Flowplayer Data Processing Agreement

THIS DATA PROCESSING AGREEMENT, including the selected modules of the Model Clauses and Annexes ("DPA"), forms part of and is subject to the Flowplayer Terms of Service or other written or electronic agreement ("Main Agreement") between you, the purchaser of Flowplayer products and services ("Customer") and Flowplayer AB ("Flowplayer," "we," "us," "our"). Customer and Flowplayer may be referred to as a "party" and together as the "parties." This DPA is incorporated into and made a part of the Main Agreement. In the event of a conflict between the terms and conditions of this DPA and the Main Agreement, the terms and conditions of this DPA supersede and control to the extent of such conflict.

Instructions for Entering into DPA

To enter into this DPA, Customer must: (a) be a Flowplayer Video customer; (b) complete the signature block below by signing and providing all relevant information; and (c) submit the completed and signed DPA to legal@flowplayer.com. This DPA will only be effective if executed and submitted to Flowplayer accurately and in accordance with (a)-(c). If Customer makes any deletions or other revisions to this DPA, this DPA will become null and void. Notwithstanding expiry or termination of the Main Agreement, this DPA and the Model Clauses (if applicable) will remain in effect until deletion by Flowplayer of all personal data covered by this DPA. This DPA incorporates the following Annexes:

Annex 1 - Details of Processing
Annex 2 - Security Measures
Annex 3 - List of Sub-Processors

1. **Definitions**

"Affiliate" means an entity that directly or indirectly controls is controlled by or is under common control with an entity, where control means an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully-diluted basis) then outstanding of the entity in question.

"Authorized User" means a user who completes a registration form within the Service (referred to as a Registered User in the Main Agreement).

"Business Purpose" has the meaning attributed to in Section 1798.140(d) of the CCPA.

"CCPA" means Sections 1798.100 et seq. of the California Civil Code, and any attendant regulations issued thereunder as may be amended from time to time.

"Customer Personal Data" means personally identifiable information that: (i) relates to an identified or identifiable natural person; or (ii) that is otherwise protected as "personal data" or "personal information," pursuant to applicable Data Protection Laws, and in the case of (i) and (ii), that Flowplayer processes as a processor or service provider on behalf of Customer in providing the Service.

"Data Protection Laws" means the data protection and privacy laws and regulations applicable to the processing of Customer Personal Data, including, where applicable, E.U. Data Protection law and U.S. Data Protection law, in each case, as may be amended, superseded, or replaced.

“EEA” means the European Economic Area, United Kingdom, and Switzerland.

“E.U. Data Protection Law” means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personally identifiable information and on the free movement of such data (“E.U. GDPR”); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom’s European Union (Withdrawal) Act 2018 (the “UK GDPR”); (iii) the E.U. e-Privacy Directive (Directive 2002/58/E.C.); and (iv) the Swiss Federal Data Protection Act (“Swiss DPA”).

“Model Clauses” (i) where the E.U. GDPR applies, the standard contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (E.U.) 2016/679 of the European Parliament and of the Council (“EU SCCs”); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (“UK SCCs”); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the “Swiss SCCs”)

“Restricted Transfer” means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

“Security Incident” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise processed by Flowplayer (or its Subprocessors). “Security Incident” does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.

“Services” or “Service” means the services that are provided by Flowplayer to Customer, as described in the Main Agreement.

“Subprocessor” means a processor engaged by Flowplayer that accesses, stores, or processes Customer Personal Data. Subprocessors include third parties or Flowplayer Affiliates but exclude employees, consultants, or independent contractors of Flowplayer where such individual performs services equivalent to those performed by an employee.

“U.S. Data Protection Law” means the data protection or privacy laws and regulations applicable to the processing of Customer Personal Data in force within the United States, including the CCPA, and any rules or regulations implementing the foregoing.

“Controller,” “processor,” “processing,” and “personal data” will have the meanings given to them under Data Protection Laws.

2. **Roles and Scope of Processing**

2.1. Processing Description. The type of Customer Personal Data processed, the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1 (Details of Processing). The parties agree that the processing description may be updated by Flowplayer from time to time to reflect new products, features, or functionality comprising the Services.

2.2. Data Processing Roles. Regarding the parties' roles under this DPA, the parties acknowledge and agree that Customer is the "controller" with respect to E.U. Data Protection Law and a "business" with respect to CCPA. Flowplayer is a "processor" with respect to E.U. Data Protection Law and a "service provider" with respect to CCPA.

2.3. Processing Instructions; Purpose Limitation. Flowplayer will process Customer Personal Data in accordance with the Main Agreement, this DPA, and/or with Customer's written instructions and only for the following purposes: (i) processing to provide the Services; (ii) processing to perform any steps necessary for the performance of the Main Agreement; (iii) processing initiated by Authorized User in their use of the Service; and (iv) processing to comply with other reasonable, lawful instructions provided by Customer (e.g., via email, phone, support tickets, or online tool).

2.4. Compliance with Laws. Flowplayer will process Customer Personal Data in accordance with this DPA and Data Protection Laws applicable to its role under this DPA. Flowplayer is not responsible for complying with Data Protection Laws uniquely applicable to Customer by virtue of its business or industry. Flowplayer will promptly inform Customer if it becomes aware that Customer's processing instructions infringe Data Protection Laws.

2.5. CCPA Compliance. With respect to the CCPA, Flowplayer will (i) comply with sections of the CCPA applicable to "service providers" as defined by the CCPA; (ii) process Customer Personal Data solely to provide the Services to Customer, consistent with Section 1798.140(e)(5) of the CCPA; and (iii) not sell Customer Personal Data, or retain, use, or disclose Customer Personal Data for any purposes other than to perform the Service or as otherwise permitted under Main Agreement or this DPA.

2.6. Customer Responsibilities. Customer, as a controller or as a business, is responsible for: (i) the accuracy, quality, and legality of the Customer Personal Data; (ii) how Customer acquired Customer Personal Data; (iii) the instructions Customer provides to Flowplayer regarding the processing of Customer Personal Data; (iv) providing all legally required notices to individuals and obtaining all legally required consents which may be necessary for Flowplayer to process Customer Personal Data; (v) ensuring that Customer's processing instructions are lawful and do not violate applicable Data Protection Laws; and (vi) ensuring that Customer Personal Data is provided to Flowplayer for a valid "Business Purpose," as defined in the CCPA. Customer will not provide or make available to Flowplayer any Customer Personal Data in violation of the Main Agreement or provide any Customer Personal Data that is inappropriate for the nature of the Services.

3. **International Data Transfer Mechanism**

3.1. Restricted Transfer; Transfer Mechanism. Where the transfer of Customer Personal Data is a Restricted Transfer, such transfer will be subject to the Model Clauses (subject to Section 3.2, 3.3, or 3.4, as applicable), which are incorporated into and form an integral part of this DPA. For the purposes of the

Model Clauses, the parties agree that: (i) Flowplayer is a "data importer" and Customer is the "data exporter"; and (ii) it is not the intention of either party to contradict or restrict any of the provisions set forth in the Model Clauses and, accordingly, if and to the extent the Model Clauses conflict with any provision of the Main Agreement (including this DPA) the Model Clauses will prevail to the extent of such conflict.

3.2. Model Clauses; EU GDPR. For purposes of the Model Clauses, (i) in Clause 7, the optional docking clause will apply; (ii) in Clause 9 of Module Two, Option 2 will apply, and the time period for prior notice of Subprocessor changes is identified in Section 4.1 of this DPA; (iii) in Clause 11, the optional language will not apply; (iv) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law; (v) in Clause 18(b), disputes will be resolved before the courts of Ireland; (vi) Annex 1 will be deemed completed with the information set out in Annex 1 (Details of Processing) of this DPA; and (vii) Annex 2 (Security Measures) will be deemed completed with the information set out in Annex 2 of this DPA; and Annex 3 (Subprocessors) will be deemed completed with the information set out in Annex 3 of this DPA.

3.3. Model Clauses; UK GDPR. In relation to transfers of Customer Personal Data protected by the UK GDPR, the EU SCCs will also apply, with the following modifications: (i) any references in the EU SCCs to "Directive 95/46/E.C." or "Regulation (E.U.) 2016/679" will be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (E.U.) 2016/679" are replaced with the equivalent Article or Section of UK GDPR; (ii) references to "E.U.", "Union" and "Member State Law" are all replaced with "U.K."; Clause 13(a) and Part C of Annex 1 of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" will be interpreted as references to the Information Commissioner and the courts of England and Wales; and (iii) Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses will be resolved by the courts of England and Wales. A data subject may bring a legal proceeding against the data exporter and/or data importer before the courts of any country in the U.K. The parties agree to submit themselves to the jurisdiction of such courts." Where the EU SCCs cannot be used to lawfully transfer such Customer Personal Data in compliance with the UK GDPR, the UK SCCs will instead be incorporated by reference and form an integral part of this DPA and will apply to such transfers. Where the UK SCCs apply, the relevant Annexes or Appendices of the UK SCCs will be populated using the information contained Annex 1, Annex 2, and Annex 3, as applicable.

3.4. Model Clauses; Swiss DPA. In relation to transfers of Customer Personal Data protected by the Swiss DPA, the EU SCCs will also apply with the following modifications: (i) any references in the EU SCCs to "Directive 95/46/E.C." or "Regulation (E.U.) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "E.U.," "Union," "Member State" and "Member State law" will be interpreted as references to Switzerland and Swiss law, as the case may be; and (iii) references to the "competent supervisory authority" and "competent courts" will be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland. Where the EU SCCs cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss DPA, the Swiss SCCs will instead be incorporated by reference and form an integral part of this DPA and will apply to such transfers. Where the Swiss SCCs apply, the relevant Annexes or Appendices of the UK SCCs will be populated using the information contained Annex 1, Annex 2, and Annex 3, as applicable.

3.5. Alternative Data Transfer Arrangements. To the extent Flowplayer adopts an alternative data export mechanism (including any new version of or successor to the Model Clauses adopted pursuant to Data Protection Laws) for the transfer of personal data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism will automatically apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Laws applicable to the EEA and extends to territories to which Customer Personal Data is transferred).

4. **Subprocessing**

4.1. Notification of New Subprocessors. Customer hereby provides its general authorization for Flowplayer to engage the Subprocessors listed In Annex 3 . If Customer would like to receive notifications of new Subprocessors added by Flowplayer, Customer must send an email to legal@flowplayer.comand opt-in to receiving updates. At least thirty (30) days before allowing a new Subprocessor to process Customer Personal Data, Flowplayer will notify Customers by email who have opted-in to receiving updates. Customer may object in writing to Flowplayer's appointment of a new Subprocessor within ten (10) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection or data privacy. In such event, the parties will discuss Customer's concerns in good faith to achieve a resolution.

4.2. Subprocessor Obligations. Flowplayer will enter into a written agreement with each Subprocessor imposing such data protection obligations as are required under applicable Data Protection Laws. To the extent the CCPA applies, each written agreement with a Subprocessor will comply with the CCPA, designate the Subprocessor as a "service provider," and prohibit the Subprocessor from selling Customer Personal Data or using Customer Personal Data for any purpose not authorized by the CCPA. Flowplayer will be responsible for any Subprocessor's breach of the terms of this DPA.

5. **Security Measures and Security Incident Response**

5.1. Security Measures. Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Flowplayer will implement and maintain technical and organizational measures that are designed to protect Customer Personal Data from an unauthorized or unlawful destruction, loss, alteration, disclosure of or to access and will implement those measures specified in Annex 2 ("Security Measures"). Flowplayer may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

5.2. Customer Responsibilities. Customer is responsible for its secure use of the Service, including securing its account authentication credentials and protecting the security of Customer Personal Data transmitted via the systems Customer administers and maintains (i.e., email encryption).

5.3. Security Incident Response. Flowplayer will notify Customer without undue delay (and in any case, within seventy-two (72) hours) after becoming aware of a Security Incident which directly affects the Customer. Flowplayer will provide information relating to the Security Incident to Customer promptly as it becomes known or as is reasonably requested by Customer. Flowplayer will take appropriate and reasonable steps to contain, investigate, and mitigate any Security Incident.

6. **Responding to Consumer Requests.** Flowplayer will provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Data Protection Laws (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, inquiry or complaint received from a data subject, regulator or another third party, in each case in respect of Customer Personal Data that Flowplayer processes on Customer's behalf. If any request, correspondence, inquiry, or complaint is made directly to Flowplayer, Flowplayer will not respond without Customer's prior authorization unless legally compelled to do so, except that Flowplayer will inform the individual that the individual should submit the request directly to Customer. Flowplayer will provide a copy of the request to Customer. If Flowplayer is legally required to respond to such a request, Flowplayer will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

7. **Audit and Records.**

7.1. Reports; Security Assessments. Upon request, Flowplayer will (i) make available to Customer a summary copy of its audit reports regarding the audit of Flowplayer's premises, systems, and documentation so that Customer assess Flowplayer's compliance with this DPA; and (ii) provide written responses to reasonable requests for information made by Customer related to its processing of Customer Personal Data, including responses to information security and audit questionnaires, that are necessary to confirm Flowplayer's compliance with this DPA; provided that, such disclosures are considered Confidential Information under the Main Agreement, and Customer will not exercise the right in 7.1(ii) more than once per calendar year.

7.2. Audit Rights and Procedures. Where Customer cannot reasonably satisfy Flowplayer's compliance with this DPA pursuant to the exercise of its rights under Section 7.1, and where required under Data Protection Laws or by a data protection authority under Data Protection Laws, Customer may, on giving at least thirty (30 days) prior written notice, request that Customer's personnel or a third party (at Customer's expense) conduct an audit of Flowplayer's facilities, equipment, documents and electronic data relating to the processing of Customer Personal Data solely to the extent necessary to inspect and/or audit Flowplayer's compliance with this DPA, provided that: (i) Customer will not exercise this right more than once per calendar year; (ii) such additional audit enquiries will not unreasonably or adversely impact in Flowplayer's regular operations; (iii) will not be incompatible with Data Protection Laws or with the instructions of the relevant data protection authority; (iv) the parties will mutually agree upon the scope, timing, and duration of the audit; and (v) at all times during the scope of the audit, Customer and any appointed third party will comply with Flowplayer's policies, procedures, and reasonable instructions governing access to its systems and facilities, including limiting or prohibiting access to information that is confidential information. No such audit will require Flowplayer to provide Customer with access to internal accounting or financial records, trade secrets, or information that could reasonably compromise the security of Flowplayer systems. The results of such audit will be considered Flowplayer's Confidential Information (as defined in the Main Agreement).

8. **Return or Deletion of Data.** Promptly upon Customer's request, Flowplayer will delete or return Customer Personal Data in its possession or control. This requirement will not apply to the extent Flowplayer is required by applicable law to retain Customer Personal Data or to Customer Personal Data that is archived on backup systems (which will be securely isolated and not subject to further processing, except to the extent required by law).

9. **Cooperation**

9.1. Requests by Law Enforcement. Flowplayer does not voluntarily provide government agencies, authorities, or law enforcement access to Customer Personal Data. If a law enforcement agency sends Flowplayer a demand for Customer Personal Data (e.g., a subpoena, court order, search warrant, or another valid legal process), Flowplayer will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Personal Data to a law enforcement agency, Flowplayer will give Customer reasonable notice to allow Customer to seek a protective order or other appropriate remedies, to the extent Flowplayer is legally permitted to do so.

10. **Limitation of Liability**. Notwithstanding anything to the contrary in the Main Agreement or this DPA, the total aggregate liability of Flowplayer for all claims under the Main Agreement and DPA (including Affiliate claims) will be subject to the limitations of liability set out in the Main Agreement, and such limitations will apply to any claims, losses, costs or other damages arising from or related to (i) a breach of this DPA; (ii) fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) violation of Data Protection Laws, including any claims relating to damages paid to a data subject; or (iv) breach of its obligations under the Model Clauses. Nothing in this DPA or the Agreement limits a party's liability with respect to any individual's direct exercise of its data protection rights against a party.

11. **General**. As between Customer and Flowplayer, this DPA is incorporated into and subject to the terms of the Main Agreement and will be effective and remain in force for the term of the Main Agreement. Each party acknowledges that the other party may disclose the Model Clauses, this DPA, and any privacy related provisions in the Main Agreement to any regulator or supervisory authority upon request. This DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto, respective permitted successors, and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person. Other than as required by the Model Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Main Agreement govern any dispute pertaining to this DPA.

IN WITNESS WHEREOF, the authorized representatives of the parties hereto have executed and delivered this DPA.

Customer		**Flowplayer AB**	
Signature:		Signature:	
Printed:		Printed:	Henrik Lovén
Title:		Title:	CEO
Date:		Date:	

ANNEX 1

DETAILS OF PROCESSING

A. LIST OF PARTIES

Data exporter:

Name: The entity listed as "Customer" in the applicable order form and/or Main Agreement

Address: The address listed on any applicable order form or in Customer's account

Contact person's name, position, and contact details: The point of contact is listed on any applicable order form, the Main Agreement, or in Customer's account

Activities relevant to the data transferred under these Clauses: Use of the Flowplayer video services, pursuant ot the Main Agreement

Role (controller/processor): Controller

Data importer(s):

Name: Flowplayer AB

Address: Regeringsgatan 29, 111 53, Stockholm, Sweden

Contact person's name, position, and contact details: Elizabeth Koehler, Director Security, and Compliance, security@flowplayer.com

Activities relevant to the data transferred under these Clauses: Provide Flowplayer Services to Customer as specified in the Main Agreement and any applicable Order Form

Signature and date: By signing or otherwise accepting the Main Agreement and order form (where applicable), Flowplayer hereby agrees to be bound by this DPA

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer, Authorized Users, and individuals who access and use the Flowplayer Services, which are made available by Customer.

Categories of personal data transferred

- IP address of individuals who accesses and uses the Flowplayer Services
- Name, email address, physical address of Customer, and individuals who communicate with Flowplayer on Customer's behalf (e.g., account registration and support tickets)
- Name, email address, I.P. address of Authorized Users
- Session activity associated with IP address
- Any content that is uploaded to Flowplayer and contains identifiable personal data (e.g. video, images, metadata)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as, for instance, strict purpose limitations, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Continuous during the term of the Main Agreement.

Nature of the processing

Video streaming services and related services, networks, and products, which are owned, controlled or licensed by Flowplayer and that allow for the acquisition, manipulation, and distribution of video, audio, and other content.

Purpose(s) of the data transfer and further processing

To provide Flowplayer Services to Customers.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

From the Effective Date of the Main Agreement until its termination.

For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing

From the Effective Date of the Main Agreement until its termination.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them or whose behavior is monitored are located will act as the competent supervisory authority.

ANNEX 2

SECURITY MEASURES

The technical and organizational measures implemented by Flowplayer (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context, and purposes of the processing, and the risks to the rights and freedoms of natural persons, are as follows:

- **Encryption of personal data**
  - Sensitive data at rest encrypted using, at a minimum, AES-256 algorithm or compensating controls are in place (including hashed passwords and encrypted machines).
  - HTTPS encryption on every web login interface, using industry standard algorithms and certificates.
  - Secure transmission of credentials using by default TLS 1.2.
  - Access to operational environments requires the use of secure protocols such as HTTPS.

- **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**
  - Strong access controls use of the principle of least privilege.
  - Access to systems is restricted by security groups and access-control lists.
  - Authorization requests are tracked and logged.
  - Employee access is removed upon termination or change of employment.
  - Enforcement of Multi-factor Authentication (MFA) for access to critical and production resources where feasible.
  - Strong passwords are required. Initial passwords must be changed after the first login.
  - Passwords are never stored in clear text and are encrypted in transit and at rest.
  - Confidentiality requirements are imposed on employees.
  - Mandatory security training for employees, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and overall security responsibilities inside and outside of Flowplayer.
  - Nondisclosure agreements with third parties.
  - Separation of networks based on trust levels.
  -
- **Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing**
  - User activity, including logins, configuration changes, deletions, and updates, are written automatically to audit logs in operational systems.
  - All logs can be accessed only by authorized Flowplayer employees, and access controls are in place to prevent unauthorized access.
  - Network segmentation and interconnections are protected by firewalls.

- **Measures for user identification and authorization**
  - Access to operational and production environments is protected using unique user accounts, strong passwords, use of Multi-Factor Authentication (MFA) where feasible, role-based access, and the least privilege principle.
  - Authorization requests and provisioning is logged, tracked, and audited.
  - User activity in operational environments, including access, modification, or deletion of data, is being logged.
  - Web Application Firewall (WAF), in addition to network-based firewalls, are in place.

- **Measures for the protection of Data during transmission**
  - HTTPS encryption for data in transit (using TLS 1.2 or greater).

- **Measures for the protection of Data during storage**
  - Flowplayer customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged.
  - Endpoint security software.
  - System inputs recorded via log files.
  - Access Control Lists (ACL) are in place.

- **Measures for ensuring system configuration, including default configuration**
  - Flowplayer has in place a Vendor Management Procedure that includes change management.
  - Flowplayer monitors changes to in-scope systems to ensure that changes follow the process, and to mitigate the risk of un-detected changes to production.

- **Measures for ensuring data minimization**
  - Data collection is limited to the purposes of the processing.
  - Security measures are in place to provide only the minimum amount of access necessary to perform required functions.

- **Measures for ensuring limited data retention**
  - After termination of all subscriptions associated with an environment, customer data submitted to the Services is retained in inactive status within the Services until deleted.

ANNEX 3
SUBPROCESSORS

Subprocessor Name	Function	Website	Location
AWS EMEA SARL	Cloud Service Provider	https://aws.amazon.com/	*Ireland (AWS datacenter)*
Sonix Inc	Transcription service	https://sonix.ai/	*USA*
Chargify (Maxio)	Billing system	https://www.chargify.com/	*USA*
Customer.io	Customer interaction	https://customer.io/	*USA*
Front	Customer support	https://front.com/	*USA*
Stripe	Payments	https://stripe.com/	*USA*
Hubspot	CRM	https://www.hubspot.com/	*USA*