mänskliga rättigheterna har konstaterats ([365]). Myndigheter är skyldiga att informera ombudet för skydd av de mänskliga rättigheterna om uppföljningen av dessa rekommendationer ([366]).

(199) För det andra övervakar nämnden för skydd av personuppgifter nationella säkerhetsmyndigheters efterlevnad av dataskyddsregler, vilket omfattar både tillämpliga bestämmelser i PIPA (se skäl 149) och de begränsningar och skyddsåtgärder som gäller för insamling av personuppgifter enligt andra lagar (lagen om post- och telehemlighet, lagen mot terrorism och lagen om telekomoperatörer, se även skäl 171) ([367]). Vid utövandet av denna tillsynsroll kan nämnden för skydd av personuppgifter utnyttja alla sina utredningsbefogenheter och korrigerande befogenheter, såsom beskrivs i detalj i avsnitt 2.4.2.

(200) För det tredje är de nationella säkerhetsmyndigheternas verksamhet föremål för oberoende tillsyn av den nationella människorättskommissionen i enlighet med de förfaranden som beskrivs i skäl 172 ([368]).

(201) För det fjärde sträcker sig revisions- och kontrollstyrelsens tillsynsfunktion också till nationella säkerhetsmyndigheter, även om den nationella underrättelsetjänsten i undantagsfall kan vägra att tillhandahålla vissa uppgifter eller material, dvs. när de utgör statshemligheter och ett offentliggörande skulle ha en allvarlig inverkan på den nationella säkerheten ([369]).

(202) Slutligen utförs den parlamentariska tillsynen av den nationella underrättelsetjänstens verksamhet (genom ett specialiserat underrättelseutskott) ([370]). I lagen om post- och telehemlighet fastställs en särskild tillsynsroll för parlamentet när det gäller användningen av kommunikationsbegränsande åtgärder för ändamål som rör den nationella säkerheten ([371]). Parlamentet får i synnerhet genomföra kontroller på plats av avlyssningsutrustning och kan kräva att både den nationella underrättelsetjänsten och de teleoperatörer som har lämnat ut kommunikationsinnehåll lägger fram en rapport om detta. Parlamentet kan också utföra sina allmänna tillsynsfunktioner (i enlighet med de förfaranden som beskrivs i skäl 174). Enligt NIS-lagen ska direktören för den nationella underrättelsetjänsten utan dröjsmål svara när underrättelseutskottet begär en rapport i en viss fråga ([372]), med särskilda regler för viss särskilt känslig information. Närmare bestämt får direktören för den nationella underrättelsetjänsten endast vägra att svara eller vittna inför kommittén i undantagsfall, dvs. om begäran avser statshemligheter som rör militära eller diplomatiska frågor eller frågor med anknytning till Nordkorea, där ett offentliggörande kan ha en allvarlig inverkan på landets framtid ([373]). I sådana fall kan underrättelseutskottet begära en förklaring från premiärministern, och om ingen förklaring ges inom sju dagar får svaret eller vittnesmålet inte vägras.

3.3.4 *Prövningsmöjligheter*

(203) Även på området nationell säkerhet erbjuds i det sydkoreanska systemet olika (rättsliga) möjligheter att erhålla prövning, däribland skadestånd. Dessa mekanismer ger de registrerade effektiva administrativa och rättsliga medel som särskilt gör det möjligt för dem att tillvarata sina rättigheter, däribland rätten att få tillgång till sina personuppgifter eller att få dessa uppgifter rättade eller raderade.

(204) För det första kan enskilda personer i enlighet med artiklarna 3.5, 4.1, 4.3 och 4.4 i PIPA utöva sin rätt till tillgång, rättelse, radering och upphörande gentemot nationella säkerhetsmyndigheter. I avsnitt 6 i meddelande nr 2021-5 (bilaga I till detta beslut) klargörs vidare hur dessa rättigheter är tillämpliga i samband med behandling

([364]) Artikel 8.1 i genomförandedekretet till lagen mot terrorism.

([365]) Artikel 9.1 i genomförandedekretet till lagen mot terrorism. Ombudet för skydd av de mänskliga rättigheterna beslutar självständigt om antagandet av rekommendationer, men måste rapportera sådana rekommendationer till ordföranden för kommissionen för terrorismbekämpning.

([366]) Artikel 9.2 i genomförandedekretet till lagen mot terrorism. Enligt den sydkoreanska regeringens officiella framställning skulle underlåtenhet att genomföra en rekommendation från ombudet för skydd av de mänskliga rättigheterna lyftas upp till kommissionen för terrorismbekämpning, där premiärministern ingår, även om det hittills inte har förekommit några fall där rekommendationer från ombudet för skydd av de mänskliga rättigheterna inte har genomförts (se avsnitt 3.3.1 i bilaga II).

([367]) Avsnitt 3.3.4 i bilaga II.

([368]) Särskilt när det gäller den nationella underrättelsetjänsten har den nationella människorättskommissionen tidigare genomfört undersökningar på eget initiativ och behandlat ett antal enskilda klagomål. Se t.ex. den nationella människorättskommissionens årsrapport för 2018, s. 128 (finns på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) och den nationella människorättskommissionens årsrapport för 2019, s. 70 (finns på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([369]) Artikel 13.1 i NIS-lagen.

([370]) Artiklarna 36 och 37.1.15 i lagen om parlamentet.

([371]) Artikel 15 i lagen om post- och telehemlighet.

([372]) Artikel 15.2 i NIS-lagen.

([373]) Artikel 17.2 i NIS-lagen. Statshemligheter definieras som (sekretessbelagda) fakta, gods eller kunskap som för att undvika allvarliga nackdelar för den nationella säkerheten inte får lämnas ut till något annat land eller någon annan organisation, och till vilka endast begränsat tillträde är tillåtet. Artikel 13.4 i NIS-lagen.

av uppgifter för ändamål som rör den nationella säkerheten. I synnerhet får en nationell säkerhetsmyndighet endast begränsa eller neka utövandet av rättigheten i den utsträckning och så länge som det är nödvändigt och proportionellt för att skydda ett viktigt syfte i allmänhetens intresse (t.ex. i den mån och så länge som beviljandet av rättigheten skulle äventyra en pågående utredning eller hota den nationella säkerheten), eller om beviljandet av rättigheten kan skada en tredje parts liv eller kropp. Vid åberopande av en sådan begränsning krävs därför en avvägning av individens rättigheter och intressen mot det relevanta allmänintresset, och det får under inga omständigheter påverka rättighetens väsentliga innehåll (artikel 37.2 i författningen). Om begäran avslås eller begränsas ska personen utan dröjsmål underrättas om skälen till detta.

(205) För det andra har enskilda personer rätt att erhålla prövning enligt PIPA om deras uppgifter har behandlats av en nationell säkerhetsmyndighet i strid med PIPA eller begränsningarna och skyddsåtgärderna i andra lagar som reglerar insamlingen av personuppgifter (särskilt lagen om post- och telehemlighet, se skäl 171) ([374]). Denna rätt kan utövas genom ett klagomål till nämnden för skydd av personuppgifter (däribland via integritetstjänsten som drivs av Sydkoreas byrå för internet och säkerhet) ([375]). För att underlätta tillgången till prövning mot sydkoreanska nationella säkerhetsmyndigheter kan dessutom enskilda personer i EU lämna in ett klagomål till nämnden för skydd av personuppgifter via sin nationella dataskyddsmyndighet ([376]). I dessa fall kommer nämnden för skydd av personuppgifter att underrätta personen via den nationella dataskyddsmyndigheten när undersökningen har avslutats (däribland, i tillämpliga fall, information om de korrigerande åtgärder som vidtagits). På grundval av förvaltningsprocesslagen kan enskilda personer dessutom överklaga/bestrida nämndens beslut eller passivitet (se skäl 132).

(206) För det tredje kan enskilda personer inge ett klagomål till ombudet för skydd av de mänskliga rättigheterna avseende överträdelser av deras rätt till integritet eller skydd av personuppgifter i samband med terrorismbekämpning (dvs. enligt lagen mot terrorism) ([377]). Ombudet kan rekommendera korrigerande åtgärder. Eftersom det inte finns några formkrav för anmälningar till ombudet behandlas ett klagomål även om den berörda personen inte kan påvisa att han eller hon faktiskt har lidit skada (t.ex. på grund av påstått olaglig insamling av hans eller hennes uppgifter som utförts av en nationell säkerhetsmyndighet) ([378]). Den berörda myndigheten ska informera ombudet för skydd av de mänskliga rättigheterna om alla åtgärder som vidtas för att genomföra dess rekommendationer.

(207) För det fjärde kan enskilda personer lämna in ett klagomål till den nationella människorättskommissionen om nationella säkerhetsmyndigheters insamling av deras uppgifter och erhålla prövning i enlighet med det förfarande som beskrivs i skäl 178 ([379]).

(208) Slutligen finns det olika rättsmedel ([380]) som gör det möjligt för enskilda att åberopa de begränsningar och skyddsåtgärder som beskrivs i avsnitt 3.3.1 för att erhålla prövning. Framför allt kan enskilda personer bestrida lagenligheten hos nationella säkerhetsmyndigheters åtgärder på grundval av förvaltningsprocesslagen (i enlighet med det förfarande som beskrivs i skäl 181 eller lagen om författningsdomstolen (se skäl 182). Dessutom kan de erhålla skadestånd på grundval av lagen om statlig kompensation (som beskrivs närmare i skäl 183).

4. SLUTSATS

(209) Kommissionen anser att Sydkorea – genom PIPA, de särskilda regler som gäller för vissa sektorer (enligt analysen i avsnitt 2) och de ytterligare skyddsåtgärder som föreskrivs i meddelande nr 2021-5 (bilaga I) – säkerställer en skyddsnivå för personuppgifter, vilka överförts från Europeiska unionen, som väsentligen är likvärdig med den skyddsnivå som garanteras genom förordning (EU) 2016/679.

(210) Kommissionen anser dessutom att det sydkoreanska rättssystemets tillsynsmekanismer och möjligheter till prövning gör att överträdelser mot dataskyddsreglerna som begås av personuppgiftsansvariga i Sydkorea kan identifieras och åtgärdas i praktiken, och dessutom erbjuds de registrerade rättsmedel för att få tillgång till sina personuppgifter. Slutligen går det också att få sådana uppgifter rättade eller raderade.

([374]) Artiklarna 58.4 och 4.5 i PIPA. Se avsnitt 3.4.2 i bilaga II.
([375]) Artiklarna 62 och 63.2 i PIPA.
([376]) Meddelande 2021-5 (avsnitt 6, bilaga I).
([377]) Artikel 8.1 led 2 i genomförandedekretet till lagen mot terrorism.
([378]) Se avsnitt 3.4.1 i bilaga II.
([379]) Den nationella människorättskommissionen mottar t.ex. regelbundet klagomål mot den nationella underrättelsetjänsten, se siffrorna i den nationella människorättskommissionens årsrapport 2019 om antalet mottagna klagomål mellan 2015 och 2019, s. 70 (finns på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Se avsnitt 3.4.4 i bilaga II.

(211) På grundval av tillgängliga uppgifter om den sydkoreanska rättsordningen, bl.a. framställningar, utfästelser och åtaganden från den sydkoreanska regeringen i bilaga II, anser kommissionen att sydkoreanska myndigheters eventuella intrång i de grundläggande rättigheterna för enskilda vilkas personuppgifter överförs från EU till Sydkorea för allmännyttiga ändamål, särskilt i straffrättsliga syften som rör brottsbekämpning och den nationella säkerheten, kommer att vara begränsade till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga, och att det finns ett faktiskt rättsligt skydd mot sådant intrång.

(212) Mot bakgrund av slutsatserna i föreliggande beslut bör det därför beslutas att Sydkorea säkerställer en adekvat skyddsnivå i den mening som avses i artikel 45 i förordning (EU) 2016/679, tolkad mot bakgrund av Europeiska unionens stadga om de grundläggande rättigheterna, för personuppgifter som överförs från Europeiska unionen till Sydkorea, till personuppgiftsansvariga i Sydkorea som omfattas av PIPA, med undantag för religiösa organisationer i den mån de behandlar personuppgifter för missionsverksamhet, politiska partier i den mån de behandlar personuppgifter i samband med nominering av kandidater och personuppgiftsansvariga som är föremål för tillsyn av kommittén för finanstjänster för behandling av personlig kreditinformation enligt lagen om kreditinformation, i den mån de behandlar sådana uppgifter.

5. EFFEKTERNA AV DETTA BESLUT OCH DATASKYDDSMYNDIGHETERNAS ÅTGÄRDER

(213) Medlemsstaterna och deras organ åläggs att vidta erforderliga åtgärder för att efterleva rättsakter från unionens institutioner, eftersom dessa antas vara giltiga och därmed ha rättsverkan så länge de inte har återkallats, upphävts enligt en talan om ogiltigförklaring eller till följd av en begäran om förhandsavgörande eller invändning om rättsstridighet.

(214) Ett beslut om adekvat skyddsnivå som antas av kommissionen enligt artikel 45.3 i förordning (EU) 2016/679 är följaktligen bindande för alla organ i medlemsstaterna som det riktar sig till, också för deras oberoende tillsynsmyndigheter. I synnerhet får överföringar från personuppgiftsansvariga eller personuppgiftsbiträden i Europeiska unionen till personuppgiftsansvariga i Sydkorea äga rum utan ytterligare tillstånd.

(215) Det bör erinras om att enligt artikel 58.5 i förordning (EU) 2016/679, och såsom domstolen förklarade i Schrems-domen ([381]), ska en nationell dataskyddsmyndighet, även vid klagomål, ifrågasätta huruvida ett kommissionsbeslut om adekvat skyddsnivå är förenligt med den enskildas grundläggande rätt till integritet och skydd av personuppgifter och därför måste den nationella lagstiftningen innehålla ett rättsmedel för att framföra dessa invändningar till en nationell domstol som kan vara skyldig att begära ett förhandsavgörande från EU-domstolen ([382]).

6. GILTIGHETSTID OCH FÖRLÄNGNING AV DETTA BESLUT

(216) Enligt domstolens rättspraxis ([383]), och som erkänts i artikel 45.4 i förordning (EU) 2016/679, bör kommissionen fortlöpande övervaka relevant utveckling i tredjelandet efter antagandet av ett beslut om adekvat skyddsnivå för att bedöma huruvida tredjelandet fortfarande säkerställer en väsentligen likvärdig skyddsnivå. En sådan kontroll krävs i alla händelser när kommissionen får information som ger upphov till motiverat tvivel i detta hänseende.

(217) Därför bör kommissionen fortlöpande övervaka läget i Sydkorea i fråga om regelverk och praxis rörande behandlingen av personuppgifter enligt definitionen i detta beslut, även de sydkoreanska myndigheternas efterlevnad av framställningarna, utfästelserna och åtagandena i bilaga II. För att underlätta detta förfarande uppmanas sydkoreanska myndigheter att underrätta kommissionen om all väsentlig utveckling som är relevant för detta beslut, rörande näringsidkares och myndigheters behandling av personuppgifter liksom de begränsningar och skyddsåtgärder som gäller myndigheters tillgång till personuppgifter.

([381]) Schrems-målet, punkt 65.

([382]) Schrems-målet, punkt 65: ”Det ankommer härvidlag på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för den nationella tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar som den anser att det finns fog för, så att nationella domstolar, för det fall att de delar myndighetens tvivel angående kommissionsbeslutets giltighet, kan hänskjuta en begäran om förhandsavgörande för att pröva detta besluts giltighet.”

([383]) Schrems-målet, punkt 76.

(218) För att kommissionen ska kunna utföra sin övervakningsfunktion på ett effektivt sätt bör medlemsstaterna dessutom informera kommissionen om alla relevanta åtgärder som vidtas av de nationella dataskyddsmyndigheterna, särskilt när det gäller förfrågningar eller klagomål från registrerade i EU om överföring av personuppgifter från Europeiska unionen till personuppgiftsansvariga i Sydkorea. Kommissionen bör även underrättas om eventuella indikationer på att åtgärder som vidtas av sydkoreanska myndigheter med ansvar för att förebygga, utreda, avslöja eller lagföra brott, eller med hänvisning till den nationella säkerheten, däribland eventuella tillsynsorgan, inte kan garantera den erforderliga skyddsnivån.

(219) Vid tillämpningen av artikel 45.3 i förordning (EU) 2016/679 ([384]), och då den skyddsnivå som åstadkoms av den sydkoreanska rättsordningen kan bli föremål för ändringar, bör kommissionen, efter antagandet av detta beslut, regelbundet ser över huruvida de konstateranden om adekvat skyddsnivå som säkerställs av Sydkorea fortfarande är sakligt och rättsligt motiverade.

(220) Därför bör detta beslut bli föremål för en första översyn inom tre år efter ikraftträdandet. Efter den första översynen, och beroende på resultatet av denna, kommer kommissionen att i nära samråd med den kommitté som inrättats enligt artikel 93.1 i förordning (EU) 2016/679 avgöra om treårscykeln bör bibehållas. Under alla omständigheter bör efterföljande översyn ske minst vart fjärde år ([385]). Översynen bör omfatta alla aspekter av tillämpningen av detta beslut, i synnerhet tillämpningen av de ytterligare skyddsåtgärder som anges i bilaga I till detta beslut (med särskild uppmärksamhet på det skydd som erbjuds i fall av vidare överföring), utveckling av rättspraxis på området, reglerna om behandling av pseudonymiserade uppgifter för statistik, vetenskaplig forskning eller arkiveringsändamål i allmänhetens intresse samt tillämpningen av undantagen enligt artikel 28.7 i PIPA, effektiviteten hos utövandet av enskildas rättigheter (bl.a. inför den nyligen reformerade nämnden för skydd av personuppgifter) och tillämpningen av undantag från dessa rättigheter, tillämpningen av de partiella undantagen enligt PIPA, samt begränsningar och skyddsåtgärder avseende myndigheters tillgång till uppgifter (enligt bilaga II till detta beslut), bl.a. samarbetet mellan nämnden för skydd av personuppgifter och dataskyddsmyndigheter i EU rörande klagomål från enskilda personer. Den bör även omfatta det faktiska utövandet och verkställigheten, både avseende PIPA och på området brottsbekämpning och nationell säkerhet (särskilt vad gäller nämnden för skydd av personuppgifter och den nationella människorättskommissionen).

(221) Inför översynen bör kommissionen sammanträda med nämnden för skydd av personuppgifter, om lämpligt tillsammans med andra sydkoreanska myndigheter med ansvar för myndigheters tillgång till uppgifter, samt med berörda tillsynsorgan. Deltagande i mötet bör vara öppet för företrädare för ledamöterna i Europeiska dataskyddsstyrelsen. I samband med översynen bör kommissionen begära att nämnden för skydd av personuppgifter förser den med omfattande information om samtliga aspekter av relevans för konstaterandet om adekvat skyddsnivå, också om begränsningar och skyddsåtgärder avseende myndigheters tillgång till uppgifter ([386]). Kommissionen bör också begära klargöranden om de uppgifter som inkommit till den och som är relevanta för detta beslut, däribland offentliga rapporter från sydkoreanska myndigheter eller andra intressenter i Sydkorea, Europeiska dataskyddsstyrelsen, enskilda dataskyddsmyndigheter, grupper i det civila samhället, rapporter från media eller andra tillgängliga informationskällor.

(222) På grundval av översynen ska kommissionen utarbeta en offentlig rapport som ska överlämnas till Europaparlamentet och rådet.

7. UPPHÄVNING, ÅTERKALLANDE ELLER ÄNDRING AV DETTA BESLUT

(223) Om tillgänglig information, särskilt information från övervakningen av detta beslut eller från Sydkoreas eller medlemsstaternas myndigheter, visar att den skyddsnivå som Sydkorea erbjuder kanske inte längre är adekvat, bör kommissionen informera de behöriga sydkoreanska myndigheterna om detta och begära att lämpliga åtgärder vidtas inom en angiven, rimlig tidsram.

(224) Om de behöriga sydkoreanska myndigheterna vid utgången av den angivna tidsfristen underlåter att vidta dessa åtgärder eller på annat tillfredsställande sätt visar att detta beslut fortfarande bygger på en adekvat skyddsnivå, kommer kommissionen att inleda det förfarande som avses i artikel 93.2 i förordning (EU) 2016/679 i syfte att helt eller delvis upphäva eller återkalla detta beslut.

(225) Alternativt kommer kommissionen att inleda förfarandet i syfte att ändra beslutet, särskilt genom att underställa överföringar av uppgifter ytterligare villkor eller genom att begränsa räckvidden för konstaterandet om adekvat skyddsnivå endast till uppgiftsöverföringar för vilka en adekvat skyddsnivå fortfarande säkerställs.

([384]) Enligt artikel 45.3 i förordning (EU) 2016/679 ska ”[g]enomförandeakten […] inrätta en mekanism för regelbunden översyn, […] som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen.”

([385]) I artikel 45.3 i förordning (EU) 2016/679 föreskrivs att en regelbunden översyn ska äga rum ”minst vart fjärde år”. Se även Europeiska dataskyddsstyrelsen, Adequacy Referential, WP 254 rev 01.

([386]) Se bilaga II till detta beslut.

(226) Kommissionen bör i synnerhet inleda förfarandet för upphävande eller återkallande vid indikationer på att de ytterligare skyddsåtgärder som anges i bilaga I inte efterlevs av näringsidkare som tar emot personuppgifter enligt detta beslut och/eller inte effektivt verkställs, eller att de sydkoreanska myndigheterna inte uppfyller de framställningar, utfästelser och åtaganden som ingår i bilaga II till detta beslut.

(227) Kommissionen bör också överväga att inleda ett förfarande som leder till ändring, upphävande eller återkallande av detta beslut, om behöriga sydkoreanska myndigheter, inom ramen för översynen eller på annat sätt, underlåter att tillhandahålla den information eller de klargöranden som är nödvändiga för bedömningen av skyddsnivån för personuppgifter vilka överförs från EU till Sydkorea och i överensstämmelse med detta beslut. I detta avseende bör kommissionen beakta i vilken utsträckning de relevanta uppgifterna kan erhållas från andra källor.

(228) Vid vederbörligen motiverade och tvingande skäl till skyndsamhet kommer kommissionen att utnyttja möjligheten att, i enlighet med det förfarande som avses i artikel 93.3 i förordning (EU) 2016/679, anta genomförandeakter med omedelbar verkan som upphäver, återkallar eller ändrar beslutet.

8. **SLUTLIGA ÖVERVÄGANDEN**

(229) Europeiska dataskyddsstyrelsen offentliggjorde sitt yttrande ([387]), vilket har beaktats vid utarbetandet av föreliggande beslut.

(230) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats i enlighet med artikel 93.1 i förordning (EU) 2016/679.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Vid tillämpning av artikel 45 i förordning (EU) 2016/679 ska Sydkorea säkerställa en adekvat skyddsnivå för personuppgifter som överförs från Europeiska unionen till enheter i Sydkorea som omfattas av lagen om skydd av personuppgifter , kompletterat med de ytterligare skyddsåtgärder som anges i bilaga I, tillsammans med de officiella framställningar, utfästelser och åtaganden som ingår i bilaga II.

2. Detta beslut omfattar inte personuppgifter som överförs till mottagare som faller inom någon av följande kategorier, i den mån som samtliga eller vissa av ändamålen med behandlingen av personuppgifter motsvarar ett av följande ändamål som förtecknas däri:

a) Religiösa organisationer i den mån de behandlar personuppgifter för missionsverksamhet.

b) Politiska partier i den mån de behandlar personuppgifter i samband med nominering av kandidater.

c) Enheter som är föremål för tillsyn av kommittén för finanstjänster för behandling av personlig kreditinformation enligt lagen om kreditinformation, i den mån de behandlar sådana uppgifter.

Artikel 2

Närhelst behöriga myndigheter i medlemsstaterna, i syfte att skydda enskilda personer vad avser behandlingen av deras personuppgifter, utövar sina befogenheter enligt artikel 58 i förordning (EU) 2016/679 med avseende på uppgiftsöverföringar som omfattas av det tillämpningsområde som anges i artikel 1 i detta beslut, ska den berörda medlemsstaten utan dröjsmål underrätta kommissionen om detta.

Artikel 3

1. Kommissionen ska fortlöpande övervaka tillämpningen av den rättsliga ram som ligger till grund för detta beslut, däribland de villkor enligt vilka vidare överföring genomförs, enskildas rättigheter utövas och sydkoreanska myndigheter har tillgång till uppgifter som överförs på grundval av detta beslut, i syfte att bedöma om Republiken Korea fortsatt säkerställer en adekvat skyddsnivå i den mening som avses i artikel 1.

([387]) Yttrande 32/2021 om Europeiska kommissionens utkast till genomförandebeslut enligt förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Republiken Korea, som finns tillgängligt på följande länk: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Medlemsstaterna och kommissionen ska underrätta varandra om fall i vilka nämnden för skydd av personuppgifter, eller någon annan behörig sydkoreansk myndighet, underlåter att säkerställa efterlevnaden av den rättsliga ram som detta beslut grundar sig på.

3. Medlemsstaterna och kommissionen ska underrätta varandra om varje indikation på att sydkoreanska myndigheters intrång i den enskildes rätt till skydd av sina personuppgifter går utöver vad som är absolut nödvändigt, eller på att det inte finns något effektivt rättsligt skydd mot denna typ av intrång.

4. Inom tre år från och med den dag medlemsstaterna delgivits detta beslut, och därefter åtminstone vart fjärde år, ska kommissionen utvärdera uppgifterna som avses i artikel 1.1 på grundval av all tillgänglig information, även information som tagits emot som ett led i den översyn som genomförs tillsammans med de berörda sydkoreanska myndigheterna.

5. Om kommissionen får indikationer om att en adekvat skyddsnivå inte längre är säkerställd, ska kommissionen underrätta behöriga sydkoreanska myndigheter. Kommissionen kan i den mån det behövs besluta att återkalla, ändra eller upphäva detta beslut eller begränsa dess tillämpningsområde, i enlighet med artikel 45.5 i förordning (EU) 2016/679, bl.a. om den får indikationer om att

a) personuppgiftsansvariga i Sydkorea, som har erhållit personuppgifter från Europeiska unionen i enlighet med detta beslut, inte efterkommer de ytterligare skyddsåtgärder som anges i bilaga I, eller tillsynen eller verkställigheten inte är tillräcklig i detta avseende,

b) de sydkoreanska myndigheterna inte efterlever de framställningar, utfästelser och åtaganden som ingår i bilaga II, även med avseende på villkoren och begränsningarna för insamling av och tillgång till personuppgifter som av sydkoreanska myndigheter överförts i enlighet med detta beslut för ändamål som avser brottsbekämpning eller den nationella säkerheten.

Kommissionen kan också besluta om sådana åtgärder i fall där bristande samarbete från den sydkoreanska regeringens sida hindrar kommissionen från att avgöra huruvida Sydkorea fortsätter att säkerställa en adekvat skyddsnivå.

Artikel 4

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 17 december 2021.

På kommissionens vägnar
Didier REYNDERS
Ledamot av kommissionen

BILAGA I

TILLÄGGSREGLER FÖR TOLKNING OCH TILLÄMPNING AV LAGEN OM SKYDD AV PERSONUPPGIFTER I SAMBAND MED BEHANDLING AV PERSONUPPGIFTER SOM ÖVERFÖRS TILL SYDKOREA

Innehåll

I. **Sammanfattning**

Sydkorea och Europeiska unionen har fört diskussioner om adekvat skyddsnivå, vilket har lett till att Europeiska kommissionen har fastställt att Sydkorea garanterar ett adekvat skydd av personuppgifter i enlighet med artikel 45 i den allmänna dataskyddsförordningen.

I detta sammanhang antog nämnden för skydd av personuppgifter denna anmälan på grundval av artikel 5 (statens förpliktelser osv.) och artikel 14 (Internationellt samarbete) ([1]) i lagen om skydd av personuppgifter (*personal information protection act*, PIPA) för att klargöra tolkningen, tillämpningen och verkställigheten av vissa bestämmelser i lagen, däribland i fråga om behandling av personuppgifter som överförs till Sydkorea på grundval av EU:s beslut om adekvat skyddsnivå.

Eftersom denna anmälan har status som ett förvaltningsbeslut som den behöriga förvaltningsorganet upprättar och tillkännager för att förtydliga normerna för tolkning, tillämpning och tillämpning av lagen om skydd av personuppgifter inom Sydkoreas rättssystem har den rättsligt bindande verkan för personuppgiftsansvariga i den meningen att varje överträdelse av denna anmälan kan betraktas som en överträdelse av de relevanta bestämmelserna i PIPA. Om personliga rättigheter och intressen kränks på grund av en överträdelse av denna anmälan har de berörda personerna dessutom rätt att erhålla prövning via nämnden för skydd av personuppgifter eller domstolen.

Om den personuppgiftsansvarige som behandlar de personuppgifter som överförs till Sydkorea i enlighet med EU:s beslut om adekvat skyddsnivå underlåter att vidta åtgärder i enlighet med denna anmälan kommer det att anses ”att det finns betydande skäl att anse att en överträdelse med avseende på personuppgifter har ägt rum och att underlåtenhet att vidta åtgärder sannolikt kan orsaka skada som är svår att avhjälpa”, i enlighet med artikel 64.1 och 64.2 i lagen. I sådana fall får nämnden för skydd av personuppgifter eller därtill hörande centrala förvaltningsorgan ålägga den personuppgiftsansvarige att vidta korrigerande åtgärder osv. enligt det tillstånd som beviljas i denna

([1]) Enligt artikel 14 i lagen om skydd av personuppgifter har den sydkoreanska regeringen befogenhet att fastställa strategier för att förbättra skyddet av personuppgifter i den internationella miljön och för att förhindra att de registrerades rättigheter kränks på grund av gränsöverskridande överföring av personuppgifter.

bestämmelse och beroende på den specifika lagöverträdelsen kan även motsvarande straff (påföljder, administrativa sanktionsavgifter osv.) åläggas.

II. **Definition av termer**

Följande är definitioner av termer som används i denna bestämmelse:

(i) *lag*: Lagen om skydd av personuppgifter (lag nr 16930, ändrad den 4 februari 2020 och verkställd den 5 augusti 2020).

(ii) *presidentdekret*: Genomförandedekretet till lagen om skydd av personuppgifter (presidentdekret nr 30509, den 3 mars 2020, om ändring av andra lagar).

(iii) *den registrerade*: En person som genom de uppgifter som behandlas kan identifieras som föremål för dessa uppgifter.

(iv) *personuppgiftsansvarig*: En offentlig institution, juridisk person, organisation, enskild person osv. som direkt eller indirekt behandlar personuppgifter som en del av sin verksamhet.

(v) *EU*: EU (i slutet av februari 202027 medlemsländer [2], vilket inkluderar Belgien, Tyskland, Frankrike, Italien, Luxemburg, Nederländerna, Danmark, Irland, Grekland, Portugal, Spanien, Österrike, Finland, Sverige, Cypern, Tjeckien, Estland, Ungern, Lettland, Litauen, Malta, Polen, Slovakien, Slovenien, Rumänien, Bulgarien och Kroatien) samt länder som är associerade till EU genom EES-avtalet (Island, Liechtenstein, Norge).

(vi) *dataskyddsförordningen*: EU:s allmänna lagstiftning om skydd av personuppgifter, den allmänna dataskyddsförordningen (förordning (EU) 2016/679).

(vii) *beslut om adekvat skyddsnivå*: Enligt artikel 45.3 i den allmänna dataskyddsförordningen har Europeiska kommissionen beslutat att ett tredjeland, ett tredjelands territorium, ett eller flera områden eller en internationell organisation garanterar ett adekvat skydd av personuppgifter.

III. **Tilläggsregler**

1. **Begränsning av användning som går utöver ändamålet och tillhandahållande av personuppgifter (artiklarna 3, 15 och 18 i lagen)**

<Lagen om skydd av personuppgifter

(Lag nr 16930, delvis ändrad den 4 februari 2020)>

Artikel 3 (Principer för skydd av personuppgifter) 1. Den personuppgiftsansvarige ska uttryckligen ange de ändamål för vilka personuppgifter behandlas och samla in personuppgifter på ett lagligt och korrekt sätt i den minsta mån som krävs för dessa ändamål.

2. Den personuppgiftsansvarige ska behandla personuppgifter på ett lämpligt sätt som är nödvändigt för de ändamål för vilka personuppgifterna behandlas och får inte använda dem utöver dessa ändamål.

Artikel 15 (Insamling och användning av personuppgifter) 1. Den personuppgiftsansvarige får samla in personuppgifter under någon av följande omständigheter och använda dem inom det tillämpningsområde för vilket uppgifterna insamlades:

1. Om samtycke erhålls från en registrerad.

2. Om det finns särskilda bestämmelser enligt lag eller om det krävs för att uppfylla rättsliga skyldigheter.

3. Om det krävs för att en offentlig institution ska kunna fullgöra uppgifter som omfattas av dess behörighet enligt lagstiftning osv.

4. Om det är ett obligatoriskt krav för att genomföra och fullgöra ett avtal med en registrerad.

[2] Till dess att övergångsperioden löper ut omfattar detta även Förenade kungariket i enlighet med artiklarna 126, 127 och 132 i avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen (2019/C 384 I/01).

5. Om det anses vara uppenbart nödvändigt för att skydda den registrerades eller tredje mans liv, kropp eller egendomsintressen mot överhängande fara om den registrerade eller hans eller hennes rättsliga företrädare inte kan uttrycka sin avsikt, eller om förhandsgodkännande inte kan erhållas på grund av okända adresser osv.

6. Om det är nödvändigt för att uppnå en personuppgiftsansvarigs berättigade intresse, när detta är uppenbart överordnat den registrerades rättigheter. I sådana fall ska behandling tillåtas endast i den mån behandlingen i väsentlig utsträckning har samband med den personuppgiftsansvariges berättigade intressen och inte går utöver ett rimligt tillämpningsområde.

Artikel 18 (Begränsning av användning som går utöver ändamålet och tillhandahållande av personuppgifter)
1. En personuppgiftsansvarig får inte använda personuppgifter utöver det tillämpningsområde som anges i artiklarna 15.1 samt 39-3.1 och 39-3.2 eller tillhandahålla dem till tredje part utöver det tillämpningsområde som anges i artikel 17.1 och 17.3.

2. Utan hinder av vad som anges i punkt 1 får en personuppgiftsansvarig använda personuppgifter eller tillhandahålla dem till en tredje part för andra ändamål om något av följande stycken är tillämpliga, såvida det inte är sannolikt att detta skulle utgöra en otillbörlig överträdelse av den registrerades eller tredje mans intressen. Leverantörer av informations- och kommunikationstjänster (enligt artikel 2.1.3 i lagen om främjande av användning av nätverk för information och kommunikation och om skydd av information osv.; nedan gäller samma definition) som behandlar användares personuppgifter (enligt artikel 2.1.4 i lagen om främjande av användning av nätverk för information och kommunikation och om skydd av information osv.; nedan gäller samma definition) omfattas endast av styckena 1 och 2, och styckena 5–9 är endast tillämpliga på offentliga institutioner.

1. Om ytterligare samtycke erhålls från den registrerade.

2. Om det finns andra särskilda bestämmelser i lagstiftningen.

3. Om det anses vara uppenbart nödvändigt för att skydda den registrerades eller tredje mans liv, kropp eller egendomsintressen mot överhängande fara om den registrerade eller hans eller hennes rättsliga företrädare inte kan uttrycka sin avsikt, eller om förhandsgodkännande inte kan erhållas på grund av okända adresser.

4. Struken <genom lag nr 16930 av den 4 februari 2020>.

5. Om det är omöjligt att utföra uppgifter som omfattas av dess behörighet enligt andra rättsakter såvida inte den personuppgiftsansvarige använder personuppgifter för andra ändamål än det avsedda, eller tillhandahåller dem till en tredje part, och omfattas av överläggning och resolution i nämnden.

6. Om personuppgifter måste tillhandahållas en utländsk regering eller internationell organisation för att genomföra ett fördrag eller annan internationell konvention.

7. Om det är nödvändigt för utredning av brott, åtal och lagföring.

8. Om det är nödvändigt för att en domstol ska kunna genomföra rättegångsrelaterade uppgifter.

9. Om det är nödvändigt för verkställighet av straff, övervakning och frihetsberövande.

3. och 4. utelämnas.

5. Om en personuppgiftsansvarig tillhandahåller personuppgifter till en tredje part för andra ändamål än de som avses i punkt 2 ska den personuppgiftsansvarige begära att mottagaren av personuppgifterna begränsar ändamålet med och metoden för användningen och andra nödvändiga frågor, eller förbereder nödvändiga skyddsåtgärder för att säkerställa personuppgifternas säkerhet. I sådana fall ska den person som mottar en sådan begäran vidta nödvändiga åtgärder för att garantera personuppgifternas säkerhet.

i) I artikel 3.1 och 3.2 i lagen föreskrivs principen att den personuppgiftsansvarige endast ska samla in den minsta mängd personuppgifter som krävs för ändamålet med behandlingen av personuppgifterna på ett lagenligt sätt och inte bör använda den för andra ändamål än det avsedda ([3]).

ii) Enligt denna princip föreskrivs det i artikel 15.1 i lagen att när en personuppgiftsansvarig samlar in personuppgifter får personuppgifter användas inom ramen för ändamålet med insamlingen, och i artikel 18.1 föreskrivs att personuppgifter inte får användas utöver ändamålet med insamlingen eller tillhandahållas en tredje part.

([3]) Eftersom dessa bestämmelser innehåller allmänna principer för all behandling av personuppgifter, inbegripet när sådan behandling specifikt regleras i andra rättsakter, gäller förtydligandena i detta avsnitt även när personuppgifter behandlas på grundval av andra lagar (se t.ex. artikel 15.1 i lagen om kreditinformation, där det särskilt hänvisas till dessa bestämmelser).

iii) Även om personuppgifter får användas för andra ändamål än de avsedda eller tillhandahållas en tredje part i de undantagsfall ([4]) som beskrivs i bestämmelserna i artikel 18.2 i lagen, måste det begäras att ändamålet med eller metoden för användningen begränsas så att personuppgifter kan behandlas på ett säkert sätt i enlighet med punkt 5, eller att åtgärder vidtas som är nödvändiga för att garantera säkerheten för personuppgifter.

iv) Ovanstående bestämmelser ska tillämpas lika på behandlingen av alla personuppgifter som tas emot inom Sydkoreas jurisdiktion från ett tredjeland, oberoende av den registrerades nationalitet.

v) Om en personuppgiftsansvarig i EU t.ex. överför personuppgifter till en sydkoreansk personuppgiftsansvarig i enlighet med Europeiska kommissionens beslut om adekvat skyddsnivå ska ändamålet med att den personuppgiftsansvarige i EU överför personuppgifterna anses vara ändamålet med att den personuppgiftsansvarige i Sydkorea samlar in personuppgifter, och i sådana fall får den personuppgiftsansvarige i Sydkorea endast använda personuppgifterna eller tillhandahålla dem till en tredje part inom ramen för ändamålet med insamlingen, förutom i de undantagsfall som beskrivs i artikel 18.2 i lagen.

2. **Begränsning av vidareöverföring av personuppgifter (artiklarna 17.3, 17.4 och 18 i lagen)**

<Lagen om skydd av personuppgifter

(Lag nr 16930, delvis ändrad den 4 februari 2020)>

Artikel 17 (Tillhandahållande av personuppgifter) 1. Utelämnas.

2. En personuppgiftsansvarig ska informera en registrerad om följande när samtycke erhålls enligt punkt 1.1. Detsamma gäller när något av följande ändras:

1. Mottagaren av personuppgifter.

2. Det ändamål för vilket mottagaren av personuppgifter använder sådana uppgifter.

3. Beskrivning av de personuppgifter som ska tillhandahållas.

4. Den period under vilken mottagaren behåller och använder personlig information.

5. Det faktum att den registrerade har rätt att neka samtycke och eventuella nackdelar till följd av vägran att ge sitt samtycke.

3. En personuppgiftsansvarig ska informera en registrerad om de frågor som avses i punkt 2 och inhämta den registrerades samtycke för att lämna personuppgifter till en tredje part utomlands. En personuppgiftsansvarig får inte ingå avtal om gränsöverskridande överföring av personuppgifter i strid med denna lag.

4. En personuppgiftsansvarig får tillhandahålla personuppgifter utan samtycke från en registrerad inom det tillämpningsområde som rimligen hänför sig till de ändamål för vilka personuppgifterna ursprungligen samlades in, i enlighet med de frågor som föreskrivs i presidentdekretet och med beaktande av huruvida nackdelar har uppkommit för den registrerade, huruvida nödvändiga åtgärder för att garantera säkerheten (såsom kryptering) har vidtagits, osv.

※ Se sidorna 3, 4 och 5 för artikel 18.

< **Genomförandedekretet till lagen om skydd av personuppgifter**

([Genomförandedatum den 5 februari 2021.] [Presidentdekret nr 30892 av den 4 augusti 2020, om ändring av andra lagar])>

Artikel 14-2 (Standarder för ytterligare användning/tillhandahållande av personuppgifter osv.)

1. Om en personuppgiftsansvarig använder eller tillhandahåller personuppgifter (*ytterligare användning eller tillhandahållande av personuppgifter*) utan den registrerades samtycke i enlighet med artikel 15.3 eller artikel 17.4 i lagen ska den personuppgiftsansvarige beakta följande:

1. Om detta har ett rimligt samband med det ursprungliga ändamålet för vilket personuppgifterna samlades in.

2. Om ytterligare användning eller tillhandahållande av personuppgifter kan förutses mot bakgrund av de omständigheter under vilka personuppgifterna samlades in och behandlingspraxis.

3. Om ytterligare användning eller tillhandahållande av personuppgifter inte utgör en otillbörlig överträdelse av den registrerades intressen.

4. Om de åtgärder som krävs för att garantera säkerhet, såsom pseudonymisering eller kryptering, har vidtagits.

([4]) Leverantörer av informations- och kommunikationstjänster omfattas endast av styckena 1 och 2 i artikel 18.2. Styckena 5–9 är endast tillämpliga på offentliga institutioner.

2. Den personuppgiftsansvarige ska i förväg offentliggöra kriterier för bedömning av de frågor som avses i bestämmelserna i punkt 1 i integritetspolicyn enligt artikel 30.1 i lagen, och den dataskyddsansvarige enligt artikel 31.1 i lagen ska kontrollera om den personuppgiftsansvarige använder eller tillhandahåller ytterligare personuppgifter i enlighet med relevanta standarder.

i) Om personuppgiftsansvariga tillhandahåller personuppgifter till en tredje part utomlands måste de informera registrerade i förväg om alla de frågor som anges i artikel 17.2 i lagen och inhämta deras samtycke, utom i fall som omfattas av punkt 1 eller 2. Inga avtal bör ingås om gränsöverskridande tillhandahållande av personuppgifter i strid med denna akt i följande fall:

(1) Om personuppgifter tillhandahålls inom det tillämpningsområde som rimligen hänför sig till det ursprungliga ändamålet med insamlingen enligt artikel 17.4 i lagen. De fall där denna bestämmelse kan tillämpas är dock begränsade till fall där de standarder för ytterligare användning och tillhandahållande av personuppgifter som föreskrivs i artikel 14-2 i genomförandedekretet är uppfyllda. Dessutom måste personuppgiftsansvariga överväga om tillhandahållandet av personuppgifter kan medföra nackdelar för de registrerade och om de har vidtagit nödvändiga säkerhetsåtgärder, t.ex. kryptering.

(2) Om personuppgifter kan tillhandahållas en tredje part i de undantagsfall som nämns i artikel 18.2 i lagen (se sidorna 3–5). Även i sådana fall kan personuppgifter dock inte tillhandahållas tredje part om det är sannolikt att tillhandahållandet av sådana personuppgifter skulle utgöra en otillbörlig överträdelse av den registrerades eller tredje mans intressen. Dessutom måste den som tillhandahåller personuppgifter begära att mottagaren av personuppgifter begränsar ändamålet med eller metoden för användningen av personuppgifterna eller vidtar de åtgärder som är nödvändiga för att garantera deras säkerhet, så att personuppgifterna kan behandlas på ett säkert sätt.

ii) Om personuppgifter tillhandahålls en tredje part utomlands omfattas de kanske inte av den skyddsnivå som garanteras i Sydkoreas lag om skydd av personuppgifter på grund av skillnader i olika länders system för skydd av personuppgifter. Följaktligen kommer sådana fall att anses vara ”fall som kan medföra nackdelar för den registrerade” som nämns i artikel 17.4 i lagen eller ”fall där den registrerades eller tredje mans intressen otillbörligt överträds” som nämns i artikel 18.2 i lagen och artikel 14-2 i genomförandedekretet till samma lag ([5]). För att uppfylla kraven i dessa bestämmelser måste personuppgiftsansvariga och tredje parter därför uttryckligen säkerställa en skyddsnivå som är likvärdig med lagen, däribland en garanti för den registrerades utövning av sina rättigheter i rättsligt bindande dokument t.ex. avtal, även efter det att personuppgifter överförts utomlands.

3. **Meddelande avseende uppgifter när personuppgifter inte har erhållits från den registrerade (artikel 20 i lagen)**

<Lagen om skydd av personuppgifter

(Lag nr 16930, delvis ändrad den 4 februari 2020)>

Artikel 20 (Anmälan av källor osv. avseende personuppgifter som samlats in från tredje part) 1. När en personuppgiftsansvarig behandlar personuppgifter som samlats in från tredje part, ska personuppgiftsansvarig omedelbart underrätta den registrerade om följande på begäran av den senare:

1. Källan till insamlade personuppgifter.

2. Ändamålet med behandlingen av personuppgifter.

3. Det faktum att den registrerade har rätt att begära att behandlingen av personuppgifter upphör, i enlighet med artikel 37.

2. Utan hinder av punkt 1 ska en personuppgiftsansvarig som uppfyller de kriterier som föreskrivs i presidentdekretet med beaktande av typ och mängd av personuppgifter, antal anställda, försäljningsbelopp osv., vid insamling av personuppgifter från tredje parter och behandling av dessa uppgifter i enlighet med artikel 17.1.1 underrätta den registrerade om de frågor som avses i punkt 1. Detta gäller inte om de uppgifter som samlats in av den personuppgiftsansvarige inte innehåller några personliga uppgifter, t.ex. kontaktinformation, som kan användas för att underrätta den registrerade.

([5]) I enlighet med artikel 18.2.2 i PIPA gäller detta även när personuppgifter lämnas ut till tredje parter utomlands på grundval av bestämmelser i andra rättsakter (t.ex. lagen om kreditinformation).

3. Nödvändiga frågor avseende tidpunkt, metod och förfarande för att meddela den registrerade i enlighet med huvudmeningen i punkt 2 ska föreskrivas i presidentdekret.

4. Punkt 1 och huvudklausulen i punkt 2 ska inte tillämpas under någon av följande omständigheter. Detta är endast fallet om det är uppenbart överordnat de registrerades rättigheter enligt denna lag.

1. Om personuppgifter som är föremål för en begäran om underrättelse ingår i de register med personuppgifter som avses i någon av punkterna i artikel 32.2.

2. Om en sådan underrättelse sannolikt kommer att skada en annan persons liv eller kropp, eller om den orättfärdigt skadar en annan persons egendom och andra intressen.

(i) Om personuppgiftsansvariga tar emot personuppgifter som överförts från EU på grundval av dess beslut om adekvat skyddsnivå ([6]), måste de utan onödigt dröjsmål meddela följande information (1–5) till den registrerade, och under alla omständigheter senast en månad efter överföringen.

(1) Namn och kontaktuppgifter för de personer som överför och tar emot personuppgifterna.

(2) De uppgifter eller kategorier av personuppgifter som överförts.

(3) Ändamålet med insamlingen och användningen av personuppgifter (som fastställts av uppgiftsutföraren i enlighet med punkt 1 i denna anmälan).

(4) Lagringsperiod för personuppgifterna.

(5) Information om den registrerades rättigheter i samband med behandlingen av personuppgifter, metoden och förfarandet för utövandet av rättigheterna och eventuella nackdelar om utövandet av dem medför sådana.

(ii) Om personuppgiftsansvariga tillhandahåller personuppgifterna i i) till en tredje part i Sydkorea eller utomlands, måste de dessutom meddela informationen enligt 1–5 till den registrerade innan personuppgifterna tillhandahålls.

(1) Namn på och kontaktuppgifter för de personer som tillhandahåller och tar emot personuppgifterna.

(2) De uppgifter eller kategorier av personuppgifter som har tillhandahållits.

(3) Det land till vilket personuppgifterna ska tillhandahållas, planerat datum och metod för tillhandahållandet (begränsat till fall där personuppgifter ska tillhandahållas en tredje part utomlands).

(4) Den personuppgiftsansvariges ändamål med och rättsliga grund för tillhandahållandet av personuppgifterna.

(5) Information om den registrerades rättigheter i samband med behandlingen av personuppgifter, metoden och förfarandet för utövandet av rättigheterna och eventuella nackdelar om utövandet av dem medför sådana.

(iii) Personuppgiftsansvariga får inte tillämpa i) eller ii) i något av följande fall (1–4):

(1) Om de personuppgifter som måste anmälas ingår i någon av följande personuppgiftskategorier som anges i artikel 32.2 i lagen, i den mån de intressen som skyddas genom denna bestämmelse är uppenbart överordnade den registrerades rättigheter, och endast så länge som anmälan skulle riskera fullgörandet av de berörda intressena, t.ex. äventyra pågående brottsutredningar eller hota den nationella säkerheten.

(2) Om och så länge som anmälan sannolikt kommer att skada en annan persons liv eller kropp, eller utgöra en otillbörlig överträdelse av en annan persons egendomsintressen, om dessa rättigheter eller intressen är uppenbart överordnade den registrerades rättigheter.

(3) Om den registrerade redan har den information som personuppgiftsansvariga måste meddela enligt i) eller ii).

(4) Om den personuppgiftsansvarige inte har någon kontaktinformation till den registrerade eller om det innebär orimliga ansträngningar att kontakta den registrerade. Detta gäller även i samband med behandling enligt de villkor som anges i avsnitt 3 i PIPA. Vid fastställandet av om det är möjligt att kontakta den registrerade eller om detta innebär alltför stora ansträngningar bör möjligheten att samarbeta med uppgiftsutföraren i EU beaktas.

([6]) Skyldigheterna enligt i), ii) och iii) gäller även när en personuppgiftsansvarig som tar emot personuppgifter från EU på grundval av beslutet om adekvat skyddsnivå behandlar sådan information på grundval av andra lagar, t.ex. lagen om kreditinformation.

4. **Tillämpningsområde för det särskilda undantaget för behandling av pseudonymiserade uppgifter (artiklarna 28-2, 28-3, 28-4, 28-5, 28-6, 28-7, 3 och 58-2 i lagen)**

<Lagen om skydd av personuppgifter

(Lag nr 16930, delvis ändrad den 4 februari 2020)>

Kapitel III Behandling av personuppgifter

AVSNITT 3 Särskilda fall som rör pseudonymiserade uppgifter

Artikel 28-2 (Behandling av pseudonymiserade uppgifter) 1. En personuppgiftsansvarig får behandla pseudonymiserad information utan de registrerades samtycke för statistiska ändamål, forskningsändamål och arkivändamål i allmänhetens intresse osv.

2. En personuppgiftsansvarig ska inte inkludera uppgifter som kan användas för att identifiera en viss person när pseudonymiserade uppgifter tillhandahålls en tredje part i enlighet med punkt 1.

Artikel 28-3 (Begränsning av sammanföring av pseudonymiserade uppgifter) 1. Utan hinder av artikel 28-2 ska sammanföring av pseudonymiserade uppgifter som behandlas av olika personuppgiftsansvariga för statistiska ändamål, forskningsändamål och arkivändamål i allmänhetens intresse osv. utföras av en specialiserad institution som utsetts av skyddsnämnden eller det centrala förvaltningsorganets chef.

2. En personuppgiftsansvarig som avser att lämna ut den kombinerade informationen utanför den organisation som sammanfört uppgifterna ska erhålla godkännande från chefen för den specialiserade institutionen efter att ha omvandlat informationen till pseudonymiserad information eller det format som avses i artikel 58-2.

3. Nödvändiga frågor, däribland förfaranden och metoder för sammanföring enligt punkt 1, standarder och förfaranden för att utnämna eller upphäva utnämningen av en specialiserad institution för ledning och tillsyn samt standarder och förfaranden för export och godkännande enligt punkt 2 ska föreskrivas i presidentdekret.

Artikel 28-4 (Skyldighet att vidta säkerhetsåtgärder för pseudonymiserade uppgifter) 1. När en personuppgiftsansvarig behandlar de pseudonymiserade uppgifterna ska tekniska, organisatoriska och fysiska åtgärder vidtas, t.ex. åtskild lagring och hantering av ytterligare uppgifter som behövs för att återställa dem till ursprungligt skick. Detta kan vara nödvändigt för att garantera säkerheten enligt vad som föreskrivs i presidentdekretet så att personuppgifterna inte kan gå förlorade, stjälas, spridas, förfalskas, ändras eller förstöras.

2. En personuppgiftsansvarig som avser att behandla de pseudonymiserade uppgifterna ska utarbeta och föra register över frågor som föreskrivs i presidentdekretet, däribland ändamålet med behandlingen av de pseudonymiserade uppgifterna och tredje parter som mottar sådana uppgifter vid tillhandahållande av pseudonymiserade uppgifter, för att hantera behandlingen av pseudonymiserade uppgifter.

Artikel 28-5 (Förbjudna åtgärder vid behandling av pseudonymiserade uppgifter) 1. Ingen får behandla de pseudonymiserade uppgifterna i syfte att identifiera en viss person.

2. Om uppgifter som identifierar en viss person framkommer vid behandling av de pseudonymiserade uppgifterna ska personuppgiftsansvarig upphöra med behandlingen av uppgifterna och omedelbart hämta och förstöra dessa uppgifter.

Artikel 28-6 (Införande av administrativa tilläggsavgifter för behandling av pseudonymiserade uppgifter) 1. Om en personuppgiftsansvarig har behandlat uppgifter i syfte att identifiera en särskild person i strid med artikel 28-5.1 får kommissionen ålägga böter som motsvarar högst tre hundradelar av den totala försäljningen. Om ingen försäljning förekommer eller vid svårighet att beräkna försäljningsintäkterna får den personuppgiftsansvarige åläggas böter om högst 400 miljoner won eller tre hundradelar av kapitalbeloppet, om det senare värdet är högre.

2. Artikel 34-2.3–34-2.5 ska i tillämpliga delar gälla för frågor som är nödvändiga för att införa och uppbära administrativa tilläggsavgifter.

Artikel 28-7 (Tillämpningsområde) Artiklarna 20, 21, 27, 34.1, 35–37, 39-3, 39-4, 39-6–39-8 ska inte tillämpas på de pseudonymiserade uppgifterna.

Kapitel I Allmänna bestämmelser

Artikel 3 (Principer för skydd av personuppgifter) 1. Den personuppgiftsansvarige ska uttryckligen ange de ändamål för vilka personuppgifter behandlas och samla in personuppgifter på ett lagligt och korrekt sätt i den minsta mån som krävs för dessa ändamål.

2. Den personuppgiftsansvarige ska behandla personuppgifter på ett lämpligt sätt som är nödvändigt för de ändamål för vilka personuppgifterna behandlas och får inte använda dem utöver dessa ändamål.

3. Den personuppgiftsansvarige ska säkerställa att personuppgifterna är korrekta, fullständiga och aktuella i den utsträckning som krävs för de ändamål för vilka personuppgifterna behandlas.

4. Den personuppgiftsansvarige ska hantera personuppgifter på ett säkert sätt i enlighet med personuppgifternas behandlingsmetoder, kategorier osv., med beaktande av möjligheten att den registrerades rättigheter överträds och hur allvarliga de relevanta riskerna är.

5. Den personuppgiftsansvarige ska offentliggöra sin integritetspolicy och andra frågor som rör behandling av personuppgifter. Dessutom ska den registrerades rättigheter garanteras, t.ex. rätten att få tillgång till sina personuppgifter.

6. Den personuppgiftsansvarige ska behandla personuppgifter på ett sätt som minimerar risken att den registrerades integritet kränks.

7. Om det fortfarande är möjligt att uppfylla ändamålet med att samla in personuppgifter genom att behandla anonymiserade eller pseudonymiserade personuppgifter ska den personuppgiftsansvarige sträva efter att behandla personuppgifter genom anonymisering, där anonymisering är möjlig, eller genom pseudonymisering om det är omöjligt att uppfylla ändamålet med att samla in personuppgifter genom anonymisering.

8. Den personuppgiftsansvarige ska sträva efter att uppnå förtroende hos de registrerade genom att iaktta och utföra sådana uppgifter och skyldigheter som föreskrivs i denna lag och andra relaterade bestämmelser.

Kapitel IX Tilläggsbestämmelser

Artikel 58-2 (Undantag från tillämpning) Denna lag ska inte tillämpas på uppgifter som inte längre identifierar en viss person när de sammanförs med andra uppgifter med rimligt beaktande av tid, kostnad, teknik osv. <Denna artikel har nyligen införts genom lag nr 16930 av den 4 februari 2020.>

i) Enligt kapitel III, avsnitt 3 Särskilda fall avseende pseudonymiserade uppgifter (artiklarna 28-2–28-7) möjliggörs behandling av pseudonymiserade uppgifter utan den registrerades samtycke i syfte att sammanställa statistik, vetenskaplig forskning, bevarande av offentliga register osv. (artikel 28-2), men i dessa fall krävs lämpliga skyddsåtgärder och förbud för att skydda de registrerades rättigheter (artiklarna 28-4 och 28-5), påföljder kan utdömas för överträdelser (artikel 28-6) och vissa skyddsåtgärder som annars skulle vara tillgängliga enligt PIPA är inte tillämpliga (artikel 28-7).

ii) Dessa bestämmelser ska inte tillämpas på fall där pseudonymiserad information behandlas för andra ändamål än att sammanställa statistik, vetenskaplig forskning, bevarande av offentliga register osv. Om exempelvis personuppgifter som gäller en person i EU har överförts till Sydkorea enligt Europeiska kommissionens beslut om adekvat skyddsnivå och är pseudonymiserade för andra ändamål än att sammanställa statistik, vetenskaplig forskning, bevarande av offentliga register osv. ska de särskilda bestämmelserna i kapitel III avsnitt 3 inte tillämpas ([7]).

iii) Om en personuppgiftsansvarig behandlar pseudonymiserade uppgifter för sammanställning av statistik, vetenskaplig forskning, bevarande av offentliga register osv. och om de pseudonymiserade uppgifterna inte har förstörts när det särskilda ändamålet med behandlingen har uppfyllts i enlighet med artikel 37 i författningen och artikel 3 (Principer för skydd av personuppgifter) i lagen, ska den personuppgiftsansvarige anonymisera uppgifterna för att säkerställa att de inte på egen hand eller när de sammanförs med andra uppgifter identifierar en specifik person. Detta så långt som rimligen möjligt med hänsyn till tid, kostnad, teknik osv. i enlighet med artikel 58-2 i PIPA.

5. **Korrigerande åtgärder osv. (artikel 64.1, 64.2 och 64.4 i lagen)**

<Lagen om skydd av personuppgifter

(Lag nr 16930, delvis ändrad den 4 februari 2020)>

Artikel 64 (Korrigerande åtgärder) 1. Om skyddsnämnden anser att det finns betydande skäl att anse att en överträdelse med avseende på personuppgifter har ägt rum och att underlåtenhet att vidta åtgärder sannolikt kan orsaka skada som är svår att avhjälpa kan den beordra att den som brutit mot denna lag (med undantag för centrala förvaltningsorgan, lokala styrelseorgan, parlamentet, domstolen, författningsdomstolen och den nationella valkommittén) ska vidta någon av följande åtgärder:

1. Avbryta överträdelsen med avseende på personuppgifter.

2. Tillfälligt avbryta behandlingen av personuppgifter.

([7]) På samma sätt gäller undantaget i artikel 40-3 i lagen om kreditinformation endast för behandling av pseudonymiserad kreditinformation för sammanställning av statistik, vetenskaplig forskning och bevarande av offentliga register.

3. Andra åtgärder som krävs för att skydda personuppgifter och för att förhindra överträdelser avseende personuppgifter.

2. Om chefen för ett relaterat centralt förvaltningsorgan anser att det finns betydande skäl att anse att en överträdelse av personuppgifter har ägt rum och att underlåtenhet att vidta åtgärder sannolikt kan orsaka skada som är svår att avhjälpa, får han eller hon beordra en personuppgiftsansvarig att vidta någon av de åtgärder som föreskrivs i punkt 1 i enlighet med ett sådan närstående centralt förvaltningsorgans stadgar och behörighet.

4. Om ett centralt förvaltningsorgan, en lokala styrelseorgan, parlamentet, domstolen, författningsdomstolen eller den nationella valkommissionen bryter mot denna lag kan skyddsnämnden rekommendera att chefen för det berörda organet vidtar någon av de åtgärder som föreskrivs i punkt 1. I sådana fall ska myndigheten efter att ha mottagit rekommendationen följa denna, såvida inga exceptionella omständigheter föreligger.

i) Först och främst tolkas enligt domstolens praxis ([8]) ([9]) ”skada som är svår att avhjälpa” som något som skulle kunna skada individens rättigheter eller integritet.

ii) Därmed hänvisar ”betydande skäl att anse att en överträdelse med avseende på personuppgifter har ägt rum och att underlåtenhet att vidta åtgärder sannolikt kan orsaka skada som är svår att avhjälpa” som föreskrivs i artikel 64.1 och 64.2 till fall där det anses att en överträdelse av lagen sannolikt inkräktar på enskilda personers rättigheter och frihet när det gäller personuppgifter. Detta kommer att tillämpas när någon av principerna, rättigheterna och skyldigheterna som ingår i lagen om skydd av personuppgifter kränks ([10]).

iii) Enligt artikel 64.4 i lagen om skydd av personuppgifter är en åtgärd avseende ”en överträdelse av denna lag” en åtgärd beträffande en överträdelse av PIPA.

Ett central förvaltningsorgan osv. får, i egenskap av myndighet bunden till rättsstatsprincipen, inte bryta mot någon lag och är skyldig att vidta en korrigerande åtgärd, bl.a. att omedelbart avbryta åtgärden, och ersätta skador i sådana undantagsfall där en olaglig handling ändå begåtts.

Därmed måste ett centralt förvaltningsorgan osv. även om skyddsnämnden inte ingriper enligt artikel 64.4 i PIPA vidta korrigerande åtgärder mot överträdelser om organet får kännedom om att lagen har åsidosatts.

Framför allt kommer det i regel att vara uppenbart för det centrala förvaltningsorganet osv. att den har åsidosatt lagen om skyddsnämnden har rekommenderat en korrigerande åtgärd. För att motivera varför den anser att en rekommendation från skyddsnämnden inte bör följas måste därför det centrala förvaltningsorganet osv. lägga fram tydliga skäl som bevisar att den inte har åsidosatt lagen. Rekommendationen måste följas om inte skyddsnämnden fastställer att så verkligen inte är fallet.

Mot bakgrund av detta måste de ”exceptionella omständigheterna” i artikel 64.4 i lagen om skydd av personuppgifter strikt begränsas till exceptionella omständigheter där ett centralt förvaltningsorgan osv. lägger fram tydliga skäl som bevisar att ”denna lag faktiskt inte åsidosatts”, t.ex. ”fall där det föreligger exceptionella (faktiska eller rättsliga) omständigheter” som skyddsnämnden inte kände till när den inledningsvis utfärdade sin rekommendation, och skyddsnämnden fastställer att ingen överträdelse har ägt rum.

6. **Tillämpning av PIPA på behandling av personuppgifter för ändamål som rör den nationella säkerheten, däribland utredning av överträdelser och verkställighet i enlighet med PIPA (artiklarna 7-8, 7-9, 58, 3, 4 och 62 i PIPA)**

<Lagen om skydd av personuppgifter

(Lag nr 16930, delvis ändrad den 4 februari 2020)>

Artikel 7-8 (Skyddsnämndens arbete) 1. Skyddsnämnden ska utföra följande arbete: […]

3. Frågor som rör utredning av överträdelser av registrerades rättigheter och de beslut som följer därav.

4. Hantering av klagomål eller korrigeringsförfaranden i samband med behandling av personuppgifter och medling vid tvister om personuppgifter.

[…]

([8]) (Högsta domstolens dom nr 97Da10215, 10222 av den 26 januari 1999) Om information angående den anklagades brottslighet avslöjas via media skulle detta sannolikt orsaka irreparabel psykisk och fysisk skada inte bara för offret, dvs. målsäganden, utan även för personer i hans eller hennes närhet, däribland familjer.

([9]) (Överdomstolen i Seoul, dom i mål nr 2006Na92006 av den 16 januari 2008) Om en ärekränkande artikel offentliggörs, kommer den sannolikt att orsaka den berörda personen allvarlig irreparabel skada.

([10]) Samma principer som i led ii) gäller för artikel 45-4 i lagen om kreditinformation.

Artikel 7-9 (Skyddsnämndens överläggningar och beslut) 1. Skyddsnämnden ska diskutera och lösa följande frågor: […]

5. Frågor som rör tolkningen och tillämpningen av lagstiftningen om skydd av personuppgifter.

[…]

Artikel 58 (Delvis undantag från tillämpningen) 1. Kapitlen III–VII ska inte tillämpas på någon av följande kategorier av personuppgifter:

1. Personuppgifter som samlas in i enlighet med statistiklagen för att behandlas av offentliga institutioner.

2. Personuppgifter som samlas in eller begärs för analys av information som rör den nationella säkerheten.

3. Personuppgifter som behandlas tillfälligt när det är absolut nödvändigt för allmän säkerhet, folkhälsa osv.

4. Personuppgifter som samlas in eller används för egna ändamål vid pressrapportering, missionärsverksamhet som bedrivs av religiösa organisationer samt politiska partiers nominering av kandidater.

[Punkterna 2 och 3 utelämnas.]

4. Vid behandling av personuppgifter enligt punkt 1 ska personuppgiftsansvariga behandla personuppgifterna i den minsta mån som krävs för att uppnå det avsedda ändamålet under den kortaste tidsperiod som krävs. De ska även vidta nödvändiga åtgärder, såsom tekniska, administrativa och fysiska skyddsåtgärder, individuell hantering av klagomål och andra nödvändiga åtgärder för en säker hantering och lämplig behandling av sådana personuppgifter.

Artikel 3 (Principer för skydd av personuppgifter) 1. Den personuppgiftsansvarige ska uttryckligen ange de ändamål för vilka personuppgifter behandlas och samla in personuppgifter på ett lagligt och korrekt sätt i den minsta mån som krävs för dessa ändamål.

2. Den personuppgiftsansvarige ska behandla personuppgifter på ett lämpligt sätt som är nödvändigt för de ändamål för vilka personuppgifterna behandlas och får inte använda dem utöver dessa ändamål.

3. Den personuppgiftsansvarige ska säkerställa att personuppgifterna är korrekta, fullständiga och aktuella i den utsträckning som krävs för de ändamål för vilka personuppgifterna behandlas.

4. Den personuppgiftsansvarige ska hantera personuppgifter på ett säkert sätt i enlighet med personuppgifternas behandlingsmetoder, kategorier osv., med beaktande av möjligheten att den registrerades rättigheter överträds och hur allvarliga de relevanta riskerna är.

5. Den personuppgiftsansvarige ska offentliggöra sin integritetspolicy och andra frågor som rör behandling av personuppgifter. Dessutom ska den registrerades rättigheter garanteras, t.ex. rätten att få tillgång till sina personuppgifter.

6. Den personuppgiftsansvarige ska behandla personuppgifter på ett sätt som minimerar risken att den registrerades integritet kränks.

7. Om det fortfarande är möjligt att uppfylla ändamålet med att samla in personuppgifter genom att behandla anonymiserade eller pseudonymiserade personuppgifter ska den personuppgiftsansvarige sträva efter att behandla personuppgifter genom anonymisering, där anonymisering är möjlig, eller genom pseudonymisering om det är omöjligt att uppfylla ändamålet med att samla in personuppgifter genom anonymisering.

8. Den personuppgiftsansvarige ska sträva efter att uppnå förtroende hos de registrerade genom att iaktta och utföra sådana uppgifter och skyldigheter som föreskrivs i denna lag och andra relaterade bestämmelser.

Artikel 4 (Registrerades rättigheter) Den registrerade har följande rättigheter i samband med att hans eller hennes personuppgifter behandlas:

1. Rätten att bli informerad om behandlingen av sådana personuppgifter.

2. Rätten att avgöra huruvida samtycke ska ges och omfattningen av samtycket när det gäller behandlingen av sådana personuppgifter.

3. Rätten att bekräfta huruvida personuppgifter behandlas eller inte och att begära tillgång (däribland tillhandahållande av kopior; nedan gäller samma definition) till sådana personuppgifter.

4. Rätten att avbryta behandlingen av och begära rättelse, radering och förstöring av sådana personuppgifter.

5. Rätt till lämplig prövning genom ett skyndsamt och rättvist förfarande för skador som uppstår till följd av behandlingen av sådana personuppgifter.

Artikel 62 (Rapportering om överträdelser) 1. Alla vars rättigheter eller intressen åsidosätts i samband med att en personuppgiftsansvarig behandlar deras personuppgifter kan rapportera sådana överträdelser till skyddsnämnden.

2. Skyddsnämnden får utse en specialiserad institution för att på ett effektivt sätt ta emot och hantera dessa rapporter enligt punkt 1, i enlighet med vad som föreskrivs i presidentdekretet. I sådana fall ska denna specialiserade institution inrätta och driva en teletjänstcentral för personuppgiftsbrott (*integritetstjänsten*).

3. Integritetstjänsten ska utföra följande uppgifter:

1. Ta emot rapporter och tillhandahålla samråd om behandling av personuppgifter.

2. Utreda och bekräfta incidenter och inhämta synpunkter från anknutna parter.

3. Uppgifter hänförliga till punkterna 1 och 2.

4. Skyddsnämnden får vid behov sända sin offentliga tjänsteman till den specialiserade institution som utsetts enligt punkt 2 i enlighet med artikel 32-4 i lagen om offentliga tjänstemän för att effektivt undersöka och bekräfta incidenter enligt punkt 3.2.

i) Insamling av personuppgifter för ändamål som rör den nationella säkerheten regleras av särskilda lagar som ger behöriga myndigheter (t.ex. den nationella underrättelsetjänsten) befogenhet att avlyssna kommunikation eller begära utlämnande på vissa villkor och underställt vissa skyddsåtgärder (*nationell säkerhetslagstiftning*). Denna nationella säkerhetslagstiftning omfattar t.ex. lagen om post- och telehemlighet, lagen om åtgärder mot terrorism till skydd för medborgare och den allmänna säkerheten samt lagen om telekomoperatörer. Dessutom måste insamlingen och vidarebehandlingen av personuppgifter uppfylla de villkor som fastställs i PIPA. I detta avseende föreskrivs i artikel 58.1 led 2 i PIPA att kapitlen III–VII inte ska tillämpas på personuppgifter som samlas in eller begärs för analys av information som rör den nationella säkerheten. Detta partiella undantag gäller därför behandling av personuppgifter för ändamål som rör den nationella säkerheten.

Samtidigt gäller kapitel I (Allmänna bestämmelser), kapitel II (Fastställande av säkerhetspolicy för personuppgifter osv.), kapitel VIII (Grupptalan vid överträdelser relaterade till personuppgifter), kapitel IX (Tilläggsbestämmelser) och kapitel X (Bestämmelser om påföljder) i PIPA för behandling av sådan personlig information. Detta inbegriper de allmänna principer för dataskydd som anges i artikel 3 (Principer för skydd av personuppgifter) och de individuella rättigheter som garanteras genom artikel 4 i PIPA (Registrerades rättigheter).

Dessutom föreskrivs i artikel 58.4 i PIPA att sådana uppgifter ska behandlas i den minsta mån som krävs för att uppnå det avsedda ändamålet och under den kortaste tidperiod som krävs. I lagen föreskrivs även att den personuppgiftsansvarige ska vidta nödvändiga åtgärder för att garantera säker uppgiftshantering och lämplig behandling, såsom tekniska, administrativa och fysiska skyddsåtgärder, samt åtgärder för lämplig hantering av enskilda klagomål.

Slutligen gäller bestämmelserna om uppgifterna och befogenheterna för nämnden för skydd av personuppgifter (bl.a. artikel 60–65 PIPA om hantering av klagomål och antagande av rekommendationer och korrigerande åtgärder) samt bestämmelserna om administrativa och straffrättsliga påföljder (artikel 70 ff. i PIPA). Enligt artikel 7-8.1.3 och 7-8.1.4 samt artikel 7-9.1.5 i PIPA omfattar dessa utredningsbefogenheter och korrigerande befogenheter (bl.a. när de utövas i samband med handläggning av klagomål) även eventuella överträdelser av bestämmelser i särskilda lagar där begränsningar och skyddsåtgärder fastställs avseende insamling av personuppgifter, t.ex. lagar om nationell säkerhet. Med hänsyn till kraven i artikel 3.1 i PIPA för laglig och korrekt insamling av personuppgifter utgör en sådan överträdelse en överträdelse av ”denna lag” i den mening som avses i artiklarna 63 och 64, vilket gör det möjligt för nämnden för skydd av personuppgifter att genomföra en utredning och vidta korrigerande åtgärder ([11]). Nämndens utövande av dessa befogenheter kompletterar, men ersätter inte, den nationella människorättskommissionens befogenheter enligt lagen om människorättskommissionen.

Tillämpningen av de grundläggande principerna, rättigheterna och skyldigheterna i PIPA när det gäller behandling av personuppgifter för ändamål som rör den nationella säkerheten återspeglar de garantier som fastställs i författningen för skydd av individens rätt att kontrollera sina egna personuppgifter. Såsom erkänns av författningsdomstolen omfattar detta en individs rätt ([12]) ”att personligen besluta när, till vem eller av vem och i vilken utsträckning hans eller hennes uppgifter kommer att lämnas ut eller användas. Det är en grundläggande rättighet ([13]), […], som finns till för att skydda individens beslutsfrihet från den risk som utvidgningen av statliga funktioner och informations- och kommunikationsteknik medför”. Varje begränsning av denna rättighet, t.ex. när det är nödvändigt för att skydda den nationella säkerheten, kräver en avvägning av individens rättigheter och intressen mot det relevanta allmänintresset och får inte påverka rättighetens väsentliga innehåll (artikel 37.2 i författningen).

([11]) När det gäller korrigerande åtgärder enligt artikel 64, se även avsnitt 5 ovan.
([12]) Författningsdomstolens dom nr 99HunMa513, 2004HunMa190 av den 26 maj 2005.
([13]) Författningsdomstolens dom nr 2003HunMa282 av den 21 juli 2005.

Vid behandling av personuppgifter för ändamål som rör den nationella säkerheten ska den personuppgiftsansvarige (t.ex. den nationella underrättelsetjänsten) därför bland annat utföra följande:

1. Uttryckligen ange de ändamål för vilka personuppgifter behandlas och samla in personuppgifter på ett lagligt och korrekt sätt i den minsta möjliga mån som krävs för detta ändamål (artikel 3.1 i PIPA). Närmare bestämt ska den personuppgiftsansvarige endast samla in och vidarebehandla personuppgifter för att utföra uppgifter enligt relevant lagstiftning, såsom lagen om den nationella underrättelsetjänsten.

2. Behandla personuppgifter i den minsta mån som krävs och under den kortaste tidsperiod som krävs för att uppnå det avsedda ändamålet (artikel 58.4 i PIPA). När ändamålet med behandlingen har uppnåtts ska den personuppgiftsansvarige oåterkalleligt förstöra personuppgifterna såvida inte vidare lagring uttryckligen krävs enligt lag. Om så är fallet ska de relevanta personuppgifterna lagras och hanteras åtskilt från andra personuppgifter, inte användas för något annat ändamål än det som anges i lagen och förstöras när lagringstiden har löpt ut.

3. Behandla personuppgifter på ett lämpligt sätt som är nödvändigt för de ändamål för vilka personuppgifterna behandlas; de får inte användas utöver dessa ändamål (artikel 3.2 i PIPA).

4. Säkerställa att personuppgifterna är korrekta, fullständiga och aktuella i den utsträckning som krävs för de ändamål för vilka personuppgifterna behandlas (artikel 3.3 i PIPA).

5. Hantera personuppgifter på ett säkert sätt i enlighet med personuppgifternas behandlingsmetoder, kategorier osv., med beaktande av möjligheten att den registrerades rättigheter överträds och hur allvarliga de relevanta riskerna är (artikel 3.4 i PIPA).

6. Offentliggöra sin integritetspolicy och andra frågor som rör behandling av personuppgifter (artikel 3.5 i PIPA).

7. Behandla personuppgifter på ett sätt som minimerar risken att den registrerades integritet kränks (artikel 3.6 i PIPA).

ii) I enlighet med artikel 58.4 i PIPA ska den personuppgiftsansvarige (t.ex. myndigheter som är behöriga inom nationell säkerhet såsom den nationella underrättelsetjänsten) vidta nödvändiga åtgärder, t.ex. införa tekniska, förvaltningsmässiga och fysiska skyddsåtgärder för att säkerställa efterlevnad av dessa principer och lämplig behandling av personuppgifter. Detta kan exempelvis omfatta särskilda åtgärder för att garantera säkerheten för personuppgifter, t.ex. begränsningar av tillgången till personuppgifter, tillträdeskontroller, loggar, tillhandahållande av särskild utbildning om hantering av personuppgifter osv.

I enlighet med artiklarna 3.5 och 4 i PIPA ska de registrerade dessutom bland annat ha följande rättigheter när det gäller personuppgifter som behandlas för ändamål som rör den nationella säkerheten:

1. Rätten att få information om huruvida hans eller hennes personuppgifter behandlas samt information om behandlingen och att få tillgång till denna information, bl.a. tillhandahållande av kopior (artikel 4.1 och 4.3 i PIPA).

2. Rätten att avbryta behandlingen och att rätta, radera och förstöra personuppgifter (artikel 4.4 i PIPA).

iii) Den registrerade kan lämna in en begäran om utövande av dessa rättigheter direkt till den personuppgiftsansvarige eller indirekt via skyddsnämnden, och får ge en företrädare tillstånd att göra detta. Om den registrerade lämnar in en begäran ska den personuppgiftsansvarige bevilja rättigheten utan dröjsmål. Den personuppgiftsansvarige kan dock fördröja, begränsa eller neka rättigheten om detta uttryckligen föreskrivs i lagstiftning eller är oundvikligt för att följa andra lagar i den utsträckning och så länge som det är nödvändigt och proportionellt för att skydda ett viktigt syfte i allmänhetens intresse (t.ex. i den mån och så länge som beviljandet av rättigheten skulle äventyra en pågående utredning eller hota den nationella säkerheten), eller om beviljandet av rättigheten kan skada en tredje parts liv eller kropp, eller utgöra obefogat åsidosättande av tredje parts rätt till egendom och andra intressen. Om begäran avslås eller begränsas ska den personuppgiftsansvarige utan dröjsmål underrätta den registrerade om skälen till detta. Den personuppgiftsansvarige ska utarbeta en metod och ett förfarande som gör det möjligt för registrerade att lämna in förfrågningar, och offentliggöra dessa så att de registrerade kan få kännedom om dem.

I enlighet med artikel 58.4 i PIPA (krav på att säkerställa lämplig hantering av enskilda klagomål) och artikel 4.5 i PIPA (rätt till lämplig prövning genom ett skyndsamt och rättvist förfarande för skador som uppstår till följd av behandlingen av personuppgifter) ska de registrerade dessutom ha rätt till prövning. Detta inbegriper rätten att rapportera en påstådd överträdelse till tjänsten som behandlar rapporter om överträdelser avseende personuppgifter (i enlighet med artikel 62.3 i PIPA), inge ett klagomål till nämnden för skydd av personuppgifter i enlighet med artikel 62 i PIPA om överträdelse av rättigheter eller intressen relaterade till en enskilds personuppgifter samt att erhålla rättslig prövning av nämndens beslut eller passivitet enligt förvaltningsprocesslagen (*Administrative Litigation Act*). Dessutom kan registrerade erhålla rättslig prövning enligt förvaltningsprocesslagen om det har förekommit en överträdelse av deras rättigheter eller intressen på grund av en personuppgiftsansvarigs beslut eller underlåtelse (t.ex. olaglig insamling av personuppgifter), eller erhålla skadestånd i enlighet med lagen om statlig kompensation (*State Compensation Act*). Dessa möjligheter till prövning finns både vid eventuella överträdelser av reglerna i särskilda lagar som fastställer begränsningar och skyddsåtgärder avseende insamling av personuppgifter, exempelvis nationell säkerhetslagstiftning, och av PIPA.

En enskild person i EU kan inge ett klagomål till nämnden för skydd av personuppgifter via sin nationella dataskyddsmyndighet och nämnden för skydd av personuppgifter underrättar den enskilde via den nationella dataskyddsmyndigheten efter det att utredningen och den korrigerande åtgärden (i tillämpliga fall) har slutförts.

BILAGA II

18 maj 2021

Didier Reynders, kommissionsledamot med ansvar för rättsliga frågor i Europeiska kommissionen

Ers excellens,

jag välkomnar de konstruktiva diskussionerna mellan Sydkorea och Europeiska kommissionen syftande till att skapa en ram för överföring av personuppgifter från EU till Sydkorea.

På en begäran från Europeiska kommissionen riktad till Sydkoreas regering översänder jag ett bifogat dokument, som härmed ger en översikt över den rättsliga ramen avseende den sydkoreanska regeringens tillgång till information.

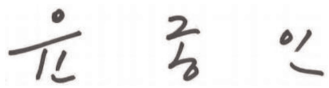
Detta dokument rör många ministerier och byråer inom den sydkoreanska regeringen, och med avseende på innehållet i dokumentet är berörda ministerier och organ (nämnden för skydd av personuppgifter, justitieministeriet, den nationella underrättelsetjänsten, Sydkoreas människorättskommission, nationella centret för terroristbekämpning, Sydkoreas finansunderrättelseenhet) ansvariga för de delar som omfattar deras respektive behörigheter. Nedan återfinns berörda ministerier och byråer samt deras respektive underskrifter.

Nämnden för skydd av personuppgifter tar emot alla förfrågningar rörande detta dokument och kommer att samordna nödvändiga åtgärder mellan berörda ministerier och byråer.

Jag hoppas att detta dokument blir till hjälp i Europeiska kommissionens beslutsfattande.

Jag är mycket tacksam för Era hittillsvarande bidrag i denna fråga.

Högaktningsfullt

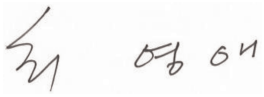


Yoon Jong In
Ordförande för nämnden för skydd av personuppgifter

Detta dokument har utarbetats av nämnden för skydd av personuppgifter och följande berörda ministerier och byråer.

Park Jie Won
Ordförande (direktör), nationella underrättelsetjänsten

Lee Jung Soo
Generaldirektör, justitieministeriet



Choi Young Ae
Ordförande, Sydkoreas människorättskommission

Kim Hyuck Soo
Direktör, nationella centret för terroristbekämpning

Kim, Jeong Kag
Kommissionär, Sydkoreas finansunderrättelseenhet

Rättslig ram för insamling och användning av personuppgifter som utförs av de sydkoreanska myndigheterna för brottsbekämpande ändamål och nationell säkerhet

Följande dokument innehåller en översikt över den rättsliga ramen för insamling och användning av personuppgifter som utförs av de sydkoreanska myndigheterna för brottsbekämpande ändamål och nationens säkerhet (*myndigheters tillgång till uppgifter*), särskilt när det gäller tillgängliga rättsliga grunder, tillämpliga villkor (begränsningar) och skyddsåtgärder, samt oberoende tillsyn och möjligheter till enskild prövning.

1. ALLMÄNNA RÄTTSLIGA PRINCIPER FÖR MYNDIGHETERS TILLGÅNG TILL UPPGIFTER

1.1. Konstitutionell ram

I Sydkoreas författning fastställs rätten till integritet i allmänhet (artikel 17) och rätten till sekretess för korrespondens i synnerhet (artikel 18). Det är statens skyldighet att garantera dessa grundläggande rättigheter ([1]). I författningen föreskrivs vidare att medborgares rättigheter och friheter endast får begränsas genom lag och när det är nödvändigt för den nationella säkerheten eller för upprätthållande av lag och ordning för den allmänna välfärden ([2]). Även när sådana restriktioner införs får de inte påverka frihetens eller rättens väsentliga innehåll ([3]). De sydkoreanska domstolarna har tillämpat dessa bestämmelser i ärenden som rör statligt intrång i privatlivet. Högsta domstolen konstaterade till exempel att övervakningen av civila kränker den grundläggande rätten till integritet och betonade att medborgarna har *rätt till självbestämmande när det gäller personuppgifter* ([4]). I ett annat fall ansåg författningsdomstolen att integritet är en grundläggande rättighet som ger skydd mot statliga ingripanden i och övervakning av medborgarnas privatliv ([5]).

I den sydkoreanska författningen garanteras dessutom att ingen person ska gripas, kvarhållas, genomsökas, förhöras eller få artiklar beslagtagna förutom i de fall som föreskrivs i lag ([6]). Dessutom får husrannsakan och beslag endast genomföras på grundval av en order utfärdad av en domare, på begäran av en åklagare, och med respekt för rättssäkerheten ([7]). I undantagsfall, dvs. om en brottsmisstänkt grips på bar gärning eller om det finns en risk för att en person som misstänks för att ha begått ett brott som leder till fängelsestraff i minst tre år kan undkomma eller förstöra bevis, får utredningsmyndigheterna utföra en husrannsakan eller ett beslag utan domstolsorder; de måste då begära en sådan order i efterhand ([8]). Dessa allmänna principer utvecklas ytterligare i specifika lagar om straffrättsliga förfaranden och skydd av kommunikation (se nedan för en detaljerad översikt).

När det gäller utländska medborgare föreskrivs i författningen att deras status garanteras i enlighet med internationell rätt och internationella fördrag ([9]). Flera internationella avtal som Sydkorea har anslutit sig till garanterar integritetsskydd, t.ex. den internationella konventionen om medborgerliga och politiska rättigheter (artikel 17), konventionen om rättigheter för personer med funktionsnedsättning (artikel 22) och konventionen om barnets rättigheter (artikel 16). Även om det i författningen i princip hänvisas till *medborgarnas* rättigheter har författningsdomstolen dessutom fastställt att även utländska medborgare har grundläggande rättigheter ([10]). Domstolen ansåg särskilt att skyddet av värdighet och en persons människovärde samt rätten att sträva efter lycka är alla människors rättigheter och inte bara

([1]) Artikel 10 i Sydkoreas författning, utfärdad den 17 juli 1948 (författningen).
([2]) Artikel 37.2 i författningen.
([3]) Artikel 37.2 i författningen.
([4]) Sydkoreas högsta domstol, beslut nr 96DA42789 av den 24 juli 1998.
([5]) Författningsdomstolens beslut nr 2002Hun-Ma51 av den 30 oktober 2003. På samma sätt klargjorde författningsdomstolen i beslut nr 99Hun-Ma513 och 2004Hun-Ma190 (konsoliderat) den 26 maj 2005 att *rätten att kontrollera sina egna personuppgifter är en rätt som tillkommer den person som uppgifterna gäller att personligen besluta när, till vem eller av vem, och i vilken utsträckning hans eller hennes uppgifter kommer att lämnas ut eller användas. Det är en grundläggande rättighet, även om den inte anges i författningen, som finns till för att skydda individens beslutsfrihet från den risk som utvidgningen av statliga funktioner och informations- och kommunikationsteknik medför*.
([6]) Artikel 12.1 första meningen i författningen.
([7]) Artiklarna 16 och 12.3 i författningen.
([8]) Artikel 12.3 i författningen.
([9]) Artikel 6.2 i författningen.
([10]) Författningsdomstolens beslut nr 93Hun-MA120 av den 29 december 1994. Se även t.ex. författningsdomstolens beslut nr 2014Hun-Ma346 (31 maj 2018), där domstolen konstaterade en överträdelse av den konstitutionella rätten att erhålla hjälp av en juridisk rådgivare för en sudanesisk medborgare som hölls i förvar på flygplatsen. I ett annat fall konstaterade författningsdomstolen att friheten att välja sin egen lagliga arbetsplats har ett nära samband med rätten att sträva efter lycka samt mänsklig värdighet och människovärde, och att den därför inte är förbehållen enbart medborgare utan även kan garanteras utlänningar som är lagligen anställda i Sydkorea (författningsdomstolens beslut nr 2007Hun-Ma1083 av den 29 september 2011).

medborgarnas ([11]). Domstolen klargjorde också att rätten att bestämma över sina uppgifter anses vara en grundläggande rättighet, grundad på rätten till värdighet och strävan efter lycka och rätten till privatliv ([12]). Även om icke-koreanska medborgares rätt till privatliv hittills inte specifikt har behandlats i rättspraxis är det därför allmänt accepterat bland forskare att artiklarna 12–22 i författningen (vilket inbegriper rätten till integritet och personlig frihet) fastställer *människors rättigheter*.

Slutligen föreskrivs i författningen även rätten att kräva rättvis ersättning från myndigheter ([13]). På grundval av lagen om författningsdomstolen får dessutom varje person vars grundläggande och författningsskyddade rättigheter kränks genom utövandet av offentlig makt (med undantag av domstolsbeslut) inge en författningsklagan till författningsdomstolen ([14]).

1.2. **Allmänna dataskyddsregler**

Den allmänna lagen om dataskydd i Sydkorea, lagen om skydd av personuppgifter (*personal information protection act*, nedan kallad PIPA), gäller både den privata och den offentliga sektorn. När det gäller myndigheter hänvisas i PIPA särskilt till skyldigheten att utforma strategier för att förhindra *missbruk och felaktig användning av personuppgifter, genomgripande övervakning och spårning osv. och att stärka människors värdighet och personliga integritet* ([15]).

Behandlingen av personuppgifter för brottsbekämpande ändamål omfattas av alla krav i PIPA. Detta innebär exempelvis att brottsbekämpande myndigheter måste uppfylla skyldigheterna avseende laglig behandling, dvs. förlita sig på en av de rättsliga grunder som anges i PIPA för insamling, användning eller tillhandahållande av personuppgifter (artiklarna 15–18 i PIPA) samt principerna om ändamålsbegränsning (artikel 3.1 och 3.2 i PIPA), proportionalitet/uppgiftsminimering (artikel 3.1 och 3.6 i PIPA), begränsad lagring av uppgifter (artikel 21 i PIPA), datasäkerhet, bl.a. anmälan av uppgiftsincidenter (artiklarna 3.4, 29 och 34 i PIPA) samt öppenhet (artiklarna 3.1, 3.5, 20, 30 och 32 i PIPA). Särskilda skyddsåtgärder gäller för känslig information (artikel 23 i PIPA). I enlighet med artiklarna 3.5 och 4 i PIPA och artiklarna 35–39-2 i PIPA kan dessutom enskilda personer utöva sin rätt till tillgång, rättelse, radering och upphörande gentemot brottsbekämpande myndigheter.

PIPA är därför fullt ut tillämplig på behandling av personuppgifter för brottsbekämpande ändamål, men innehåller ett undantag när personuppgifter behandlas för ändamål som rör den nationella säkerheten. Enligt artikel 58.1 led 2 i PIPA är artiklarna 15–50 i PIPA inte tillämpliga på personuppgifter som samlas in eller begärs för analys av information som rör den nationella säkerheten ([16]). Omvänt fortsätter kapitel I (Allmänna bestämmelser), kapitel II (Fastställande av säkerhetspolicy för personuppgifter osv.), kapitel VIII (Grupptalan vid överträdelser relaterade till personuppgifter), kapitel IX (Tilläggsbestämmelser) och kapitel X (Bestämmelser om påföljder) i PIPA att gälla. Detta inbegriper de allmänna principer för dataskydd som anges i artikel 3 (Principer för skydd av personuppgifter) och de individuella rättigheter som garanteras genom artikel 4 i PIPA (Registrerades rättigheter). Detta innebär att de viktigaste principerna och rättigheterna garanteras även på detta område. Dessutom föreskrivs i artikel 58.4 i PIPA att sådana uppgifter ska behandlas i den minsta mån som krävs för att uppnå det avsedda ändamålet och under den kortaste tidperiod som krävs. Där föreskrivs även att den personuppgiftsansvarige ska vidta nödvändiga åtgärder för att säkerställa säker uppgiftshantering och lämplig behandling, såsom tekniska, administrativa och fysiska skyddsåtgärder, samt åtgärder för lämplig hantering av enskilda klagomål.

I anmälan nr 2021-1 om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter har nämnden för skydd av personuppgifter (*nämnden för skydd av personuppgifter* eller *nämnden*) ytterligare klargjort hur PIPA är tillämplig på behandling av personuppgifter för ändamål som rör den nationella säkerheten, mot bakgrund av detta partiella undantag ([17]). Detta omfattar i synnerhet enskilda personers rättigheter (tillgång, rättelse, upphörande och radering) och skälen till dessa rättigheter samt begränsningar av eventuella inskränkningar i dem. Enligt anmälan återspeglar tillämpningen av de grundläggande principerna, rättigheterna och skyldigheterna i PIPA när det gäller

([11]) Författningsdomstolens beslut nr 99HeonMa494 av den 29 november 2001.
([12]) Se t.ex. författningsdomstolens beslut nr 99HunMa513.
([13]) Artikel 29.1 i författningen.
([14]) Artikel 68.1 i lagen om författningsdomstolen.
([15]) Artikel 5.1 i PIPA.
([16]) Artikel 58.1 led 2 i PIPA.
([17]) Anmälan nr 2021-1 från nämnden för skydd av personuppgifter om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter, avsnitt III, 6.

behandling av personuppgifter för ändamål som rör den nationella säkerheten de garantier som fastställs i författningen för skydd av individens rätt att kontrollera sina egna personuppgifter. Varje begränsning av denna rättighet, t.ex. när det är nödvändigt för att skydda den nationella säkerheten, kräver en avvägning av individens rättigheter och intressen mot det relevanta allmänintresset och får inte påverka rättighetens väsentliga innehåll (artikel 37.2 i författningen).

2. MYNDIGHETERS TILLGÅNG TILL UPPGIFTER FÖR BROTTSBEKÄMPANDE ÄNDAMÅL

2.1. **Behöriga myndigheter på området brottsbekämpning**

På grundval av straffprocesslagen (*Criminal Procedure Act*), lagen om post- och telehemlighet (*Communications Privacy Protection Act*) och lagen om telekomoperatörer (*Telecommunications Business Act*) får polis, åklagare och domstolar samla in personuppgifter för brottsbekämpande ändamål. I den utsträckning som denna befogenhet även ges till den nationella underrättelsetjänsten enligt lagen om den nationella underrättelsetjänsten måste den följa ovannämnda lagar ([18]). Slutligen utgör lagen om rapportering och användning av specificerad information om finansiella transaktioner (*Act on Reporting and Using Specified Financial Transaction Information*, - *lagen om finansiella transaktioner*) en rättslig grund för finansinstitut att lämna ut information till Sydkoreas finansunderrättelseenhet i syfte att förhindra penningtvätt och finansiering av terrorism. Detta specialiserade organ får i sin tur tillhandahålla sådan information till brottsbekämpande myndigheter. Dessa upplysningskrav gäller dock endast personuppgiftsansvariga som behandlar personlig kreditinformation enligt lagen om kreditinformation och som är föremål för tillsyn av kommissionen för finansiella tjänster. Eftersom behandling av personlig kreditinformation som utförs av sådana personuppgiftsansvariga inte ingår i tillämpningsområdet för beslutet om adekvat skyddsnivå beskrivs de begränsningar och skyddsåtgärder som tillämpas enligt lagen om finansiella transaktioner inte närmare i detta dokument.

2.2. **Rättsliga grunder och begränsningar**

Straffprocesslagen (se 2.2.1), om post- och telehemlighet (se 2.2.2) och lagen om telekomoperatörer (se 2.2.3) ger rättsliga grunder för insamling av personuppgifter för brottsbekämpande ändamål och fastställer tillämpliga begränsningar och skyddsåtgärder.

2.2.1. *Husrannsakan och beslag*

2.2.1.1. Rättslig grund

Åklagare och högre tjänstemän vid kriminalpolisen får endast inspektera föremål, visitera personer eller beslagta artiklar om 1) en person misstänks ha begått ett brott (en brottsmisstänkt), 2) det är nödvändigt för utredningen och 3) de föremål som ska inspekteras, personer som ska visiteras och alla föremål som beslagtas anses ha anknytning till fallet ([19]). På samma sätt får domstolar utföra husrannsakningar och beslagta föremål som ska användas som bevis eller som kan förverkas, så länge sådana föremål eller personer anses ha anknytning till ett enskilt fall ([20]).

2.2.1.2. Begränsningar och skyddsåtgärder

Det är en allmän skyldighet för åklagare och tjänstemän vid kriminalpolisen att respektera den brottsmisstänktes och andra berörda personers mänskliga rättigheter ([21]). Dessutom får obligatoriska åtgärder för att uppnå syftet med undersökningen endast vidtas om det uttryckligen föreskrivs i straffprocesslagen och endast i den mån det är nödvändigt ([22]).

Husrannsakningar, inspektioner eller beslag av poliser eller åklagare som en del av en brottsutredning får endast ske på grundval av en domstolsorder ([23]). Den myndighet som begär en domstolsorder måste lägga fram handlingar som visar att en person är misstänkt för ett brott, att husrannsakan, inspektion eller beslag krävs och att det finns relevanta föremål som ska beslagtas ([24]). Domstolsordern måste bland annat innehålla uppgifter om den brottsmisstänktes namn och brottet, den plats, person eller föremål som ska genomsökas, eller föremål som ska beslagtas, datum för utfärdande samt den faktiska tillämpningsperioden ([25]). På samma sätt måste en domstolsorder inhämtas i förväg när husrannsakan och beslag är en del av pågående domstolsförfaranden och utförs på annat sätt än vid offentlig förhandling ([26]). Den berörda personen och hans eller hennes försvarare underrättas i förväg om husrannsakningen eller beslaget och får närvara när ordern verkställs ([27]).

([18]) Se artikel 3 i NIS-lagen (lag nr 12948) som avser brottsutredningar av vissa brott, t.ex. uppror, revolt och brott med anknytning till nationell säkerhet (t.ex. spionage). De förfaranden för husrannsakan och beslag som anges i straffprocesslagen skulle vara tillämpliga i ett sådant sammanhang, medan om post- och telehemlighet skulle reglera insamlingen av kommunikationsuppgifter (se del 3 om bestämmelserna om tillgång till kommunikation för ändamål som rör den nationella säkerheten).
([19]) Artikel 215.1 och 215.2 i straffprocesslagen.
([20]) Artiklarna 106.1, 107 och 109 i straffprocesslagen.
([21]) Artikel 198.2 i straffprocesslagen.
([22]) Artikel 199.1 i straffprocesslagen.
([23]) Artikel 215.1 och 215.2 i straffprocesslagen.
([24]) Artikel 108.1 i förordningen om straffrättsligt förfarande.
([25]) Artikel 114.1 i straffprocesslagen jämförd med artikel 219 i straffprocesslagen.
([26]) Artikel 113 i straffprocesslagen.
([27]) Artiklarna 121 och 122 i straffprocesslagen.

Vid husrannsakan eller beslag där det föremål som ska genomsökas är en hårddisk eller annat datalagringsmedium, kommer i princip endast själva uppgifterna (kopierade eller utskrivna) att beslagtas i stället för hela mediet ([28]). Datalagringsmediet i sig får endast beslagtas om det anses vara praktiskt omöjligt att skriva ut eller kopiera de begärda uppgifterna separat, eller om det anses praktiskt ogenomförbart att på annat sätt uppnå syftet med genomsökningen ([29]). Den berörda personen måste utan dröjsmål underrättas om beslagtagandet ([30]). Det finns inga undantag från detta anmälningskrav enligt straffprocesslagen.

Husrannsakan, inspektion och beslag utan domstolsbeslut får endast utföras i begränsade fall. För det första när det är omöjligt att erhålla ett domstolsbeslut på grund av brådskande omständigheter vid brottsplatsen ([31]). Därefter måste dock ett domstolsbeslut erhållas utan dröjsmål ([32]). För det andra kan husrannsakan och inspektion utan domstolsbeslut äga rum på plats när en brottsmisstänkt grips eller frihetsberövas ([33]). Slutligen får en åklagare eller högre tjänsteman vid kriminalpolisen beslagta ett föremål utan domstolsbeslut när föremålet har kasserats av en brottsmisstänkt eller tredje man, eller har ingetts frivilligt ([34]).

Bevis som erhållits i strid med straffprocesslagen kommer inte att godtas ([35]). Dessutom föreskrivs i strafflagen att olagliga genomsökningar av personer eller personers bostad, bevakade byggnader, strukturer, bilar, fartyg, flygplan eller belagda rum bestraffas med fängelse i högst tre år ([36]). Denna bestämmelse gäller därför även när föremål, t.ex. datalagringsenheter, beslagtas vid en rättsstridig genomsökning.

2.2.2. *Insamling av kommunikationsinformation*

2.2.2.1. Rättslig grund

Insamling av kommunikationsinformation regleras av en särskild lag: om post- och telehemlighet. I om post- och telehemlighet föreskrivs särskilt ett förbud mot censur av post, avlyssning av telekommunikation, tillhandahållande av uppgifter om kommunikationsbekräftelse, inspelning eller avlyssning av samtal mellan personer som inte offentliggjorts, förutom när detta sker på grundval av straffprocesslagen, om post- och telehemlighet eller lagen om militärdomstolen ([37]). Begreppet kommunikation i den mening som avses i om post- och telehemlighet omfattar både vanlig post och telekommunikationer ([38]). I detta avseende görs i lagen om post- och telehemlighet en åtskillnad mellan *kommunikationsbegränsande åtgärder* ([39]) och insamling av *uppgifter om kommunikationsbekräftelse*.

Begreppet kommunikationsbegränsande åtgärder omfattar *censur*, dvs. insamling av innehållet i traditionell post, samt *teleavlyssning*, dvs. direkt avlyssning (förvärv eller inspelning) av innehållet i telekommunikationer ([40]). Begreppet uppgifter om kommunikationsbekräftelse omfattar *uppgifter om telekommunikationsregister*, vilket inbegriper datum för telekommunikation, start- och sluttid, antal utgående och inkommande samtal samt den andra partens abonnentnummer, användningsfrekvens, loggfiler avseende användningen av telekommunikationstjänster och lokaliseringsuppgifter (t.ex. från sändningstorn där signaler tas emot) ([41]).

([28]) Artikel 106.3 i straffprocesslagen.
([29]) Artikel 106.3 i straffprocesslagen.
([30]) Artikel 219 i straffprocesslagen jämförd med artikel 106.4 i straffprocesslagen.
([31]) Artikel 216.3 i straffprocesslagen.
([32]) Artikel 216.3 i straffprocesslagen.
([33]) Artikel 216.1 och 216.2 i straffprocesslagen.
([34]) Artikel 218 i straffprocesslagen. När det gäller personuppgifter omfattar detta endast frivilligt ingivande av den berörda personen själv, inte av en personuppgiftsansvarig som innehar sådana uppgifter (vilket skulle kräva en särskild rättslig grund enligt lagen om skydd av personuppgifter). Frivilligt ingivna föremål godtas endast som bevis i domstolsförfaranden om offentliggörandet utom rimligt tvivel är frivilligt, vilket det är åklagarens uppgift att visa. Se högsta domstolens beslut nr 2013Do11233 av den 10 mars 2016.
([35]) Artikel 308-2 i straffprocesslagen.
([36]) Artikel 321 i strafflagen.
([37]) Artikel 3 i lagen om post- och telehemlighet. I lagen om militärdomstolen regleras i princip insamling av uppgifter om militär personal och den kan endast tillämpas på civila i ett begränsat antal fall (t.ex. kan förfaranden inledas vid en militär domstol om militär personal och civila begår ett brott tillsammans, eller om en person begår ett brott mot militären; se artikel 2 i lagen om militärdomstolen). De allmänna bestämmelserna om husrannsakan och beslag liknar straffprocesslagen, se t.ex. artiklarna 146–149 och 153–156 i lagen om militärdomstolen. Exempelvis kan post endast samlas in om det är nödvändigt för en utredning och på grundval av en domstolsorder från militärdomstolen. In den mån elektronisk kommunikation samlas in gäller de begränsningar och skyddsåtgärder som anges i lagen om post- och telehemlighet.
([38]) Artikel 2.1 i lagen om post- och telehemlighet, dvs. *sändning eller mottagning av ljud, ord, symboler eller bilder, på trådbunden eller trådlös väg, via fiberkabel eller andra elektromagnetiska system, bl.a. telefon, e-post, informationstjänster för medlemmar, faxapparat och radioburen personsökning*.
([39]) Artiklarna 2.7 och 3.2 i lagen om post- och telehemlighet.
([40]) *Censur* definieras som att öppna post utan den berörda partens samtycke eller att inhämta kunskap om, spela in eller undanhålla innehållet på andra sätt (artikel 2.6 i lagen om post- och telehemlighet). *Teleavlyssning* avser *förvärv eller inspelning av innehållet i telekommunikationer genom att lyssna på eller gemensamt läsa av ljud, ord, symboler eller bilder i kommunikationen med hjälp av elektronisk och mekanisk utrustning utan den berörda partens samtycke, eller genom att störa kommunikationens överföring och mottagning* (artikel 2.7 i lagen om post- och telehemlighet).
([41]) Artikel 2.11 i lagen om post- och telehemlighet.

I lagen om post- och telehemlighet fastställs begränsningar och skyddsåtgärder för insamling av båda typerna av uppgifter, och för flera av dessa krav gäller att överträdelser är föremål för straffrättsliga påföljder ([42]).

2.2.2.2. Begränsningar och skyddsåtgärder som är tillämpliga på insamling av kommunikationsinnehåll (kommunikationsbegränsande åtgärder)

Insamling av kommunikationsinnehåll får endast ske som ett kompletterande medel för att underlätta en brottsutredning (dvs. som en sista utväg) och insatser måste göras för att minimera intrånget i enskilda personers kommunikationshemligheter ([43]). I enlighet med denna allmänna princip får kommunikationsbegränsande åtgärder endast användas om det är svårt att på annat sätt förhindra att ett brott begås, gripa brottslingen eller samla in bevis ([44]). De brottsbekämpande organ som samlar in kommunikationsinnehåll måste omedelbart upphöra med detta när fortsatt tillgång inte längre anses vara nödvändigt och på så sätt säkerställa att intrånget i kommunikationens integritet är så begränsat som möjligt ([45]).

Dessutom får kommunikationsbegränsande åtgärder endast användas om det finns betydande skäl att misstänka att vissa allvarliga brott som är särskilt förtecknade i lagen om post- och telehemlighet planeras, begås eller har begåtts. Dessa inbegriper brott som uppror, narkotikarelaterade brott eller brott med sprängämnen, samt brott med anknytning till nationell säkerhet, diplomatiska förbindelser eller militära baser och installationer ([46]). Målet för en kommunikationsbegränsande åtgärd måste vara specifika postförsändelser eller telekommunikationer som skickas eller tas emot av den misstänkte, eller postförsändelser eller telekommunikationer som skickas eller tas emot av den misstänkte under en bestämd tidsperiod ([47]).

Även när dessa krav är uppfyllda får insamling av innehållsdata endast ske på grundval av en domstolsorder. En åklagare får särskilt begära att domstolen tillåter insamling av innehållsdata som rör den misstänkte eller den person som är föremål för utredning ([48]). På samma sätt kan en tjänsteman vid kriminalpolisen ansöka om tillstånd hos en åklagare, som i sin tur kan begära en domstolsorder ([49]). En begäran om en domstolsorder måste göras skriftligen och innehålla särskilda uppgifter. Följande ska särskilt anges: 1) välgrundade skäl till misstanke om att ett av de förtecknade brotten planeras, begås eller har begåtts samt underlag som fastställer ett prima facie-fall av misstanke, 2) de kommunikationsbegränsande åtgärderna samt deras mål, omfattning, syfte och faktiska tillämpningsperiod, 3) var och hur åtgärderna i sådana fall skulle genomföras ([50]).

Om de rättsliga kraven är uppfyllda får domstolen ge skriftligt tillstånd att vidta kommunikationsbegränsande åtgärder med avseende på den misstänkte eller den person som är föremål för utredning ([51]). I denna domstolsorder anges vilka typer av åtgärder som ska vidtas samt deras mål, omfattning, faktiska tillämpningsperiod, plats för genomförande och hur de ska genomföras ([52]).

Kommunikationsbegränsande åtgärder får endast genomföras under två månader ([53]). Om syftet med åtgärderna uppnås tidigare under denna period måste åtgärderna omedelbart upphöra. Om villkoren fortfarande är uppfyllda får däremot en begäran om förlängning av den faktiska tillämpningsperioden för kommunikationsbegränsande åtgärder lämnas in inom tidsfristen på två månader. En sådan begäran måste innehålla underlag som fastställer ett prima facie-argument för att förlänga åtgärderna ([54]). Den förlängda perioden får inte överstiga totalt ett år, eller tre år för vissa särskilt allvarliga brott (t.ex. brott med anknytning till uppror, utländsk aggression, nationell säkerhet osv.) ([55]).

De brottsbekämpande myndigheterna får kräva att kommunikationsoperatörer bistår dem och gör detta genom att förse dem med domstolens skriftliga tillstånd ([56]). Kommunikationsoperatörer måste samarbeta och förvara det tillstånd de erhållit i sina register ([57]). De får vägra att samarbeta om information som gäller den person åtgärderna riktar sig mot enligt domstolens skriftliga tillstånd (t.ex. personens telefonnummer) är felaktig. Dessutom förbjuds de under alla omständigheter att lämna ut lösenord som används för telekommunikation ([58]).

([42]) Artiklarna 16 och 17 i lagen om post- och telehemlighet. Detta gäller t.ex. insamling utan domstolsorder, underlåtenhet att föra register, underlåtenhet att avbryta insamlingen när en nödsituation upphör eller underlåtenhet att underrätta den berörda personen.
([43]) Artikel 3.2 i lagen om post- och telehemlighet.
([44]) Artikel 5.1 i lagen om post- och telehemlighet.
([45]) Artikel 2 i genomförandedekretet till lagen om post- och telehemlighet.
([46]) Artikel 5.1 i lagen om post- och telehemlighet.
([47]) Artikel 5.2 i lagen om post- och telehemlighet.
([48]) Artikel 6.1 i lagen om post- och telehemlighet.
([49]) Artikel 6.2 i lagen om post- och telehemlighet.
([50]) Artikel 6.4 i lagen om post- och telehemlighet och artikel 4.1 i genomförandedekretet till lagen om post- och telehemlighet.
([51]) Artikel 6.5 och 6.8 i lagen om post- och telehemlighet.
([52]) Artikel 6.6 i lagen om post- och telehemlighet.
([53]) Artikel 6.7 i lagen om post- och telehemlighet.
([54]) Artikel 6.7 i lagen om post- och telehemlighet.
([55]) Artikel 6.8 i lagen om post- och telehemlighet.
([56]) Artikel 9.2 i lagen om post- och telehemlighet.
([57]) Artikel 15-2 i lagen om post- och telehemlighet och artikel 12 i genomförandedekretet till lagen om post- och telehemlighet.
([58]) Artikel 9.4 i lagen om post- och telehemlighet.

Alla som vidtar kommunikationsbegränsande åtgärder eller som uppmanas att samarbeta måste föra register över åtgärdernas mål, deras genomförande, datum för samarbetet och målet ([59]). Brottsbekämpande myndigheter som genomför kommunikationsbegränsande åtgärder måste också föra register med detaljerade uppgifter och erhållna resultat ([60]). Tjänstemän vid kriminalpolisen måste lämna dess upplysningar i form av en rapport till åklagaren när de avslutar en utredning ([61]).

När en åklagare väcker åtal i ett fall där kommunikationsbegränsande åtgärder har använts, eller utfärdar ett beslut om att inte åtala eller gripa den berörda personen (dvs. inte bara en vilandeförklaring av åtalet), måste åklagaren underrätta den person som är föremål för de kommunikationsbegränsande åtgärderna om att kommunikationsbegränsande åtgärder har vidtagits, det verkställande organet och verkställighetsperioden. Ett sådant meddelande ska lämnas skriftligen inom 30 dagar från beslutet ([62]). Underrättelsen får skjutas upp om den sannolikt skulle utgöra ett allvarligt hot mot den nationella säkerheten eller störa den allmänna säkerheten eller ordningen eller om den sannolikt kan leda till väsentlig skada på andras liv eller kroppsskada ([63]). Om åklagaren eller tjänstemannen vid kriminalpolisen har för avsikt att skjuta upp underrättelsen måste godkännande erhållas från chefen för den lokala åklagarmyndigheten ([64]). När skälen för hänskjutande inte längre föreligger ska delgivning ske inom 30 dagar från den tidpunkten ([65]).

I lagen om post- och telehemlighet fastställs också ett särskilt förfarande för insamling av kommunikationsinnehåll i nödsituationer. I synnerhet får brottsbekämpande organ samla in kommunikationsinnehåll om planering eller genomförande av organiserad brottslighet eller annat grovt brott som direkt kan orsaka dödsfall eller allvarlig skada är nära förestående, och det föreligger en nödsituation som gör det omöjligt att genomgå det ordinarie förfarandet (enligt ovan) ([66]). I en sådan nödsituation får en polis eller åklagare vidta kommunikationsbegränsande åtgärder utan föregående domstolstillstånd, men ska omedelbart efter verkställighet ansöka om domstolstillstånd. Om den brottsbekämpande myndigheten inte erhåller domstolstillstånd inom 36 timmar från den tidpunkt då nödåtgärderna genomfördes, måste insamlingen omedelbart upphöra, vanligtvis följt av förstöring av den insamlade informationen ([67]). Poliser som utför nödövervakning gör detta under överinseende av en åklagare. Om det är omöjligt att ta emot åklagarens instruktioner i förväg på grund av att det är nödvändigt att agera skyndsamt måste polisen inhämta en åklagares godkännande omedelbart efter det att verkställigheten påbörjats ([68]). Reglerna om underrättelse till personen såsom beskrivs ovan gäller även insamling av kommunikationsinnehåll i nödsituationer.

Insamling av uppgifter i nödsituationer måste alltid ske i enlighet med ett *uttalande om nödcensur/nödavlyssning* och den myndighet som utför insamlingen måste föra ett register över eventuella nödåtgärder ([69]). Begäran till en domstol om tillstånd för nödåtgärder måste åtföljas av ett skriftligt dokument som anger de nödvändiga kommunikationsbegränsande åtgärderna, målet, ämnet, omfattningen, tidsperioden, platsen för genomförandet, metoden och en förklaring av hur de relevanta kommunikationsbegränsande åtgärderna uppfyller artikel 5.1 i lagen om post- och telehemlighet ([70]), tillsammans med styrkande handlingar.

I de fall då nödåtgärderna slutförs inom en kort tid, vilket utesluter domstolstillstånd (t.ex. om den misstänkte grips omedelbart efter det att avlyssningen inletts, vilken därför upphör), delger chefen för den behöriga åklagarmyndigheten ett meddelande om nödåtgärd till den behöriga domstolen ([71]). Däri ska följande anges: syfte, mål, tillämpningsområde, tidsperiod, platsen för genomförandet och insamlingsmetod samt skälen för att inte ha lämnat in en begäran om domstolstillstånd ([72]). Detta meddelande gör det möjligt för den mottagande domstolen att granska lagenligheten hos insamlingen, och det måste föras in i ett register över meddelanden om nödåtgärder.

([59]) Artikel 9.3 i lagen om post- och telehemlighet.
([60]) Artikel 18.1 i genomförandedekretet till lagen om post- och telehemlighet.
([61]) Artikel 18.2 i genomförandedekretet till lagen om post- och telehemlighet.
([62]) Artikel 9-2.1 i lagen om post- och telehemlighet.
([63]) Artikel 9-2.4 i lagen om post- och telehemlighet.
([64]) Artikel 9-2.5 i lagen om post- och telehemlighet.
([65]) Artikel 9-2.6 i lagen om post- och telehemlighet.
([66]) Artikel 8.1 i lagen om post- och telehemlighet.
([67]) Artikel 8.2 i lagen om post- och telehemlighet.
([68]) Artikel 8.3 i lagen om post- och telehemlighet och artikel 16.3 i genomförandedekretet till denna lag.
([69]) Artikel 8.4 i lagen om post- och telehemlighet.
([70]) Det vill säga att det finns starka skäl att misstänka att vissa allvarliga brott planeras eller begås, eller har begåtts, och att det är ogenomförbart att på annat sätt förhindra att detta brott begås, gripa brottslingen eller samla in bevis.
([71]) Artikel 8.5 i lagen om post- och telehemlighet.
([72]) Artikel 8.6–8.7 i lagen om post- och telehemlighet.

Som ett allmänt krav får kommunikationsinnehåll som har erhållits vid genomförande av kommunikationsbegränsande åtgärder på grundval av lagen om post- och telehemlighet endast användas för att utreda, lagföra eller förhindra de specifika brott som anges ovan, i disciplinära förfaranden för samma typer av brott, för skadeståndsanspråk som tas upp av en part i kommunikationen eller där detta tillåts enligt andra lagar ([73]).

Särskilda skyddsåtgärder gäller vid insamling av telekommunikation som överförs via internet ([74]). Sådana uppgifter får endast användas för att utreda de allvarliga brott som förtecknas i artikel 5.1 i lagen om post- och telehemlighet. För att lagra uppgifterna måste godkännande inhämtas från den domstol som godkände de kommunikationsbegränsande åtgärderna ([75]). En begäran om lagring måste innehålla information om de kommunikationsbegränsande åtgärderna, en sammanfattning av resultaten av åtgärderna, skälen till lagringen (tillsammans med underlag) och den telekommunikation som ska lagras ([76]). Om ingen sådan begäran inges måste den erhållna telekommunikationen raderas inom 14 dagar efter det att de kommunikationsbegränsande åtgärderna har avslutats ([77]). Om en begäran avslås måste telekommunikationen raderas inom sju dagar ([78]). Om telekommunikation raderas ska en rapport inges inom sju dagar till den domstol som godkände de kommunikationsbegränsande åtgärderna, med angivande av skälen till raderingen samt närmare uppgifter om och tidpunkt för detta.

Mer generellt kommer information som erhållits på olaglig väg genom kommunikationsbegränsande åtgärder inte att godtas som bevis i rättsliga eller disciplinära förfaranden ([79]). Enligt lagen om post- och telehemlighet är det dessutom förbjudet för personer som vidtar kommunikationsbegränsande åtgärder att lämna ut konfidentiell information som erhållits i samband med genomförandet av sådana åtgärder och att använda den information som erhållits för att skada anseendet hos dem som omfattas av åtgärderna ([80]).

2.2.2.3. Begränsningar och skyddsåtgärder som är tillämpliga på insamling av uppgifter om kommunikationsbekräftelse

På grundval av lagen om post- och telehemlighet får brottsbekämpande myndigheter begära att teleoperatörer tillhandahåller uppgifter om kommunikationsbekräftelse när så krävs för att genomföra en utredning eller verkställa en påföljd ([81]). Till skillnad från insamling av innehållsdata är möjligheten att samla in uppgifter om kommunikationsbekräftelse inte begränsad till vissa specifika brott. Precis som för innehållsdata kräver dock insamling av uppgifter om kommunikationsbekräftelse ett skriftligt förhandstillstånd från en domstol, på samma villkor som beskrivs ovan ([82]). När brådskande skäl föreligger som gör det omöjligt att inhämta domstolstillstånd får uppgifter om kommunikationsbekräftelse samlas in utan domstolsorder. I dessa fall måste tillstånd inhämtas omedelbart efter att uppgifterna har begärts och sedan meddelas telekommunikationsleverantören ([83]). Om inget efterföljande tillstånd erhålls måste de insamlade uppgifterna förstöras ([84]).

Åklagare, tjänstemän vid kriminalpolisen och domstolar måste föra register över begäranden om uppgifter om kommunikationsbekräftelse ([85]). Dessutom måste telekommunikationsleverantörer två gånger per år rapportera om utlämnande av uppgifter om kommunikationsbekräftelse till ministern för vetenskap och IKT, och bevara dessa uppgifter i sju år från och med den dag då uppgifterna lämnades ut ([86]).

Enskilda personer underrättas i princip om att uppgifter om kommunikationsbekräftelse har samlats in ([87]). Tidpunkten för en sådan underrättelse beror på omständigheterna för undersökningen ([88]). När ett beslut har fattats om att (inte) väcka åtal måste underrättelse ske inom 30 dagar. Om åtalet däremot skjuts upp ska underrättelsen delges inom 30 dagar ett år efter det att ett sådant beslut har fattats. Under alla omständigheter måste underrättelsen delges inom 30 dagar ett år efter det att uppgifterna har samlats in.

Underrättelsen får skjutas upp om det är sannolikt att den kan 1) äventyra den nationella säkerheten, den allmänna säkerheten och ordningen, 2) orsaka dödsfall eller kroppsskada, 3) hindra rättvisa rättsliga förfaranden (t.ex. leda till att

([73]) Artikel 12 i lagen om post- och telehemlighet.
([74]) Artikel 12-2 i lagen om post- och telehemlighet.
([75]) Den åklagare eller polis som genomför de kommunikationsbegränsande åtgärderna måste välja ut den telekommunikation som ska lagras inom 14 dagar efter det att åtgärderna har upphört och begära godkännande från domstol (när det gäller en polistjänsteman ska ansökan göras till en åklagare, som i sin tur inger begäran till domstolen), se artikel 12-2.1 och 12-2.2 i lagen om post- och telehemlighet.
([76]) Artikel 12-2.3 i lagen om post- och telehemlighet.
([77]) Artikel 12-2.5 i lagen om post- och telehemlighet.
([78]) Artikel 12-2.5 i lagen om post- och telehemlighet.
([79]) Artikel 4 i lagen om post- och telehemlighet.
([80]) Artikel 11.2 i genomförandedekretet till lagen om post- och telehemlighet.
([81]) Artikel 13.1 i lagen om post- och telehemlighet.
([82]) Artiklarna 13 och 6 i lagen om post- och telehemlighet.
([83]) Artikel 13.2 i lagen om post- och telehemlighet. I likhet med vad som gäller för brådskande kommunikationsbegränsande åtgärder måste ett dokument utarbetas med närmare information om fallet (den misstänkte, de åtgärder som ska vidtas, det misstänkta brottet och anledningen till brådskan). Se artikel 37.5 i genomförandedekretet till lagen om post- och telehemlighet.
([84]) Artikel 13.3 i lagen om post- och telehemlighet.
([85]) Artikel 13.5 och 13.6 i lagen om post- och telehemlighet.
([86]) Artikel 13.7 i lagen om post- och telehemlighet.
([87]) Se artikel 13-3.7 jämförd med artikel 9-2 i lagen om post- och telehemlighet.
([88]) Artikel 13-3.1 i lagen om post- och telehemlighet.

bevis förstörs eller vittnen hotas) eller 4) innebära förtal av den misstänkte, brottsoffer eller andra personer med anknytning till målet, eller inkräkta på deras privatliv ([89]). Underrättelse på någon av ovanstående grunder kräver tillstånd från chefen för en behörig distriktsåklagarmyndighet ([90]). När skälen för uppskjutande av underrättelsen inte längre föreligger ska delgivning ske inom 30 dagar från den tidpunkten ([91]).

Enskilda personer som har underrättats kan inge en skriftlig begäran till åklagaren eller tjänstemannen vid kriminalpolisen angående ändamålen med insamlingen av uppgifterna om kommunikationsbekräftelse ([92]). I så fall ska åklagaren eller tjänstemannen vid kriminalpolisen skriftligen ange ändamålen inom 30 dagar från mottagandet av begäran, såvida inte något av ovanstående skäl (undantag som gäller uppskjutande av underrättelse) är tillämpligt ([93]).

2.2.3. *Teleoperatörers frivilliga utlämnande av uppgifter*

Enligt artikel 83.3 i lagen om telekomoperatörer får teleoperatörer frivilligt tillmötesgå en begäran från en domstol, åklagare eller chef för ett utredningsorgan om att lämna ut ”kommunikationsuppgifter” till stöd för en brottsutredning, utredning eller verkställighet av en dom. Inom ramen för lagen om telekomoperatörer omfattar *kommunikationsuppgifter* användarnas namn, nummer i folkbokföringsregistret, adress och telefonnummer, datum då användarna tecknar eller avslutar sitt abonnemang samt deras identifieringskoder (dvs. koder som används för att identifiera den rättmätiga användaren av datorsystem eller kommunikationsnät) ([94]). I lagen om telekomoperatörer betraktas endast personer som direkt förvärvar tjänster från en sydkoreansk telekommunikationsleverantör som användare ([95]). Till följd av detta är det sannolikt att antalet fall där enskilda personer i EU vars uppgifter har överförts till Sydkorea betraktas som användare enligt lagen om telekomoperatörer kommer att vara mycket begränsade, eftersom dessa personer normalt inte skulle ingå ett direkt avtal med en sydkoreansk teleoperatör.

Begäran om att erhålla kommunikationsuppgifter på grundval av lagen om telekomoperatörer ska göras skriftligen och däri ska skälen till begäran, länken till den relevanta användaren och de begärda uppgifternas omfattning anges ([96]). Om det är omöjligt att lämna in en skriftlig begäran på grund av brådskande omständigheter ska den skriftliga begäran lämnas så snart som skälet till att ärendet är brådskande inte längre föreligger ([97]). Teleoperatörer som tillmötesgår begäran om utlämnande av kommunikationsuppgifter måste föra liggare som innehåller uppgifter som visar att kommunikationsuppgifter har tillhandahållits samt tillhörande material, såsom den skriftliga begäran ([98]). Dessutom måste teleoperatörer två gånger per år rapportera om tillhandahållandet av kommunikationsuppgifter till ministern för vetenskap och IKT ([99]).

Det finns ingen skyldighet för teleoperatörer att efterkomma en begäran om att lämna ut kommunikationsuppgifter på grundval av lagen om telekomoperatörer. Varje begäran måste därför bedömas av verksamhetsutövaren mot bakgrund av de tillämpliga dataskyddskraven i PIPA. I synnerhet måste en teleoperatör ta hänsyn till den registrerades intressen och får inte röja informationen om det är sannolikt att det skulle utgöra en otillbörlig överträdelse av den enskildes eller tredje mans intressen ([100]). I enlighet med anmälan nr 2021-1 om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter måste den berörda personen dessutom underrättas om utlämnandet. I undantagsfall får en sådan underrättelse skjutas upp, särskilt om och så länge som underrättelsen skulle äventyra en pågående brottsutredning eller sannolikt skada en annan persons liv eller kropp, om dessa rättigheter eller intressen är uppenbart överordnade den registrerades rättigheter ([101]).

År 2016 bekräftade högsta domstolen att teleoperatörers frivilliga tillhandahållande av kommunikationsuppgifter utan domstolsorder på grundval av lagen om telekomoperatörer inte i sig strider mot rätten att bestämma över information om sig själv som tillerkänns användaren av telekommunikationstjänsten. Samtidigt klargjorde domstolen att det skulle föreligga en sådan överträdelse om det är uppenbart att det ansökande organet missbrukade sin befogenhet att begära utlämnande av kommunikationsuppgifter, vilket skulle strida mot den berörda personens eller tredje mans intressen ([102]). Mer allmänt måste varje begäran om frivilligt utlämnande som inges av en brottsbekämpande myndighet följa principerna om laglighet, nödvändighet och proportionalitet som följer av den sydkoreanska författningen (artiklarna 12.1 och 37.2).

([89]) Artikel 13-3.2 i lagen om post- och telehemlighet.
([90]) Artikel 13-3.3 i lagen om post- och telehemlighet.
([91]) Artikel 13-3.4 i lagen om post- och telehemlighet.
([92]) Artikel 13-3.5 i lagen om post- och telehemlighet.
([93]) Artikel 13-3.6 i lagen om post- och telehemlighet.
([94]) Artikel 83.3 i lagen om telekomoperatörer.
([95]) Artikel 2.9 i lagen om telekomoperatörer.
([96]) Artikel 83.4 i lagen om telekomoperatörer.
([97]) Artikel 83.4 i lagen om telekomoperatörer.
([98]) Artikel 83.5 i lagen om telekomoperatörer.
([99]) Artikel 83.6 i lagen om telekomoperatörer.
([100]) Artikel 18.2 i PIPA.
([101]) Anmälan nr 2021-1 från nämnden för skydd av personuppgifter om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter, avsnitt III, 2 iii).
([102]) Högsta domstolens beslut nr 2012Da105482 av den 10 mars 2016.

2.3. **Tillsyn**

Tillsynen av brottsbekämpande myndigheter på det straffrättsliga området sker genom olika mekanismer, både internt och av externa organ.

2.3.1. *Internrevision*

I enlighet med lagen om revisioner i den offentliga sektorn uppmuntras myndigheter att inrätta ett internt revisionsorgan, med uppgift att bland annat utföra laglighetskontroller ([103]). Cheferna för sådana revisionsorgan måste i största möjliga utsträckning garanteras oberoende ([104]). Närmare bestämt utses de utanför den berörda myndigheten (t.ex. före detta domare, professorer) för en period om två till fem år och kan endast avsättas av motiverade skäl (t.ex. om de inte kan utföra sina uppgifter på grund av psykisk eller fysisk sjukdom, eller om de är föremål för disciplinära åtgärder) ([105]). Revisorer utses också på grundval av de särskilda villkor som fastställs i lagen ([106]). Revisionssrapporterna kan innehålla rekommendationer eller ansökningar om kompensation eller korrigering, samt reprimander och rekommendationer eller begäranden om disciplinåtgärder ([107]). De delges chefen för den myndighet som är föremål för revisionen samt till revisions- och kontrollstyrelsen (se avsnitt 2.3.2) inom 60 dagar efter det att revisionen slutförts ([108]). Den berörda myndigheten måste genomföra de åtgärder som krävs och rapportera resultaten till revisions- och kontrollstyrelsen ([109]). Dessutom görs revisionsresultaten i allmänhet tillgängliga för allmänheten ([110]). Vägran eller hindrande av internrevision omfattas av administrativa sanktionsavgifter ([111]). För att följa ovannämnda lagstiftning tillämpar den nationella polismyndigheten ett system med generalinspektörer för internrevisioner på det straffrättsliga området, bl.a. eventuella kränkningar av de mänskliga rättigheterna ([112]).

2.3.2. *Revisions- och kontrollstyrelsen*

Revisions- och kontrollstyrelsen (*Board of Audit and Inspection*) får kontrollera myndigheters verksamhet och på grundval av sådana kontroller utfärda rekommendationer, begära disciplinära åtgärder eller inge en brottsanmälan ([113]). Revisions- och kontrollstyrelsen är inrättat under Sydkoreas president, men har en oberoende ställning med avseende på dess uppgifter ([114]). Dessutom kräver lagen om inrättande av revisions- och kontrollstyrelsen att revisions- och kontrollstyrelsen i största möjliga utsträckning ska beviljas oberoende när det gäller utnämning, avskedande och organisation av personal samt sammanställning av styrelsens budget ([115]). Revisions- och kontrollstyrelsens ordförande utses av presidenten med parlamentets samtycke ([116]). De sex återstående ledamöterna utses av presidenten för en fyraårsperiod på rekommendation av ordföranden ([117]). Ledamöterna (inklusive ordföranden) måste uppfylla de särskilda kvalifikationer som fastställs i lag ([118]) och får endast avsättas i händelse av riksrättsförfarande, frihetsstraff eller oförmåga att utföra sina uppgifter på grund av långvarig bristande psykisk eller fysisk kapacitet ([119]). Dessutom är ledamöterna förbjudna att delta i politisk verksamhet och att samtidigt inneha uppdrag i parlamentet, förvaltningsorgan, organisationer som är föremål för revision och inspektion av revisions- och kontrollstyrelsen eller andra avlönade uppdrag eller befattningar ([120]).

Revisions- och kontrollstyrelsen utför en allmän revision på årsbasis, men kan också utföra särskilda revisioner i frågor av särskilt intresse. Revisions- och kontrollstyrelsen kan begära in handlingar under en kontroll och begära att enskilda personer ska närvara ([121]). Som en del av en revision granskar revisions- och kontrollstyrelsen statens inkomster och

([103]) Artiklarna 3 och 5 i lagen om revisioner i den offentliga sektorn.
([104]) Artikel 7 i lagen om revisioner i den offentliga sektorn.
([105]) Artiklarna 8–11 i lagen om revisioner i den offentliga sektorn.
([106]) Artikel 16 ff. i lagen om revisioner i den offentliga sektorn.
([107]) Artikel 23.2 i lagen om revisioner i den offentliga sektorn.
([108]) Artikel 23.1 i lagen om revisioner i den offentliga sektorn.
([109]) Artikel 23.3 i lagen om revisioner i den offentliga sektorn.
([110]) Artikel 26 i lagen om revisioner i den offentliga sektorn.
([111]) Artikel 41 i lagen om revisioner i den offentliga sektorn.
([112]) Se särskilt avdelningarna under generaldirektören för revision och kontroll: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Artiklarna 24 och 31–35 i lagen om revisions- och kontrollstyrelsen (*Board of Audit and Inspection Act -BAI-lagen*).
([114]) Artikel 2.1 i BAI-lagen.
([115]) Artikel 2.2 i BAI-lagen.
([116]) Artikel 4.1 i BAI-lagen.
([117]) Artiklarna 5.1 och 6 i BAI-lagen.
([118]) T.ex. ha tjänstgjort som domare, allmän åklagare eller advokat i minst tio år, ha arbetat som offentlig tjänsteman eller professor eller ha haft en högre uppsatt tjänst vid ett universitet i minst åtta år, eller ha arbetat i minst tio år på ett börsnoterat aktiebolag eller vid en offentlig institution (varav minst fem år som verkställande direktör), se artikel 7 i BAI-lagen.
([119]) Artikel 8 i BAI-lagen.
([120]) Artikel 9 i BAI-lagen.
([121]) Se t.ex. artikel 27 i BAI-lagen.

utgifter, men övervakar också den allmänna efterlevnaden av myndigheternas och de offentliga tjänstemännens skyldigheter i syfte att förbättra den offentliga förvaltningens verksamhet ([122]). Dess tillsyn sträcker sig därför utöver budgetaspekterna och omfattar även en laglighetskontroll.

2.3.3. *Parlamentet*

Parlamentet får utreda och kontrollera myndigheter ([123]). Under en utredning eller kontroll får parlamentet begära att handlingar lämnas ut och tvinga vittnen att framträda ([124]). Den som begår mened vid en utredning som utförs av parlamentet är föremål för straffrättsliga påföljder (fängelse i upp till tio år) ([125]). Förfarandet och resultaten av kontroller kan offentliggöras ([126]). Om parlamentet finner olaglig eller otillbörlig verksamhet kan den begära att den berörda myndigheten vidtar korrigerande åtgärder, bl.a. beviljande av kompensation, disciplinära åtgärder och förbättrade interna förfaranden ([127]). Efter en sådan begäran måste myndigheten agera utan dröjsmål och rapportera resultatet till parlamentet ([128]).

2.3.4. *Nämnden för skydd av personuppgifter*

Nämnden för skydd av personuppgifter (*nämnden*) utövar tillsyn över brottsbekämpande myndigheters behandling av personuppgifter i enlighet med PIPA. Dessutom omfattar nämndens tillsyn enligt artiklarna 7-8.3, 7-8.4 och 7-9.5 i PIPA även eventuella överträdelser av bestämmelserna om begränsningar och skyddsåtgärder i fråga om insamling av personuppgifter, bl.a. sådana som ingår i de särskilda lagar som reglerar insamlingen av (elektroniska) bevis för brottsbekämpande ändamål (se avsnitt 2.2). Med hänsyn till kraven i artikel 3.1 PIPA för laglig och korrekt insamling av personuppgifter utgör en sådan överträdelse också en överträdelse av PIPA, vilket gör det möjligt för nämnden för skydd av personuppgifter att genomföra en utredning och vidta korrigerande åtgärder ([129]).

Vid utövandet av sin övervakningsfunktion har nämnden för skydd av personuppgifter tillgång till all relevant information ([130]). Nämnden för skydd av personuppgifter kan ge råd till brottsbekämpande myndigheter för att förbättra nivån på skyddet av personuppgifter vid behandling, vidta korrigerande åtgärder (t.ex. avbryta behandlingen av uppgifter eller vidta nödvändiga åtgärder för att skydda personuppgifter) eller råda myndigheten att vidta disciplinära åtgärder ([131]). Slutligen planeras straffrättsliga påföljder för vissa överträdelser av PIPA, såsom olaglig användning eller utlämnande av personuppgifter till tredje part eller olaglig behandling av känslig information ([132]). I detta avseende får nämnden för skydd av personuppgifter hänskjuta ärendet till det behöriga utredningsorganet (däribland en åklagare) ([133]).

2.3.5. *Den nationella människorättskommissionen*

Den nationella människorättskommissionen – ett oberoende organ som har till uppgift att skydda och främja de grundläggande rättigheterna ([134]) – har befogenhet att utreda och avhjälpa brott mot artiklarna 10–22 i författningen, som inbegriper rätten till integritet och till sekretess för korrespondens. Den nationella människorättskommissionen består av elva ledamöter som utnämns efter nominering av parlamentet (fyra), presidenten (fyra) och högsta domstolens ordförande (tre) ([135]). För att utses måste en ledamot 1) ha tjänstgjort i minst tio år vid ett universitet eller ett godkänt forskningsinstitut, åtminstone som biträdande professor, 2) ha tjänstgjort som domare, åklagare eller advokat i minst tio år, 3) ha varit verksam inom området mänskliga rättigheter i minst tio år (t.ex. för en ideell, icke-statlig organisation eller internationell organisation) eller 4) ha rekommenderats av grupper i det civila samhället ([136]). Ordföranden utses av

([122]) Artiklarna 20 och 24 i BAI-lagen.
([123]) Artikel 128 i lagen om parlamentet och artiklarna 2, 3 och 15 i lagen om kontroll och utredning av statsförvaltningen. Detta inbegriper årliga kontroller av offentliga angelägenheter som helhet och utredningar av specifika frågor.
([124]) Artikel 101 i lagen om kontroll och utredning av statsförvaltningen. Se även artiklarna 128 och 129 i lagen om parlamentet.
([125]) Artikel 14 i lagen om vittnesmål, utvärdering osv. inför parlamentet.
([126]) Artikel 12-2 i lagen om kontroll och utredning av statsförvaltningen.
([127]) Artikel 16.2 i lagen om kontroll och utredning av statsförvaltningen.
([128]) Artikel 16.3 i lagen om kontroll och utredning av statsförvaltningen.
([129]) Se anmälan nr 2021-1 från nämnden för skydd av personuppgifter om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter.
([130]) Artikel 63 i PIPA.
([131]) Artiklarna 61.2, 65.1, 65.2 och 64.4 i PIPA.
([132]) Artiklarna 70–74 i PIPA.
([133]) Artikel 65.1 i PIPA.
([134]) Artikel 1 i lagen om människorättskommissionen (*Human Rights Commission Act*, nedan *NHRC-lagen*).
([135]) Artikel 5.1 och 5.2 i NHRC-lagen.
([136]) Artikel 5.3 i NHRC-lagen.

presidenten bland ledamöterna och måste bekräftas av parlamentet ([137]). Ledamöterna (däribland ordföranden) utses för en förnybar period på tre år och kan endast avsättas om de döms till fängelse eller inte längre kan utföra sina uppgifter på grund av långvarig bristande fysisk eller psykisk kapacitet (i vilket fall två tredjedelar av ledamöterna måste gå med på avskedandet) ([138]). Den nationella människorättskommissionens ledamöter är förbjudna att samtidigt inneha ett uppdrag i parlamentet, lokala råd eller något statligt eller lokalt styrelseorgan (som offentlig tjänsteman) ([139]).

Den nationella människorättskommissionen får inleda en utredning på eget initiativ eller på grundval av en framställning från en enskild person. Som en del av sin undersökning får den nationella människorättskommissionen begära att relevant material lämnas in, att kontroller utförs och att enskilda personer kallas att vittna ([140]). Efter en utredning kan den nationella människorättskommissionen utfärda rekommendationer för att förbättra eller korrigera särskilda strategier och metoder och får offentliggöra dem ([141]). Myndigheterna måste underrätta den nationella människorättskommissionen om en plan för att genomföra sådana rekommendationer inom 90 dagar från mottagandet ([142]). Vid underlåtenhet att genomföra rekommendationer måste den berörda myndigheten dessutom informera kommissionen om detta ([143]). Den nationella människorättskommissionen får i sin tur upplysa parlamentet om sådana brister och/eller offentliggöra dem. Myndigheterna följer i allmänhet den nationella människorättskommissionens rekommendationer och har ett starkt incitament att göra detta eftersom deras genomförande har bedömts vara en del av den allmänna utvärdering som genomförs av byrån för samordning av regeringens politik, under ledning av premiärministerns kansli.

2.4. **Prövning för enskilda**

2.4.1. *Prövningsmekanismer som finns tillgängliga enligt PIPA*

Enskilda personer får utöva sina rättigheter till tillgång, rättelse, radering och upphörande enligt PIPA när det gäller personuppgifter som behandlas av brottsbekämpande myndigheter på det straffrättsliga området. Tillgång kan begäras direkt från den berörda myndigheten, eller indirekt via nämnden för skydd av personuppgifter ([144]). Den behöriga myndigheten får begränsa eller neka tillgång endast om detta föreskrivs i lag, om det sannolikt skulle orsaka skada på en tredje parts liv eller kropp, eller sannolikt leda till överträdelser av en annan persons äganderättigheter och andra intressen (dvs. om den andra personens intressen skulle väga tyngre än intressena hos den person som inkommer med begäran) ([145]). Om en begäran om tillgång avslås måste personen informeras om skälen till detta och om hur man överklagar ([146]). På samma sätt kan en begäran om rättelse eller radering avslås om detta föreskrivs i andra lagar, varvid personen måste informeras om de bakomliggande skälen och möjligheten att överklaga ([147]).

I fråga om prövning kan enskilda personer inge ett klagomål till nämnden för skydd av personuppgifter, bland annat genom den integritetstjänst som drivs av Sydkoreas byrå för internet och säkerhet ([148]). Dessutom kan en enskild person få medling genom kommittén för tvistlösning avseende personuppgifter ([149]). Dessa möjligheter till prövning finns tillgängliga både vid eventuella överträdelser av reglerna i särskilda lagar om begränsningar och skyddsåtgärder i fråga om insamling av personuppgifter (avsnitt 2.2) och av PIPA. Dessutom kan enskilda personer bestrida nämndens beslut eller passivitet enligt förvaltningsprocesslagen (se avsnitt 2.4.3).

([137]) Artikel 5.5 i NHRC-lagen.
([138]) Artiklarna 7.1 och 8 i NHRC-lagen.
([139]) Artikel 10 i NHRC-lagen.
([140]) Artikel 36 i NHRC-lagen. I enlighet med artikel 36.7 i lagen får inlämning av material eller föremål avslås om det skulle inverka menligt på statlig sekretess som kan ha en väsentlig inverkan på statens säkerhet eller diplomatiska förbindelser, eller utgöra ett allvarligt hinder för en brottsutredning eller pågående rättegång. I sådana fall får kommissionen begära ytterligare information från chefen för det berörda organet (som måste efterkomma denna begäran i god tro) när detta krävs för att avgöra om vägran att lämna information är motiverad.
([141]) Artikel 25.1 i NHRC-lagen.
([142]) Artikel 25.3 i NHRC-lagen.
([143]) Artikel 25.4 i NHRC-lagen.
([144]) Artikel 35.2 i PIPA.
([145]) Artikel 35.4 i PIPA.
([146]) Artikel 42.2 i genomförandedekretet till PIPA.
([147]) Artiklarna 36.1–2 i PIPA och artikel 43.3 i genomförandedekretet till PIPA.
([148]) Artikel 62 i PIPA.
([149]) Artiklarna 40–50 i PIPA och artiklarna 48-2–57 i genomförandedekretet till PIPA.

2.4.2. *Prövning inför den nationella människorättskommissionen*

Den nationella människorättskommissionen hanterar klagomål från enskilda (både sydkoreanska och utländska medborgare) om kränkningar av de mänskliga rättigheterna som begåtts av myndigheter ([150]). Det finns inget stående krav på att enskilda personer ska lämna in ett klagomål till den nationella människorättskommissionen ([151]). Till följd av detta kommer den nationella människorättskommissionen att handlägga ett klagomål även om den berörda personen inte kan påvisa någon skada i det skede som avser upptagande till prövning. När det gäller insamling av personuppgifter för brottsbekämpande ändamål skulle en enskild person därför inte vara skyldig att visa att sydkoreanska myndigheter har haft tillgång till hans eller hennes personuppgifter för att klagomålet ska kunna tas upp till prövning inför den nationella människorättskommissionen. En person kan också begära att klagomålet ska lösas genom medling ([152]).

För att utreda ett klagomål kan den nationella människorättskommissionen utnyttja sina utredningsbefogenheter, bland annat genom att begära in relevant material, genomföra kontroller och kalla enskilda personer att vittna ([153]). Om utredningen visar att en överträdelse av relevanta lagar har ägt rum, får den nationella människorättskommissionen rekommendera att åtgärder vidtas eller att relevanta stadgar, institutioner, riktlinjer eller praxis korrigeras eller förbättras ([154]). Föreslagna åtgärder kan omfatta medling, upphörande av kränkningar av de mänskliga rättigheterna, skadestånd och åtgärder för att förhindra att samma eller liknande kränkningar upprepas ([155]). Vid olaglig insamling av personuppgifter enligt tillämpliga regler kan korrigerande åtgärder inbegripa radering av de insamlade personuppgifterna. Om det anses mycket sannolikt att överträdelsen pågår och det anses troligt att skador som är svåra att avhjälpa kan orsakas om detta lämnas utan åtgärd får den nationella människorättskommissionen vidta brådskande åtgärder ([156]).

Även om den nationella människorättskommissionen inte har någon tvingande befogenhet kan dess beslut (t.ex. ett beslut om att inte fortsätta undersökningen av ett klagomål) ([157]) och rekommendationer överklagas till de sydkoreanska domstolarna enligt förvaltningsprocesslagen (se avsnitt 2.4.3) ([158]). Om den nationella människorättskommissionens slutsatser visar att personuppgifter olagligt har samlats in av en myndighet kan en enskild person dessutom begära vidare prövning inför de sydkoreanska domstolarna mot denna myndighet, t.ex. genom att bestrida insamlingen enligt förvaltningsprocesslagen, inge en författningsklagan till författningsdomstolen enligt lagen om författningsdomstolen eller ansöka om skadestånd enligt lagen om statlig kompensation (se avsnitt 2.4.3).

2.4.3. *Rättslig prövning*

Enskilda personer kan åberopa de begränsningar och skyddsåtgärder som beskrivs i föregående avsnitt för att få sin sak prövad i sydkoreansk domstol på olika sätt.

För det första kan den berörda personen och hans eller hennes ombud enligt straffprocesslagen närvara när en domstolsorder för husrannsakan eller beslag verkställs och kan därmed göra invändningar vid den tidpunkt då ordern verkställs ([159]). I straffprocesslagen föreskrivs dessutom en så kallad ”mekanism för halva klagomål”, som gör det möjligt för enskilda personer att göra en framställning till den behöriga domstolen med en begäran om att upphäva eller ändra ett beslut som en åklagare eller polis har fattat om ett beslag ([160]). Detta gör det möjligt för enskilda att bestrida de åtgärder som vidtagits för att verkställa en domstolsorder om beslag.

([150]) I artikel 4 i lagen om den nationella kommissionen för mänskliga rättigheter hänvisas till medborgare och utlänningar som är bosatta i Sydkorea, men begreppet ”bosatta” återspeglar snarare ett begrepp om jurisdiktion än territorium. Om en statlig institution i Sydkorea överträder grundläggande rättigheter tillhörande en utländsk medborgare utanför Sydkorea kan den personen inge ett klagomål till den nationella människorättskommissionen. Se t.ex. den därmed sammanhängande frågan på den nationella människorättskommissionens sida med vanliga frågor som finns tillgänglig på https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Detta skulle vara fallet om de sydkoreanska myndigheterna har olaglig tillgång till personuppgifter som har överförts till Sydkorea avseende en utländsk medborgare.

([151]) Ett klagomål måste i princip inges inom ett år från överträdelsen, men den nationella människorättskommissionen kan fortfarande besluta att utreda ett klagomål som inges efter den tidsperioden så länge preskriptionstiden enligt straffrätten eller civilrätten inte har löpt ut (artikel 32.1 led 4 i NHRC-lagen).

([152]) Artikel 42 ff. i NHRC-lagen.

([153]) Artiklarna 36 och 37 i NHRC-lagen.

([154]) Artikel 44 i NHRC-lagen.

([155]) Artikel 42.4 i NHRC-lagen.

([156]) Artikel 48 i NHRC-lagen.

([157]) Om den nationella människorättskommissionen t.ex. i undantagsfall inte kan kontrollera visst material eller vissa anläggningar på grund av att det rör sig om statshemligheter som kan ha en väsentlig inverkan på statens säkerhet eller diplomatiska förbindelser, eller om kontrollen skulle utgöra ett allvarligt hinder för en brottsutredning eller pågående rättegång (se fotnot 166) och om detta hindrar den nationella människorättskommissionen från att genomföra den utredning som krävs för att bedöma om talan är befogad, kommer den nationella människorättskommissionen att informera den enskilda personen om orsakerna till att klagomålet avslogs, i enlighet med artikel 39 i NHRC-lagen. I detta fall skulle personen kunna överklaga den nationella människorättskommissionens beslut enligt förvaltningsprocesslagen.

([158]) Se t.ex. överdomstolen i Seoul, beslut nr 2007Nu27259 av den 18 april 2008, bekräftad genom högsta domstolens beslut nr 2008Du7854 av den 9 oktober 2008; överdomstolen i Seoul, beslut nr 2017Nu69382 av den 2 februari 2018.

([159]) Artiklarna 121 och 219 i straffprocesslagen.

([160]) Artikel 417 i straffprocesslagen jämförd med artikel 414.2 i straffprocesslagen. Se även högsta domstolens beslut nr 97Mo66 av den 29 september 1997.

Dessutom kan enskilda personer få ersättning för skador vid de sydkoreanska domstolarna. På grundval av lagen om statlig kompensation kan enskilda personer ansöka om ersättning för skador som offentliga tjänstemän åsamkar dem vid lagstridigt fullgörande av sina officiella uppgifter ([161]). Ett skadeståndsanspråk enligt lagen om statlig kompensation kan inges till ett specialiserat ”kompensationsråd” eller direkt till de sydkoreanska domstolarna ([162]). Om offret är en utländsk medborgare tillämpas lagen om statlig kompensation under förutsättning att den medborgarens ursprungsland även säkerställer statlig kompensation för sydkoreanska medborgare ([163]). Enligt rättspraxis är detta villkor uppfyllt om kraven vid begäran om skadestånd i det andra landet *inte i någon större utsträckning avviker mellan Sydkorea och det andra landet* och *generellt sett inte är strängare än de krav som fastställts av Sydkorea, utan några materiella och väsentliga skillnader* ([164]). Civilrätten reglerar statens skadeståndsansvar, och följaktligen omfattar statens skadeståndsansvar även skadestånd som inte avser egendom (t.ex. psykiskt lidande) ([165]).

När det gäller överträdelser av dataskyddsregler finns det ytterligare ett rättsmedel inom ramen för PIPA. Enligt artikel 39 i PIPA kan var och en som lider skada till följd av en överträdelse av PIPA eller förlust, stöld, spridning, förfalskning, ändring av eller skada på hans eller hennes personuppgifter erhålla ersättning för skada vid en domstol. Det finns inget liknande krav på ömsesidighet som enligt lagen om statlig kompensation.

Utöver skadestånd kan administrativ prövning erhållas mot åtgärder eller underlåtelse från förvaltningsorganens sida enligt förvaltningsprocesslagen. Alla enskilda personer kan bestrida ett beslut (dvs. utövande av eller vägran att utöva offentlig makt i ett visst fall) eller underlåtelse (en förvaltningsorgans långvariga underlåtenhet att fatta ett visst beslut trots en rättslig förpliktelse att göra detta), vilket kan leda till återkallande eller ändring av ett olagligt beslut, ett konstaterande av ogiltighet (dvs. ett konstaterande om att beslutet inte har någon rättslig verkan eller att det inte existerar i rättsordningen) eller ett konstaterande om att underlåtelsen är rättsstridig ([166]). För att kunna bestrida ett förvaltningsbeslut måste det direkt påverka medborgerliga rättigheter och skyldigheter ([167]). Detta inbegriper åtgärder för att samla in personuppgifter, antingen direkt (t.ex. avlyssning av kommunikation) eller genom en begäran om utlämnande (t.ex. till en tjänsteleverantör).

Ovannämnda anspråk kan först inges till administrativa överklagandenämnder som inrättats av vissa myndigheter (t.ex. NIS, NHRC) eller till den centrala administrativa överklagandenämnd som inrättats inom ramen för kommissionen för medborgerliga rättigheter och bekämpning av korruption ([168]). Ett sådant administrativt överklagande ger en alternativ, mer informell möjlighet att bestrida en myndighets beslut eller underlåtelse att agera. Ett anspråk kan dock även inges direkt till de sydkoreanska domstolarna enligt förvaltningsprocesslagen.

En begäran om återkallande eller ändring av ett beslut enligt förvaltningsprocesslagen får inges av varje person som har ett rättsligt intresse av att begära återkallandet eller ändringen, eller att få sina rättigheter återställda genom återkallandet/ändringen om beslutet inte längre har verkan ([169]). På samma sätt kan talan om ogiltighet väckas av en person som har ett rättsligt intresse av en sådan bekräftelse, medan en tvist för att bekräfta att en underlåtelse att agera är rättsstridig kan inledas av varje person som har begärt ett beslut och har ett rättsligt intresse av att begära att underlåtelsens rättsstridighet bekräftas ([170]). Enligt högsta domstolens rättspraxis tolkas ”rättsligt intresse” som ett ”rättsligt skyddat intresse”, dvs. ett direkt och specifikt intresse som skyddas av lagar och andra författningar som ligger till grund för administrativa beslut (dvs. inte allmänhetens generella, indirekta och abstrakta intressen) ([171]). Enskilda personer har därför ett rättsligt intresse vid överträdelse av begränsningar och skyddsåtgärder när det gäller insamlingen av deras personuppgifter för brottsbekämpande ändamål (enligt särskilda lagar eller PIPA). Parterna är bundna till en slutlig dom enligt förvaltningsprocesslagen ([172]).

En begäran om återkallande/ändring av ett beslut och en begäran om att bekräfta att en underlåtelse att agera är rättsstridig ska lämnas in inom 90 dagar från den dag personen får kännedom om beslutet eller underlåtelsen och i

([161]) Artikel 2.1 i lagen om statlig kompensation.

([162]) Artiklarna 9 och 12 i lagen om statlig kompensation. Genom lagen inrättas distriktsråd (under ledning av vice åklagaren vid motsvarande åklagarmyndighet), ett centralråd (under ledning av vice justitieministern) och ett särskilt råd (under ledning av vice försvarsministern och ansvarigt för skadeståndsanspråk för skador som orsakas av militär personal eller civilanställda inom militären). Skadeståndsanspråk hanteras i princip av distriktsrådet, som under vissa omständigheter måste vidarebefordra ärenden till det centrala eller särskilda rådet, t.ex. om skadeståndet överstiger ett visst belopp eller om en enskild person ansöker om ny granskning. Alla råd består av ledamöter som utses av justitieministern (t.ex. bland tjänstemän vid justitieministeriet, domstolar, advokater och personer med sakkunskap om statlig kompensation) och omfattas av särskilda regler om intressekonflikter (se artikel 7 i genomförandedekretet till lagen om statlig kompensation).

([163]) Artikel 7 i lagen om statlig kompensation.

([164]) Högsta domstolens beslut nr 2013Da208388 av den 11 juni 2015.

([165]) Se artikel 8 i lagen om statlig kompensation och artikel 751 i civillagen.

([166]) Artiklarna 2 och 4 i förvaltningsprocesslagen.

([167]) Högsta domstolens beslut nr 98Du18435 av den 22 oktober 1999, högsta domstolens beslut nr 99Du1113 av den 8 september 2000 och högsta domstolens beslut nr 2010Du3541 av den 27 september 2012.

([168]) Artikel 6 i lagen om administrativa överklaganden och artikel 18.1 i förvaltningsprocesslagen.

([169]) Artikel 12 i förvaltningsprocesslagen.

([170]) Artiklarna 35 och 36 i förvaltningsprocesslagen.

([171]) Högsta domstolens beslut nr 2006Du330 av den 26 mars 2006.

([172]) Artikel 30.1 i förvaltningsprocesslagen.

princip senast ett år efter den dag då beslutet utfärdades eller underlåtelsen inträffade, såvida det inte finns välgrundade skäl ([173]). Enligt högsta domstolens rättspraxis ska begreppet ”välgrundade skäl” tolkas i vidare bemärkelse och det måste bedömas om det är socialt godtagbart att tillåta ett försenat klagomål mot bakgrund av alla omständigheter i ärendet ([174]). Detta omfattar exempelvis (men är inte begränsat till) skäl till förseningen som den berörda parten inte kan hållas ansvarig för (dvs. situationer som ligger utanför klagandens kontroll, t.ex. om han eller hon inte har underrättats om insamlingen av hans eller hennes personuppgifter) eller force majeure (t.ex. naturkatastrof, krig).

Slutligen kan enskilda personer även inge en författningsklagan till författningsdomstolen ([175]). På grundval av lagen om författningsdomstolen får dessutom personer vars grundläggande och författningsskyddade rättigheter kränks genom utövandet av offentlig makt (med undantag av domstolsbeslut) begära avgörande gällande en författningsklagan. Om andra rättsmedel finns tillgängliga måste dessa först vara uttömda. Enligt författningsdomstolens rättspraxis kan utländska medborgare inge en författningsklagan i den mån deras grundläggande rättigheter erkänns i den sydkoreanska författningen (se förklaringarna i avsnitt 1.1) ([176]). En författningsklagan måste inges inom 90 dagar efter det att en person har fått kännedom om överträdelsen, och inom ett år efter det att den ägt rum. Med hänsyn till att förfarandet enligt förvaltningsprocesslagen är tillämpligt enligt lagen om författningsdomstolen ([177]) kan ett klagomål fortfarande tas upp till prövning om det finns ”välgrundade skäl”, i den tolkning som anges i högsta domstolens rättspraxis enligt ovan.

Om andra rättsmedel först måste uttömmas ska en författningsklagan inges inom 30 dagar efter det slutliga beslutet om ett sådant rättsmedel ([178]). Författningsdomstolen kan ogiltigförklara utövandet av den offentliga makt som orsakade överträdelsen eller bekräfta att en viss underlåtenhet att agera är författningsstridig ([179]). I så fall ska den berörda myndigheten vidta åtgärder för att rätta sig efter domstolens beslut.

3. MYNDIGHETERS TILLGÅNG TILL UPPGIFTER FÖR ÄNDAMÅL SOM RÖR DEN NATIONELLA SÄKERHETEN

3.1. **Behöriga myndigheter på området nationell säkerhet**

Sydkorea har två särskilda underrättelseorgan: den nationella underrättelsetjänsten och försvarets säkerhetskommando. Utöver detta får även polis och åklagare samla in personuppgifter för ändamål som rör den nationella säkerheten.

Den nationella underrättelsetjänsten är inrättad genom lagen om den nationella underrättelsetjänsten (*National Intelligence Service Act*, nedan kallad *NIS-lagen*) och verkar direkt under presidentens behörighet och överinseende ([180]). I synnerhet samlar den nationella underrättelsetjänsten in, sammanställer och distribuerar information om andra länder (och Nordkorea) ([181]), underrättelser som rör uppgiften att motverka spionage (däribland militär- och industrispionage), terrorism och internationella brottssyndikats verksamhet, underrättelser om vissa typer av brott som riktas mot allmän och nationell säkerhet (t.ex. inhemska uppror, utländsk aggression) och underrättelser som rör uppgiften att säkerställa it-säkerhet och förhindra eller motverka it-angrepp ([182]). I NIS-lagen, genom vilken den nationella underrättelsetjänsten är inrättad, fastställs dess uppgifter. Den innehåller även allmänna principer för all dess verksamhet. Som en allmän princip måste den nationella underrättelsetjänsten upprätthålla politisk neutralitet och skydda individens frihet och rättigheter ([183]). Direktören för den nationella underrättelsetjänsten har i uppgift att utarbeta allmänna riktlinjer som fastställer principerna, tillämpningsområdet och förfarandena för den nationella underrättelsetjänstens uppgifter i samband med insamling och användning av information, och ska rapportera dem till parlamentet ([184]). Parlamentet (genom sitt underrättelseutskott) kan kräva att riktlinjerna korrigeras eller kompletteras om den anser att de är olagliga eller orättvisa. Allmänt sett får direktören för den nationella underrättelsetjänsten och dess personal vid utförandet av sina uppgifter inte tvinga någon institution, organisation eller individ att göra något som de inte är skyldiga att göra eller hindra någon från att utöva sina rättigheter genom att missbruka sin myndighetsutövning ([185]). Dessutom måste all censur av post, avlyssning av telekommunikationer, insamling av lokaliseringsuppgifter, insamling av uppgifter om

([173]) Artikel 20 i förvaltningsprocesslagen. Denna tidsfrist gäller även för en begäran om bekräftelse av att en underlåtelse att agera är rättsstridig, se artikel 38.2 i förvaltningsprocesslagen.
([174]) Högsta domstolens beslut nr 90Nu6521 av den 28 juni 1991.
([175]) Artikel 68.1 i lagen om författningsdomstolen.
([176]) Författningsdomstolens beslut nr 99HeonMa194 av den 29 november 2001.
([177]) Artikel 40 i lagen om författningsdomstolen.
([178]) Artikel 69 i lagen om författningsdomstolen.
([179]) Artikel 75.3 i lagen om författningsdomstolen.
([180]) Artiklarna 2 och 4.2 i NIS-lagen.
([181]) Detta begrepp omfattar inte uppgifter om enskilda personer, utan allmän information om andra länder (trender, utveckling) och uppgifter om verksamhet som bedrivs av statliga aktörer i tredjeländer.
([182]) Artikel 3.1 i NIS-lagen.
([183]) Artiklarna 3.1, 6.2, 11 och 21. Se även reglerna om intressekonflikter, särskilt artiklarna 10 och 12.
([184]) Artikel 4.2 i NIS-lagen.
([185]) Artikel 13 i NIS-lagen.

kommunikationsbekräftelse eller registrering eller avlyssning av privat kommunikation som utförs av den nationella underrättelsetjänsten vara förenligt med lagen om post- och telehemlighet, lagen om lokaliseringsuppgifter eller straffprocesslagen ([186]). Maktmissbruk eller insamling av uppgifter i strid med dessa lagar är föremål för straffrättsliga påföljder ([187]).

Försvarets säkerhetskommando är en militär underrättelsetjänst som inrättats under försvarsministeriet. Det ansvarar för säkerhetsfrågor inom det militära, militära brottsutredningar (som omfattas av lagen om militärdomstolen) och den militära underrättelsetjänsten. Försvarets säkerhetskommando övervakar i allmänhet inte civila annat än om detta är nödvändigt för att utföra dess militära uppgifter. Personer som kan komma att undersökas är militär personal, militärens civila anställda, personer i militär utbildning, personer i militärreserv eller rekryteringstjänst och krigsfångar ([188]). Vid insamling av kommunikationsinformation för ändamål som rör den nationella säkerheten omfattas försvarets säkerhetskommando av de begränsningar och skyddsåtgärder som fastställs i lagen om post- och telehemlighet och genomförandedekretet till denna.

3.2. **Rättsliga grunder och begränsningar**

Lagen om post- och telehemlighet, lagen om åtgärder mot terrorism till skydd för medborgare och den allmänna säkerheten (*Act on Anti-Terrorism for the Protection of Citizens and Public Security*, nedan kallad *lagen mot terrorism*) och lagen om telekomoperatörer tillhandahåller rättsliga grunder för insamling av personuppgifter för ändamål som rör den nationella säkerheten och fastställer tillämpliga begränsningar och skyddsåtgärder ([189]). Dessa begränsningar och skyddsåtgärder, som beskrivs i följande avsnitt, säkerställer att insamling och behandling av uppgifter begränsas till vad som är absolut nödvändigt för att uppnå ett legitimt mål. Detta utesluter all massinsamling och godtycklig insamling av personuppgifter för ändamål som rör den nationella säkerheten.

3.2.1. *Insamling av kommunikationsinformation*

3.2.1.1. Underrättelsetjänsters insamling av kommunikationsinformation

3.2.1.1.1. Rättslig grund

I lagen om post- och telehemlighet ges underrättelsetjänsterna befogenhet att samla in kommunikationsuppgifter och föreskrivs att kommunikationsleverantörer ska samarbeta vid förfrågningar från dessa organ ([190]). Som beskrivs i avsnitt 2.2.2.1 görs i lagen om post- och telehemlighet en åtskillnad mellan insamling av kommunikationsinnehåll (dvs. *kommunikationsbegränsande åtgärder* såsom *teleavlyssning* eller *censur* ([191])) och insamling av *uppgifter om kommunikationsbekräftelse* ([192]).

Tröskeln för insamling av dessa två typer av information skiljer sig åt, men tillämpliga förfaranden och skyddsåtgärder är i stor utsträckning identiska ([193]). Insamling av uppgifter om kommunikationsbekräftelse (eller metauppgifter) får ske i syfte att förebygga hot mot den nationella säkerheten ([194]). En högre tröskel gäller för utförandet av kommunikationsbegränsande åtgärder (dvs. insamling av kommunikationsinnehåll), som endast får vidtas när den nationella säkerheten förväntas utsättas för allvarlig fara och insamling av underrättelser är nödvändigt för att förhindra sådan fara (dvs. om det finns en allvarlig risk för den nationella säkerheten och insamlingen är nödvändig för att förhindra denna) ([195]). Dessutom får åtkomst till kommunikationsinnehållet endast ske som en sista utväg för att säkerställa den nationella säkerheten, och ansträngningar måste göras för att minimera överträdelser av kommunikationens integritet ([196]). Även när vederbörligt godkännande eller tillstånd har erhållits måste sådana åtgärder upphöra omedelbart när de inte längre är nödvändiga, så att alla överträdelser av den enskildes kommunikationshemligheter begränsas till ett minimum ([197]).

3.2.1.1.2. Begränsningar och skyddsåtgärder för insamling av kommunikationsinformation som omfattar minst en sydkoreansk medborgare

Insamling av kommunikationsinformation (både innehåll och metauppgifter) där antingen en eller båda de personer som deltar i kommunikationen är sydkoreanska medborgare får endast ske med tillstånd från chefen för en

([186]) Artikel 14 i NIS-lagen.
([187]) Artiklarna 22 och 23 i NIS-lagen.
([188]) Artikel 1 i lagen om militärdomstolen.
([189]) När polisen och den nationella underrättelsetjänsten utreder brott med anknytning till nationell säkerhet agerar de på grundval av straffprocesslagen, medan försvarets säkerhetskommando är underställt lagen om militärdomstolen.
([190]) Artikel 15-2 i lagen om post- och telehemlighet.
([191]) Artiklarna 2.6 och 2.7 i lagen om post- och telehemlighet.
([192]) Artikel 2.11 i lagen om post- och telehemlighet.
([193]) Se även artikel 13-4.2 i lagen om post- och telehemlighet och artikel 37.4 i genomförandedekretet till lagen om post- och telehemlighet, där det föreskrivs att de förfaranden som är tillämpliga på insamling av kommunikationsinnehåll ska gälla i tillämpliga delar för insamling av uppgifter om kommunikationsbekräftelse.
([194]) Artikel 13-4 i lagen om post- och telehemlighet.
([195]) Artikel 7.1 i lagen om post- och telehemlighet.
([196]) Artikel 3.2 i lagen om post- och telehemlighet.
([197]) Artikel 2 i genomförandedekretet till lagen om post- och telehemlighet.

överdomstol ([198]). Begäran från underrättelsetjänsten måste göras skriftligen till en åklagare eller en överåklagarmyndighet ([199]). I begäran ska skälen till insamlingen anges (dvs. att den nationella säkerheten förväntas utsättas för allvarlig fara, eller att insamlingen är nödvändig för att förebygga hot mot den nationella säkerheten), tillsammans med material som stöder dessa skäl och fastställer ett prima facie-fall, samt närmare uppgifter om begäran (dvs. målsättningar, den individ eller de individer som berörs, omfattning, den faktiska insamlingsperioden, samt hur och var insamlingen kommer att äga rum) ([200]). Åklagaren eller överåklagarmyndigheten begär i sin tur tillstånd från en chef för överdomstolen ([201]). Chefen för överdomstolen får endast bevilja skriftligt tillstånd om han eller hon anser att ansökan är motiverad och avvisar begäran om han eller hon anser den vara ogrundad ([202]). I domstolsordern anges typ, syfte, mål, omfattning och den faktiska insamlingsperioden samt var och hur insamlingen får utföras ([203]).

Särskilda regler gäller om åtgärden syftar till att utreda en konspirationshandling som hotar den nationella säkerheten och om det föreligger en nödsituation som gör det omöjligt att genomgå ovannämnda förfaranden ([204]). Om dessa villkor är uppfyllda får underrättelsetjänsterna vidta övervakningsåtgärder utan föregående domstolsgodkännande ([205]). Omedelbart efter det att nödåtgärderna har vidtagits måste dock underrättelsetjänsten begära tillstånd från domstolen. Om tillstånd inte erhålls inom 36 timmar efter det att åtgärderna har vidtagits, måste de omedelbart upphöra ([206]). Insamling av information i nödsituationer måste alltid ske i enlighet med ett uttalande om nödcensur/nödavlyssning och den underrättelsetjänst som utför insamlingen måste föra ett register över eventuella nödåtgärder ([207]).

Om övervakningen slutförs inom en kort tid och domstolstillstånd utesluts ska chefen för behörig överåklagarmyndighet skicka ett meddelande om nödåtgärd som utarbetats av underrättelsetjänsten till ordföranden för den behöriga domstolen, som ska behålla registret över nödåtgärder ([208]). Detta gör det möjligt för domstolen att undersöka om insamlingen är lagenlig.

3.2.1.1.3. Begränsningar och skyddsåtgärder för insamling av kommunikationsinformation som omfattar minst en icke-sydkoreansk medborgare

För att samla in information om kommunikation mellan endast icke-sydkoreanska medborgare måste underrättelsetjänsterna få skriftligt förhandsgodkännande från presidenten ([209]). Sådan kommunikation kommer endast att samlas in för ändamål som rör den nationella säkerheten om de ingår i en av flera förtecknade kategorier, dvs. kommunikation mellan regeringstjänstemän eller andra individer från länder som är fientliga mot Sydkorea, utländska organ, grupper eller medborgare som misstänks bedriva verksamhet riktad mot Sydkorea ([210]), eller medlemmar i grupper på Koreahalvön som i praktiken inte omfattas av Sydkoreas suveränitet samt paraplyorganisationer till dessa som är baserade i utlandet ([211]). Om en part i kommunikationen däremot är en sydkoreansk medborgare och den andra en icke-sydkoreansk medborgare krävs domstolsgodkännande i enlighet med förfarandet i avsnitt 3.2.1.1.2.

Chefen för en underrättelsetjänst måste lägga fram en plan för de åtgärder som ska vidtas till direktören för den nationella underrättelsetjänsten ([212]). Direktören för den nationella underrättelsetjänsten granskar om planen är lämplig och lämnar i så fall in den till presidenten för godkännande ([213]). Den information som ska ingå i planen är densamma som den information som krävs för en ansökan om domstolstillstånd för att samla in information om sydkoreanska medborgare (enligt beskrivningen ovan) ([214]). I synnerhet ska skälen till insamlingen anges (dvs. att den nationella säkerheten förväntas utsättas för allvarlig fara, eller att insamlingen är nödvändig för att förebygga hot mot den

([198]) Artikel 7.1.1 i lagen om post- och telehemlighet. Den behöriga domstolen är den överdomstol som är behörig på den plats där den ena eller båda parter som är föremål för övervakningen har sin hemvist eller säte.
([199]) Artikel 7.3 i genomförandedekretet till lagen om post- och telehemlighet.
([200]) Artiklarna 7.3 och 6.4 i lagen om post- och telehemlighet.
([201]) Artikel 7.4 i genomförandedekretet till lagen om post- och telehemlighet. Åklagarens begäran till domstolen måste ange de huvudsakliga skälen till misstanke och, i den mån flera tillstånd begärs samtidigt, motiveringen till detta (se artikel 4 i genomförandedekretet till lagen om post- och telehemlighet).
([202]) Artiklarna 7.3, 6.5 och 6.9 i lagen om post- och telehemlighet.
([203]) Artiklarna 7.3 och 6.6 i lagen om post- och telehemlighet.
([204]) Artikel 8 i lagen om post- och telehemlighet.
([205]) Artikel 8.1 i lagen om post- och telehemlighet.
([206]) Artikel 8.2 i lagen om post- och telehemlighet.
([207]) Artikel 8.4 i lagen om post- och telehemlighet. Se avsnitt 2.2.2.2 för nödåtgärder i samband med brottsbekämpning.
([208]) Artikel 8.5 och 8.7 i lagen om post- och telehemlighet. I detta meddelande ska anges syfte, mål, tillämpningsområde, tidsperiod, platsen för genomförandet och övervakningsmetod, samt skälen för att inte ha lämnat in en begäran innan åtgärden genomfördes (artikel 8.6 i lagen om post- och telehemlighet).
([209]) Artikel 7.1.2 i lagen om post- och telehemlighet.
([210]) Detta gäller verksamhet som hotar nationens existens och säkerhet, den demokratiska ordningen eller folkets överlevnad och frihet.
([211]) Om en part är en person som avses i artikel 7.1.2 i lagen om post- och telehemlighet och den andra är okänd eller inte kan specificeras kommer det förfarande som föreskrivs i artikel 7.1.2 att tillämpas.
([212]) Artikel 8.1 i genomförandedekretet till lagen om post- och telehemlighet. Direktören för den nationella underrättelsetjänsten utses av presidenten efter bekräftelse från parlamentet (artikel 7 i NIS-lagen).
([213]) Artikel 8.2 i genomförandedekretet till lagen om post- och telehemlighet.
([214]) Artikel 8.3 i genomförandedekretet till lagen om post- och telehemlighet jämförd med artikel 6.4 i lagen om post- och telehemlighet.

nationella säkerheten), de huvudsakliga skälen till misstanke, tillsammans med de material som stöder dessa skäl och fastställer ett prima facie-fall, samt närmare uppgifter om begäran (dvs. målsättningar, den individ eller de individer som berörs, omfattning, den faktiska insamlingsperioden samt hur och var insamlingen kommer att äga rum). Om flera tillstånd begärs samtidigt, ska anledningen och grunderna till detta anges ([215]).

I nödsituationer ([216]) måste förhandsgodkännande inhämtas från den minister som den berörda underrättelsetjänsten tillhör. I detta fall måste underrättelsetjänsten dock begära godkännande från presidenten omedelbart efter det att nödåtgärderna har vidtagits. Om en underrättelsetjänst inte erhåller godkännande inom 36 timmar efter det att ansökan lämnats in, måste insamlingen omedelbart upphöra ([217]). I sådana fall kommer den insamlade informationen alltid att förstöras.

3.2.1.1.4. Allmänna begränsningar och skyddsåtgärder

När underrättelsetjänsterna begär samarbete med privata enheter måste de förse dem med domstolsordern/presidentens tillstånd eller en kopia av försättsbladet till ett uttalande om nödcensur, som den förpliktade enheten måste förvara i sina register ([218]). Enheter som ombeds lämna ut information till underrättelsetjänster på grundval av lagen om post- och telehemlighet får vägra att göra detta om tillståndet eller uttalandet om nödcensur avser fel identifierare (t.ex. ett telefonnummer som tillhör en annan person än den identifierade). Under alla förhållanden får lösenord som används för kommunikation inte lämnas ut ([219]).

Underrättelsetjänster kan anförtro genomförandet av kommunikationsbegränsande åtgärder eller insamling av uppgifter om kommunikationsbekräftelse till ett postkontor eller en leverantör av telekommunikationstjänster (enligt definitionen i lagen om telekomoperatörer) ([220]). Både den berörda underrättelsetjänsten och den leverantör som tar emot en begäran om samarbete måste föra register som anger orsaken till att åtgärderna begärs, datum för genomförandet eller samarbetet och mot vad åtgärderna riktas (t.ex. post, telefon, e-post) i tre år ([221]). Leverantörer av telekommunikationstjänster som tillhandahåller uppgifter om kommunikationsbekräftelse måste föra register med information om hur ofta insamlingen sker i sju års tid och två gånger per år rapportera till ministern för vetenskap och IKT ([222]).

Underrättelsetjänsterna ska lämna rapporter om den information de har samlat in och resultatet av övervakningen till direktören för den nationella underrättelsetjänsten ([223]). När det gäller insamling av uppgifter om kommunikationsbekräftelse ska register föras över att en begäran om sådana uppgifter gjorts, liksom den skriftliga begäran och den institution som förlitat sig på den ([224]).

Insamling av både kommunikationsinnehåll och uppgifter om kommunikationsbekräftelse får endast pågå i högst fyra månader och ska om det eftersträvade målet uppnås under tiden omedelbart upphöra ([225]). Om villkoren för tillståndet kvarstår får perioden förlängas med upp till fyra månader med domstolens tillstånd eller presidentens godkännande. Ansökan om tillstånd att utöka övervakningsåtgärderna ska göras skriftligen med angivande av skälen till att en utökning begärs. Ansökan ska även omfatta underlag ([226]).

Beroende på den rättsliga grunden för insamlingen underrättas i allmänhet enskilda personer när deras kommunikation samlas in. Oavsett om den information som samlas in gäller kommunikationsinnehåll eller uppgifter om kommunikationsbekräftelse, och oavsett om informationen erhållits genom det ordinarie förfarandet eller i en nödsituation, ska underrättelsetjänstens chef skriftligen underrätta den berörda personen om övervakningsåtgärden inom 30 dagar från den dag då övervakningen avslutades ([227]). I underrättelsen ska följande anges: 1) det faktum att informationen har

([215]) Artiklarna 8.3 och 4 i genomförandedekretet till lagen om post- och telehemlighet.
([216]) Dvs. när åtgärden gäller en konspirationshandling som hotar den nationella säkerheten och det inte finns tillräckligt med tid för att inhämta godkännande från presidenten, när underlåtenhet att vidta nödåtgärder kan skada den nationella säkerheten (artikel 8.8 i lagen om post- och telehemlighet).
([217]) Artikel 8.9 i lagen om post- och telehemlighet.
([218]) Artikel 9.2 i lagen om post- och telehemlighet och artikel 12 i genomförandedekretet till lagen om post- och telehemlighet.
([219]) Artikel 9.4 i lagen om post- och telehemlighet.
([220]) Artikel 13 i genomförandedekretet till lagen om post- och telehemlighet.
([221]) Artikel 9.3 i lagen om post- och telehemlighet och artikel 17.2 i genomförandedekretet till lagen om post- och telehemlighet. Denna tidsperiod gäller inte uppgifter om kommunikationsbekräftelse (se artikel 39 i genomförandedekretet till lagen om post- och telehemlighet).
([222]) Artikel 13.7 i lagen om post- och telehemlighet och artikel 39 i genomförandedekretet till lagen om post- och telehemlighet.
([223]) Artikel 18.3 i genomförandedekretet till lagen om post- och telehemlighet.
([224]) Artikel 13.5 och 13-4.3 i lagen om post- och telehemlighet.
([225]) Artikel 7.2 i lagen om post- och telehemlighet.
([226]) Artikel 7.2 i lagen om post- och telehemlighet och artikel 5 i genomförandedekretet till lagen om post- och telehemlighet.
([227]) Artikel 9-2.3 i lagen om post- och telehemlighet. I enlighet med artikel 13-4 i lagen om post- och telehemlighet gäller detta både insamling av kommunikationsinnehåll och uppgifter om kommunikationsbekräftelse.

samlats in, 2) det verkställande organet och 3) genomförandeperioden. Underrättelsen får dock skjutas upp om det är sannolikt att den skulle äventyra den nationella säkerheten eller skada människors liv och fysiska säkerhet ([228]). Underrättelse ska lämnas inom 30 dagar så snart skälen för uppskjutande av underrättelsen inte längre föreligger ([229]).

Detta krav på underrättelse gäller dock endast insamling av information där minst en av parterna är sydkoreansk medborgare. Till följd av detta kommer icke-sydkoreanska medborgare endast att underrättas när deras kommunikation med sydkoreanska medborgare samlas in. Det finns därför inget krav på underrättelse när endast kommunikation mellan icke-sydkoreanska medborgare samlas in.

Innehållet i all kommunikation samt uppgifter om kommunikationsbekräftelse som inhämtats genom övervakning på grundval av lagen om post- och telehemlighet får endast användas 1) för utredning, lagföring eller förebyggande av vissa brott, 2) för disciplinära förfaranden, 3) för rättsliga förfaranden där en part kopplad till kommunikationen förlitar sig på den i en skadeståndstalan eller 4) på grundval av annan lagstiftning ([230]).

3.2.1.2. Polis eller åklagares insamling av kommunikationsinformation för ändamål som rör den nationella säkerheten

Polis eller åklagare får samla in kommunikationsinformation (både kommunikationsinnehåll och uppgifter om kommunikationsbekräftelse) för ändamål som rör den nationella säkerheten på samma villkor som beskrivs i avsnitt 3.2.1.1 I nödsituationer ([231]) är det tillämpliga förfarandet det som beskrevs tidigare med avseende på insamlingen av kommunikationsinnehåll för brottsbekämpande ändamål i nödsituationer (dvs. artikel 8 i lagen om post- och telehemlighet).

3.2.2. *Insamling av uppgifter om misstänkta terrorister*

3.2.2.1. Rättslig grund

Lagen mot terrorism ger direktören för den nationella underrättelsetjänsten befogenhet att samla in information om misstänkta terrorister ([232]). *Misstänkt terrorist* definieras som en medlem av en terroristgrupp ([233]), en person som har propagerat för en terroristgrupp (genom att främja och sprida en terroristgrupps idéer eller taktik), samlat in eller bidragit till finansiering av terrorism ([234]) eller deltagit i annan verksamhet som förbereder, konspirerar, sprider eller uppmuntrar till terrorism, eller en person som det finns goda skäl att misstänka för att ha bedrivit sådan verksamhet ([235]). Som en allmän regel måste varje offentlig tjänsteman som tillämpar lagen mot terrorism respektera de grundläggande rättigheter som fastställs i den sydkoreanska författningen ([236]).

Lagen mot terrorism fastställer inte i sig några särskilda befogenheter, begränsningar och garantier för insamling av uppgifter om misstänkta terrorister, utan hänvisar snarare till förfarandena i andra lagar. Direktören för den nationella underrättelsetjänsten kan på grundval av lagen mot terrorism samla in 1) information om inresa till och utresa från Sydkorea, 2) information om finansiella transaktioner och 3) kommunikationsinformation. Beroende på vilken typ av uppgifter som efterfrågas finns de relevanta förfarandekraven i immigrationslagen och tullagen, lagen om finansiella transaktioner respektive lagen om post- och telehemlighet ([237]). När det gäller insamling av uppgifter om inresa till och avresa från Sydkorea hänvisas i lagen mot terrorism till de förfaranden som fastställs i immigrationslagen och tullagen.

([228]) Artikel 9-2.4 i lagen om post- och telehemlighet.
([229]) Artiklarna 13-4.2 och 9-2.6 i lagen om post- och telehemlighet.
([230]) Artiklarna 5.1–5.2, 12 och 13-5 i lagen om post- och telehemlighet.
([231]) Dvs. om åtgärden gäller en konspirationshandling som hotar den nationella säkerheten och det föreligger en nödsituation som gör det omöjligt att genomgå det ordinarie förfarandet för godkännande (artikel 8.1 i lagen om post- och telehemlighet).
([232]) Artikel 9 i lagen mot terrorism.
([233]) *Terroristgrupp* definieras som en grupp terrorister som angetts av Förenta nationerna (artikel 2.2 i lagen mot terrorism).
([234]) *Terrorism* definieras i artikel 2.1 i lagen mot terrorism som ett agerande som utförs i syfte att hindra utövandet av befogenheter som vilar hos staten, ett lokal styrelseorgan eller en utländsk myndighet (bl.a. lokala styrelseorgan och internationella organisationer), eller i syfte att förmå dessa enheter att agera på ett sätt som inte är obligatoriskt för dem, eller för att hota allmänheten. Detta omfattar a) att döda en person eller utgöra en risk för en persons liv genom att orsaka kroppsskada eller gripa, spärra in, kidnappa eller ta en person som gisslan, b) vissa typer av beteenden som är riktade mot ett luftfartyg (t.ex. krascha, kapa eller skada ett luftfartyg under flygning), c) vissa typer av beteenden som rör ett fartyg (t.ex. beslagtagande av ett fartyg eller en marin konstruktion i drift, förstörelse av ett fartyg eller en marin konstruktion i drift eller tillfogande av skada på ett fartyg eller en marin konstruktion i en sådan omfattning att säkerheten äventyras, däribland skada på den last som befinner sig på ett fartyg eller en marin konstruktion i drift), d) att placera, detonera eller på annat sätt använda ett biokemiskt, explosivt eller brandfarligt vapen eller anordning i syfte att orsaka dödsfall, allvarlig skada eller allvarlig materiell skada, eller som har sådan inverkan på vissa typer av fordon eller anläggningar (t.ex. tåg, spårvagnar, motorfordon, allmänna parker och stationer, anläggningar för tillhandahållande av elektricitet, gas, telekommunikation osv.), e) vissa typer av beteenden som rör kärnmaterial, radioaktiva material eller kärntekniska anläggningar (t.ex. att skada människoliv, kroppar eller egendom eller på annat sätt störa allmänhetens säkerhet genom att förstöra en kärnreaktor eller felaktigt handha radioaktiva material osv.).
([235]) Artikel 2.3 i lagen mot terrorism.
([236]) Artikel 3.3 i lagen mot terrorism.
([237]) Artikel 9.1 i lagen mot terrorism.

Dessa rättsakter innehåller dock för närvarande inga sådana befogenheter. När det gäller insamling av kommunikationsinformation och information om finansiella transaktioner hänvisas i lagen mot terrorism till begränsningar och skyddsåtgärder i lagen om post- och telehemlighet (som beskrivs närmare nedan) och i lagen om finansiella transaktioner (som förklarades i avsnitt 2.1 är denna senare lag inte relevant i samband med beslutet om adekvat skyddsnivå).

Dessutom anges i artikel 9.3 i lagen mot terrorism att direktören för den nationella underrättelsetjänsten får begära personuppgifter eller lokaliseringsuppgifter gällande en misstänkt terrorist från personuppgiftsansvariga ([238]) eller leverantörer av lokaliseringsuppgifter ([239]). Denna möjlighet är begränsad till begäranden om frivilligt utlämnande, som personuppgiftsansvariga och leverantörer av lokaliseringsuppgifter inte är skyldiga att svara på, och under alla omständigheter får de endast göra detta i enlighet med PIPA och lagen om lokaliseringsuppgifter (se avsnitt 3.2.2.2).

3.2.2.2. Begränsningar och skyddsåtgärder för frivilligt utlämnande enligt PIPA och lagen om lokaliseringsuppgifter

Ansökningar om frivilligt samarbete enligt lagen mot terrorism måste begränsas till uppgifter om misstänkta terrorister (se avsnitt 3.2.2.1). Varje sådan begäran från den nationella underrättelsetjänsten måste följa principerna om laglighet, nödvändighet och proportionalitet som följer av den sydkoreanska författningen (artiklarna 12.1 och 37.2) ([240]) samt kraven enligt PIPA för insamling av personuppgifter (artikel 3.1 i PIPA, se avsnitt 1.2). I NIS-lagen anges vidare att den nationella underrättelsetjänsten inte får tvinga någon institution, organisation eller individ att göra något som de inte är skyldiga att göra eller hindra någon från att utöva sina rättigheter genom att missbruka sin offentliga makt ([241]). En överträdelse av detta förbud kan leda till straffrättsliga påföljder ([242]).

Personuppgiftsansvariga och leverantörer av lokaliseringsuppgifter som tar emot en begäran från den nationella underrättelsetjänsten på grundval av lagen mot terrorism behöver inte efterkomma den. De kan samarbeta på frivillig basis, men får endast göra detta med beaktande av kraven i PIPA och lagen om lokaliseringsuppgifter. Vad gäller efterlevnad av PIPA måste personuppgiftsansvariga i synnerhet ta hänsyn till den registrerades intressen och får inte röja informationen om det är sannolikt att det skulle utgöra en otillbörlig överträdelse av den enskildes eller tredje mans intressen ([243]). I enlighet med anmälan nr 2021-1 om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter måste den berörda personen dessutom underrättas om utlämnandet. I undantagsfall får en sådan underrättelse skjutas upp, särskilt om och så länge som underrättelsen skulle äventyra en pågående brottsutredning eller sannolikt skada en annan persons liv eller kropp, om dessa rättigheter eller intressen är uppenbart överordnade den registrerades rättigheter ([244]).

3.2.2.3. Begränsningar och skyddsåtgärder enligt lagen om post- och telehemlighet

På grundval av lagen mot terrorism får underrättelsetjänster endast samla in kommunikationsinformation (både kommunikationsinnehåll och uppgifter om kommunikationsbekräftelse) när så är nödvändigt för att bekämpa terrorism, dvs. verksamhet som rör förebyggande av och motåtgärder mot terrorism. De förfaranden enligt lagen om post- och telehemlighet som beskrivs i avsnitt 3.2.1 gäller för insamling av kommunikationsinformation i syfte att bekämpa terrorism.

3.2.3. *Teleoperatörers frivilliga utlämnande av uppgifter*

På grundval av lagen om telekomoperatörer får teleoperatörer efterkomma en begäran om att lämna ut ”kommunikationsuppgifter” från en underrättelsetjänst som har för avsikt att samla in uppgifterna för att förhindra ett hot mot den nationella säkerheten ([245]). Varje sådan begäran måste följa principerna om laglighet, nödvändighet och proportionalitet som följer av den sydkoreanska författningen (artiklarna 12.1 och 37.2) ([246]) samt kraven enligt PIPA för insamling av personuppgifter (artikel 3.1 i PIPA, se avsnitt 1.2). Dessutom gäller samma begränsningar och skyddsåtgärder som när det gäller frivilligt utlämnande för brottsbekämpande ändamål (se avsnitt 2.2.3) ([247]).

([238]) Enligt definitionen i artikel 2 i PIPA, dvs. en offentlig institution, en juridisk person, en organisation, en enskild person osv. som direkt eller indirekt behandlar personuppgifter för officiella eller affärsmässiga ändamål.

([239]) Enligt definitionen i artikel 5 i lagen om skydd, användning osv. av lokaliseringsuppgifter (*Act on the Protection, Use, etc. of Location Information*, nedan kallad *lagen om lokaliseringsuppgifter*), dvs. alla som har fått tillstånd från Sydkoreas kommunikationskommitté att bedriva verksamhet relaterad till lokaliseringsuppgifter.

([240]) Se även artikel 3.2 och 3.3 i lagen mot terrorism.

([241]) Artikel 11.1 i NIS-lagen.

([242]) Artikel 19 i NIS-lagen.

([243]) Artikel 18.2 i PIPA.

([244]) Anmälan nr 2021-1 från nämnden för skydd av personuppgifter om tilläggsregler för tolkning och tillämpning av lagen om skydd av personuppgifter, avsnitt III, 2 iii).

([245]) Artikel 83.3 i lagen om telekomoperatörer.

([246]) Se även artikel 3.2 och 3.3 i lagen mot terrorism.

([247]) I synnerhet ska begäran vara skriftlig och däri ska anges skälen till begäran samt länken till den relevanta användaren och omfattningen av den begärda informationen. Teleoperatören ska dessutom föra register och två gånger per år rapportera till ministern för vetenskap och IKT.

En teleoperatör behöver inte efterkomma begäran, men får göra det på frivillig basis och då endast i enlighet med PIPA. I detta avseende gäller samma skyldigheter för teleoperatörer som när de tar emot begäranden från brottsbekämpande myndigheter, däribland vad gäller underrättelse till enskilda personer, såsom förklaras mer ingående i avsnitt 2.2.3.

3.3. **Tillsyn**

Olika organ övervakar de sydkoreanska underrättelsetjänsternas verksamhet. Övervakning av försvarets säkerhetskommando utförs av försvarsministeriet i enlighet med ministeriets direktiv om genomförande av internrevision. Den nationella underrättelsetjänsten är föremål för tillsyn av den verkställande makten, parlamentet och andra oberoende organ, vilket förklaras närmare nedan.

3.3.1. *Ombudet för skydd av de mänskliga rättigheterna*

När underrättelsetjänster samlar in information om misstänkta terrorister föreskrivs i lagen mot terrorism tillsyn som utförs av kommissionen för terrorismbekämpning och ombudet för skydd av de mänskliga rättigheterna ([248]).

Kommissionen för terrorismbekämpning utvecklar bland annat strategier för terrorismbekämpning och övervakar genomförandet av åtgärder för terrorismbekämpning samt de olika behöriga myndigheternas verksamhet på området terrorismbekämpning ([249]). Kommissionen leds av premiärministern och består av flera ministrar och chefer för statliga organ, däribland utrikesministern, justitieministern, försvarsministern, ministern för inrikesfrågor och säkerhet, direktören för den nationella underrättelsetjänsten, generalkommissionären för den nationella polismyndigheten och ordföranden för kommissionen för finansiella tjänster ([250]). När utredningar utförs som avser terrorismbekämpning och spårande av misstänkta terrorister för att samla in uppgifter eller material som krävs för att bekämpa terrorism, måste direktören för den nationella underrättelsetjänsten rapportera till ordföranden för kommissionen för terrorismbekämpning (dvs. premiärministern) ([251]).

Genom lagen mot terrorism inrättas dessutom ombudet för skydd av de mänskliga rättigheterna för att skydda enskilda personers grundläggande rättigheter mot överträdelser som orsakas av terrorismbekämpning ([252]). Ombudet för skydd av de mänskliga rättigheterna utses av ordföranden för terrorismbekämpningskommissionen bland personer som innehar de kvalifikationer som anges i genomförandedekretet till lagen mot terrorism (dvs. vara advokat med minst tio års arbetslivserfarenhet, eller ha sakkunskap på området mänskliga rättigheter och tjänstgöra eller ha tjänstgjort (åtminstone) som biträdande professor i minst tio år, eller ha tjänstgjort som högre tjänsteman vid ett statligt organ eller lokala styrelseorgan, eller ha minst tio års arbetslivserfarenhet på området mänskliga rättigheter, t.ex. vid en icke-statlig organisation) ([253]). Ombudet för skydd av de mänskliga rättigheterna utses för två år (med möjlighet till förnyad mandatperiod) och kan endast avsättas från sitt uppdrag på särskilda, begränsade grunder och när starka skäl föreligger, t.ex. åtal i ett brottmål som rör hans eller hennes arbetsuppgifter, avslöjande av hemlig information eller på grund av långvarig psykisk eller fysisk oförmåga ([254]).

När det gäller befogenheter kan ombudet för skydd av de mänskliga rättigheterna utfärda rekommendationer för att förbättra hur organ som deltar i terrorismbekämpning skyddar de mänskliga rättigheterna, och behandla civila framställningar (se avsnitt 3.4.3) ([255]). Om det rimligen kan fastställas att det föreligger en kränkning av de mänskliga rättigheterna vid tjänsteutövning kan ombudet för skydd av de mänskliga rättigheterna rekommendera chefen för det ansvariga organet att korrigera en sådan överträdelse ([256]). Det ansvariga organet måste i sin tur underrätta ombudet för skydd av de mänskliga rättigheterna om de åtgärder som vidtagits för att genomföra en sådan rekommendation ([257]). Om ett organ skulle underlåta att genomföra en rekommendation från ombudet för skydd av de mänskliga rättigheterna lyfts frågan till kommissionen, däribland dess ordförande, premiärministern. Hittills har det inte förekommit några fall där rekommendationer från ombudet för skydd av de mänskliga rättigheterna inte har genomförts.

3.3.2. *Parlamentet*

Såsom beskrivs i avsnitt 2.3.2 får parlamentet utreda och kontrollera myndigheter och i detta sammanhang begära att handlingar lämnas ut och tvinga vittnen att framträda. När det gäller frågor som omfattas av den nationella underrättelsetjänsten behörighet utförs denna parlamentariska tillsyn av parlamentets underrättelseutskott ([258]). Direktören för den nationella underrättelsetjänsten, som övervakar byråns tjänsteutövning, rapporterar till underrättelseutskottet (samt

([248]) Artikel 7 i lagen mot terrorism.
([249]) Artikel 5.3 i lagen mot terrorism.
([250]) Artikel 3.1 i genomförandedekretet till lagen mot terrorism.
([251]) Artikel 9.4 i lagen mot terrorism.
([252]) Artikel 7 i lagen mot terrorism.
([253]) Artikel 7.1 i genomförandedekretet till lagen mot terrorism.
([254]) Artikel 7.3 i genomförandedekretet till lagen mot terrorism.
([255]) Artikel 8.1 i genomförandedekretet till lagen mot terrorism.
([256]) Artikel 9.1 i genomförandedekretet till lagen mot terrorism. Ombudet för skydd av de mänskliga rättigheterna beslutar självständigt om antagandet av rekommendationer, men måste rapportera sådana rekommendationer till ordföranden för kommissionen för terrorismbekämpning.
([257]) Artikel 9.2 i genomförandedekretet till lagen mot terrorism.
([258]) Artiklarna 36 och 37.1.16 i lagen om parlamentet.

till presidenten) ([259]). Underrättelseutskottet får också själv begära en rapport i en viss fråga, och direktören för den nationella underrättelsetjänsten ska svara på detta utan dröjsmål ([260]). Han eller hon får endast vägra att ge svar till eller vittna inför underrättelseutskottet när det gäller statshemligheter som rör militära eller diplomatiska frågor eller frågor med anknytning till Nordkorea, där ett offentliggörande kan ha en allvarlig inverkan på landets framtid ([261]). I sådana fall kan underrättelseutskottet begära en förklaring från premiärministern. Om en sådan förklaring inte lämnas inom sju dagar efter det att begäran lämnats in, får svaret eller vittnesmålet inte längre vägras.

Om parlamentet finner olaglig eller otillbörlig verksamhet kan den begära att den berörda myndigheten vidtar korrigerande åtgärder, däribland beviljande av kompensation, disciplinära åtgärder och förbättrade interna förfaranden ([262]). Efter en sådan begäran måste myndigheten agera utan dröjsmål och rapportera resultatet till parlamentet. Det finns särskilda regler för parlamentarisk tillsyn av användningen av kommunikationsbegränsande åtgärder (dvs. insamling av kommunikationsinnehåll) inom ramen för lagen om post- och telehemlighet ([263]). När det gäller det sistnämnda kan parlamentet begära en rapport från underrättelsetjänsternas chefer om särskilda kommunikationsbegränsande åtgärder. Dessutom får den utföra inspektioner på plats av avlyssningsutrustning. Slutligen måste underrättelsetjänster som har samlat in och operatörer som har lämnat ut innehållsuppgifter för ändamål som rör den nationella säkerheten rapportera om sådant utlämnande på begäran av parlamentet.

3.3.3. *Revisions- och kontrollstyrelsen*

Revisions- och kontrollstyrelsen utför samma tillsynsuppgifter med avseende på underrättelsetjänster som på området brottsbekämpning (se avsnitt 2.3.2) ([264]).

3.3.4. *Nämnden för skydd av personuppgifter*

När det gäller databehandling för ändamål som rör den nationella säkerheten, däribland insamlingsfasen, utför nämnden för skydd av personuppgifter ytterligare tillsyn. Som förklaras närmare i avsnitt 1.2 omfattar detta de allmänna principer och skyldigheter som anges i artiklarna 3 och 58.4 i PIPA samt utövandet av individuella rättigheter som garanteras genom artikel 4 i PIPA. Dessutom omfattar nämndens tillsyn enligt artiklarna 7-8.3, 7-8.4 och 7-9.5 i PIPA även eventuella överträdelser av bestämmelserna i särskilda lagar där begränsningar och skyddsåtgärder fastställs när det gäller insamling av personuppgifter, t.ex. lagen om post- och telehemlighet, lagen mot terrorism och lagen om telekomoperatörer. Med hänsyn till kraven i artikel 3.1 i PIPA om laglig och korrekt insamling av personuppgifter utgör varje överträdelse av dessa rättsakter en överträdelse av PIPA. Nämnden för skydd av personuppgifter har därför befogenhet att utreda ([265]) överträdelser av de lagar som reglerar tillgången till uppgifter för ändamål som rör den nationella säkerheten samt av bestämmelserna om databehandling i PIPA, utfärda råd för förbättring, vidta korrigerande åtgärder, rekommendera disciplinära åtgärder och hänskjuta potentiella brott till de berörda utredningsmyndigheterna ([266]).

3.3.5. *Den nationella människorättskommissionen*

Den nationella människorättskommissionens tillsyn gäller på samma sätt för underrättelsetjänster som för andra statliga myndigheter (se avsnitt 2.3.2).

3.4. **Prövning för enskilda**

3.4.1. *Prövning inför ombudet för skydd av de mänskliga rättigheterna*

När det gäller insamling av personuppgifter inom ramen för terrorismbekämpning tillhandahåller ombudet för skydd av de mänskliga rättigheterna en särskild möjlighet till prövning som inrättats inom ramen för kommissionen för terrorismbekämpning. Ombudet för skydd av de mänskliga rättigheterna behandlar civila framställningar som rör kränkningar av de mänskliga rättigheterna till följd av terrorismbekämpning ([267]). Han eller hon kan rekommendera korrigerande åtgärder och det berörda organet måste rapportera till ombudet om de åtgärder som vidtagits för att genomföra en sådan rekommendation. Det finns inget stående krav på att enskilda personer ska lämna in ett klagomål till ombudet för skydd av de mänskliga rättigheterna. Till följd av detta kommer ombudet för skydd av de mänskliga rättigheterna att behandla ett klagomål även om den berörda personen inte kan påvisa någon skada i det skede som avser upptagande till prövning.

([259]) Artikel 18 i NIS-lagen.
([260]) Artikel 15.2 i NIS-lagen.
([261]) Artikel 17.2 i NIS-lagen. *Statshemligheter* definieras som *fakta, varor eller kunskap som klassificeras som statshemligheter, som endast ett begränsat antal personer har tillgång till och som inte får lämnas ut till något annat land eller organisation för att undvika allvarliga olägenheter för den nationella säkerheten*, se artikel 13.4 i NIS-lagen.
([262]) Artikel 16.2 i lagen om kontroll och utredning av statsförvaltningen.
([263]) Artikel 15 i lagen om post- och telehemlighet.
([264]) Liksom när det gäller parlamentets underrättelseutskott får direktören för den nationella underrättelsetjänsten endast vägra att svara revisions- och kontrollstyrelsen på frågor som utgör statshemligheter och om ett offentliggörande skulle ha en allvarlig inverkan på den nationella säkerheten (artikel 13.1 i NIS-lagen).
([265]) Artikel 63 i PIPA.
([266]) Artiklarna 61.2, 65.1, 65.2 och 64.4 i PIPA.
([267]) Artikel 8.1 led 2 i genomförandedekretet till lagen mot terrorism.

3.4.2. *Prövningsmekanismer som finns tillgängliga enligt PIPA*

Enskilda personer får utöva sina rättigheter till tillgång, rättelse, radering och upphörande enligt PIPA när det gäller personuppgifter som behandlas för ändamål som rör den nationella säkerheten ([268]). Begäran om att utöva dessa rättigheter kan inges direkt till underrättelsetjänsten, eller indirekt via nämnden för skydd av personuppgifter. Underrättelsetjänsten kan dock fördröja, begränsa eller neka utövandet av rättigheten i den utsträckning och så länge som det är nödvändigt och proportionellt för att skydda ett viktigt syfte i allmänhetens intresse (t.ex. i den mån och så länge som beviljandet av rättigheten skulle äventyra en pågående utredning eller hota den nationella säkerheten), eller om beviljandet av rättigheten kan skada en tredje parts liv eller kropp. Om begäran avslås eller begränsas ska personen utan dröjsmål underrättas om skälen till detta.

I enlighet med artikel 58.4 i PIPA (krav på att säkerställa lämplig hantering av enskilda klagomål) och artikel 4.5 i PIPA (rätt till lämplig prövning genom ett skyndsamt och rättvist förfarande för skador som uppstår till följd av behandlingen av personuppgifter) ska enskilda personer dessutom ha rätt till prövning. Detta inbegriper rätten att rapportera en påstådd överträdelse till integritetstjänsten som drivs av Sydkoreas byrå för internet och säkerhet och att lämna in ett klagomål till nämnden för skydd av personuppgifter ([269]). Dessa möjligheter till prövning finns både vid eventuella överträdelser av reglerna i särskilda lagar som fastställer begränsningar och skyddsåtgärder i fråga om insamling av personuppgifter för ändamål som rör den nationella säkerheten, och av PIPA. Såsom förklaras i anmälan nr 2021-1 kan en enskild person i EU inge ett klagomål till nämnden för skydd av personuppgifter via sin nationella dataskyddsmyndighet. I dessa fall kommer nämnden för skydd av personuppgifter att underrätta personen via den nationella dataskyddsmyndigheten när undersökningen har avslutats (däribland, i tillämpliga fall, information om de korrigerande åtgärder som vidtagits). Nämndens beslut eller underlåtenhet att agera kan ytterligare överklagas till de sydkoreanska domstolarna enligt förvaltningsprocesslagen.

3.4.3. *Prövning inför den nationella människorättskommissionen*

Möjligheten att erhålla enskild prövning inför den nationella människorättskommissionen gäller på samma sätt för underrättelsetjänster som för andra statliga myndigheter (se avsnitt 2.4.2).

3.4.4. *Rättslig prövning*

Liksom när det gäller brottsbekämpande myndigheters verksamhet kan enskilda personer på olika vägar erhålla rättslig prövning gentemot underrättelsetjänster när det gäller överträdelser av ovannämnda begränsningar och skyddsåtgärder.

För det första kan enskilda personer få ersättning för skador enligt lagen om statlig kompensation. I ett fall beviljades exempelvis ersättning för olaglig övervakning utförd av försvarskommandot (föregångaren till försvarets säkerhetskommando) ([270]).

För det andra tillåts enligt förvaltningsprocesslagen enskilda personer att bestrida förvaltningsorgams beslut och underlåtelse att agera. Detta inbegriper underrättelsetjänster ([271]).

Slutligen kan enskilda personer på grundval av lagen om författningsdomstolen inge en författningsklagan till författningsdomstolen avseende åtgärder som vidtas av underrättelsetjänster.

([268]) Artikel 3.5 och artikel 4.1, 4.3 och 4.4 i PIPA.
([269]) Artiklarna 62 och 63.2 i PIPA.
([270]) Högsta domstolens beslut nr 96Da42789 av den 24 juli 1998.
([271]) Artiklarna 3 och 4 i förvaltningsprocesslagen.