

## **Data Processing Agreement**

### **1. Subject of the Agreement**

Fullview ApS (the “**Processor**”) provides a Software as a Service (“Fullview”) to the customer (the “**Customer**”, together with the Processor the “**Parties**”). The provision of the Fullview requires the processing of personal data of Customer’s employees and customers. Whereas Processor may act as a controller with respect to certain personal data transferred by Customer, for example used for billing or contract fulfillment purposes, Customer acts as a controller pursuant to data protection law regarding Customer’s customer or employee data (the “**Customer Data**”) processed by Fullview. This data processing agreement (the “**DPA**”) specifies the data protection obligations and rights of the Parties in connection with the Processor’s use and handling of Customer Data.

### **2. Scope of the Processing**

- 2.1 The Processor shall process the Customer Data on behalf and in accordance with the instructions of the Customer within the meaning of Art. 28 General Data Protection Regulation (“**GDPR**”). The Customer remains the controller of Customer Data pursuant to Art. 28 GDPR.
- 2.2 The processing of Customer Data by the Processor occurs in the manner and the scope and for the purpose determined in **Annex 1** to this DPA; the processing relates to the types of personal data and categories of data subjects specified therein. This DPA shall remain valid as long as Customer operates an active account in Fullview.

### **3. Right of the Customer to Issue Instructions**

- 3.1 The Processor processes the Customer Data in accordance with the instructions of the Customer, unless the Processor is legally required to do otherwise. In the latter case, the Processor shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
- 3.2 The Processor shall ensure that the Customer Data is processed in accordance with the instructions given by the Customer. If the Processor is of the opinion that an instruction given by the Customer infringes this DPA or applicable data protection law, he may suspend the execution of the instruction upon notification of the Customer until the latter confirms the instruction.

### **4. Responsibility of the Customer**

- 4.1 Upon request, the Customer shall provide the Processor with the information specified in Art. 30 para. 2 lit. a GDPR, insofar as it is not already available to Processor.

- 4.2 If the Processor is required to provide information to a governmental body or person on the processing of Customer Data or to cooperate with these bodies in any other way, the Customer is obliged to assist the Processor at first request in providing such information and in fulfilling other appropriate cooperation obligations.

## **5. Requirements for Personnel and Systems**

The Processor shall commit all persons engaged in processing Customer Data to confidentiality with respect to the processing of Customer Data.

## **6. Security of Processing**

- 6.1 The Processor takes necessary appropriate technical and organizational measures according to Art. 32 GDPR, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Customer Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection of Customer Data appropriate to the risk.
- 6.2 The technical and organizational measures undertaken by the Processor are described in **Annex 3**.
- 6.3 The Processor shall have the right to modify technical and organizational measures during the term of this DPA, if they continue to comply with the statutory requirements.

## **7. Engagement of Further Processors**

- 7.1 The Customer grants the Processor the general authorization to engage further processors ("**Subprocessors**") regarding the processing of Customer Data, as described hereinafter. Subprocessors engaged at the time of conclusion of this DPA are listed in **Annex 2**.
- 7.2 The Processor shall notify the Customer of any intended changes in relation to adding new or replacing Subprocessors. In individual cases, the Customer has the right to object to the engagement of a potential further processor. An objection may only be raised by the Customer for important reasons which have to be substantiated vis-à-vis the Processor. Insofar as the Customer does not object within 14 days after receipt of the notification, his right to object lapses.
- 7.3 The agreement between the Processor and Subprocessor must impose the same obligations on the Subprocessor as those imposed upon the Processor under this DPA. The Parties agree that this requirement is fulfilled if the respective DPA has a level of protection corresponding to this DPA.
- 7.4 Subject to compliance with the requirements of Sec. 2.3 of this DPA, the provisions of this

Sec. 7 shall also apply if a Subprocessor is located outside of the EAA.

## **8. Data Subjects' Rights**

- 8.1 The Processor shall support the Customer within reason by virtue of technical and organizational measures in fulfilling the Customer's obligation to respond to requests for exercising data subjects' rights.
- 8.2 As far as a data subject submits a request for the exercise of his rights directly to the Processor, the Processor will forward this request to the Customer without undue delay.
- 8.3 The Processor shall inform the Customer of any information relating to the stored Customer Data, about the recipients of Customer Data to which the Processor may disclose it in accordance with the instructions and about the purpose of storage, as far as the Customer does not have this information at his disposal and as far as he is not able to collect it himself.
- 8.4 The Processor shall, within the bounds of what is reasonable and necessary, enable the Customer to correct, delete or restrict the further processing of Customer Data, or at the instruction of the Customer correct, block or restrict further processing himself, if and to the extent that this is impossible for the Customer.
- 8.5 Insofar as the data subject has a right of data portability vis-à-vis the Customer in respect of the Customer Data pursuant to Art. 20 GDPR, the Processor shall support the Customer within the bounds of what is reasonable and necessary in handing over the Customer Data in a structured, commonly used and machine-readable format, if the Customer is unable to obtain the data elsewhere.

## **9. Notification and Support Obligations of the Processor**

- 9.1 The Processor shall inform the Customer without undue delay of any reportable events in his area of responsibility which may constitute a personal data breach. The Processor shall assist the Customer in fulfilling the notification obligations at the Processor's request to the extent reasonable and necessary.
- 9.2 The Processor shall assist the Customer to the extent reasonable and necessary with data protection impact assessments to be carried out by the Customer and, if necessary, subsequent consultations with the supervisory authority pursuant to Art. 35, 36 GDPR.

## **10. Deletion and Return of Customer Data**

- 10.1 Upon termination of this DPA, the Processor shall, in the discretion of the Customer,
  - a) either delete or return the Customer Data; and
  - b) delete existing copies thereof

unless the Processor is obligated by law to further store the Customer Data.

10.2 The Processor may keep documentations which serve as evidence of the orderly and accurate processing of Customer Data, also after the termination of this DPA.

## **11. Evidence and audits**

11.1 The Processor shall provide the Customer, at the Customer's request, with all information required and available to the Processor to prove compliance with his obligations under this DPA.

11.2 The Customer shall be entitled to audit (including inspections) the Processor regarding compliance with the provisions of this DPA, in particular the implementation of the technical and organizational measures.

11.3 In order to carry out inspections in accordance with Sec. 11.2., the Customer is entitled to access the business premises of the Processor in which Customer Data is processed within the usual business hours (Mondays to Fridays from 9 am to 5 pm) after timely advance notification in accordance with Sec. 11.5 at his own expense, without disruption of the course of business and under strict secrecy of the Processor's business and trade secrets.

11.4 The Processor is entitled, at his own discretion and taking into account the Customer's legal obligations, not to disclose information which is sensitive with regard to the Processor's business or if the Processor would be in breach of statutory or other contractual provisions as a result of its disclosure. The Customer is not entitled to get access to data or information about the Processor's other customers, cost information, quality control and contract management reports, or any other confidential data of the Processor that is not directly relevant for the agreed audit purposes.

11.5 The Customer shall inform the Processor in due time (usually at least two weeks in advance) of all circumstances in relation to the performance of the audit.

11.6 If the Customer commissions a third party to carry out the audit, the Customer shall obligate the third party in writing in the same way as the Customer is obliged vis-à-vis the Processor according to this Sec. 11. In addition, the Customer shall by way of written agreement obligate the third party to maintain secrecy and confidentiality unless the third party is subject to a professional obligation of secrecy. At the request of the Processor, the Customer shall immediately submit to him the commitment and confidentiality agreements with the third party. The Customer may not commission any of the Processor's competitors to carry out the audit.

11.7 Without limiting rights of the Customer under Art. 28 GDPR, proof of compliance with the obligations under this DPA may be provided by submitting an appropriate current opinion

or report from an independent authority (e.g. auditor, audit department, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit (the “**Audit Report**”).

## **12. Contract term and termination**

The term and termination of this DPA shall be governed by the term and termination provisions of the Contract. A termination of the Contract automatically results in the termination of this DPA. An isolated termination of the DPA is excluded.

## **13. Final provisions**

- 13.1 In case individual provisions of this DPA are ineffective or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The Parties undertake to replace the ineffective provision by a legally permissible provision which comes closest to the purpose of the ineffective provision and that thereby satisfies the requirements of Art. 28 GDPR.
- 14.2 In case of conflicts between this DPA and other arrangements of the Parties, in particular the Contract, the provisions of this DPA shall prevail.

**Annex 1**  
**Further Information on the Processing of Customer Data**

1. Live synchronous features

|   |                                       |                                                                                                                                                                                          |
|---|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Purpose and extent of Data Processing | Fullview Enabling the Customer to engage with their users in real-time and help them to solve their issues in a collaborative sharing of a defined window or tab between multiple users. |
| 2 | Types of personal data                | Any content of the shared screen, depending on the service provided by the Controller to their clients.                                                                                  |
| 3 | Categories of data subjects           | Customer's customers and/or employees or other users Customer selects to share.                                                                                                          |

2. Asynchronous customer support features

|   |                                       |                                                                                                                                                  |
|---|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Purpose and extent of Data Processing | Capturing and recording the interactions of a user with the Customer's system for internal troubleshooting or improving the customer experience. |
| 2 | Types of personal data                | Name, company, user ID, interactions, and usage of Customer's software.                                                                          |
| 3 | Categories of data subjects           | Users of Customer's software.                                                                                                                    |

**Annex 2**  
**Subprocessors**

| No. | Name of the further processor                                                                           | Location of processing / Safeguards | Description of processing via this further processor            |
|-----|---------------------------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------|
| 1   | <b>Amazon Web Services EMEA</b><br>SARL, 38 Avenue John F. Kennedy<br>1855 Luxembourg<br>- Luxembourg - | EU hosted<br>(eu-central-1)         | Secure cloud service platform for hosting services and storage. |

**Annex 3 - Technical and Organizational Measures**

**1. Confidentiality (Art. 32 para. 1 lit. b GDPR)**

**Physical Access Control**

**Purpose:** To prevent unauthorized persons from gaining access to data processing equipment with which personal data is processed or used.

**Measures:**

- Access control system with e.g. chip card and keys to access Fullview offices
- Physical access control with e.g. a receptionist during business hours
- Door locking with secure locks
- Video/CCTV
- Alarm systems
- Issue and withdrawal of chip cards and keys is controlled by means of a documented process
- Requirement for visitors to be accompanied by staff

**Measures of third-party service providers:**

Fullview is hosting its solution exclusively on high-security AWS servers in the European Union. The data centers have ISO 27001 certification. For an overview of security measures, visit <https://aws.amazon.com/compliance/data-center/controls/>

**Systems Access Control**

**Purpose:** To prevent data processing systems from being used by unauthorized persons.

**Measures:**

- Password policy (passwords must have at least 12 characters and sufficient complexity (at least 1 upper and lower case letter, number, special character each)
- Passwords must be stored in approved password managers that reliably encrypt passwords

- Remote Work Policy requires employees to ensure classified information is not displayed in public or in video call when screens are shared
- Clean Desk Policy requires each employee to properly dispose of documents and lock computers when leaving the workplace
- Automatic screen- and keylock within 10 minutes of inactivity
- Encryption of device hard drives is monitored technically
- Process to ensure active and up to date anti-malware and firewall protection on all company devices
- Immediate blocking of authorizations when employees leave the company
- Encryption of all backups
- Authorizations that are no longer required are revoked promptly.
- Access blocking via session timeout
- Employees must use devices issued by Fullview and storing classified information outside of such devices or approved cloud storage services is prohibited

#### **Measures of third party service providers:**

Fullview is hosting its solution exclusively on high-security AWS servers in Germany. The data centers have ISO 27001 certification. For an overview of security measures, visit <https://aws.amazon.com/security/>

#### **Data Access control**

Purpose: to ensure that those authorized to use a data processing system can access only the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

#### **Measures:**

- Encryption at rest of hosted data
- Encryption in transit of all the data
- Restrictive granting of access to productive environment
- Allocation of minimal authorizations (need-to-know principle)
- Authorizations are granted based on a comprehensive Access Management Policy (e.g. in the form of profiles, roles), which includes a defined process for account provisioning, immediate withdrawal of access rights and regular reviews
- Documented information classification concept
- Binding procedure for restoring data from backup

#### **Separation control**

**Purpose:** To ensure that data collected for different purposes can be processed separately.

- System design includes logical tenant separation
- Control via authorization concept
- Fullview has a Secure Development Lifecycle which includes the separation of test, staging and production environment



## **2. Integrity (Art. 32 para. 1 lit. b GDPR)**

### **Transfer control**

Purpose: to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment.

#### **Measures:**

- Secured transport protocols (SSL, TLS, SFTP)
- Encryption of data in transit
- Prohibition of use of private data carriers
- Work instructions for the use of mobile data carriers
- Procedure for data protection-compliant deletion/disposal of data carriers and documents
- Backup in an ISO 27001 certified data center
- Access to production and development systems only via certificate-based authentication over encrypted connection
- All employees have been obliged to the data privacy in written form during the onboarding process. Employees have been informed about their personal liability and criminal implications of data breaches and receive regular trainings
- Fullview has a Secure Development Lifecycle which includes code review and security testing.

### **Input control**

**Purpose:** to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

#### **Measures:**

- Access to data is recorded and trackable:
- Logging and reports on data-access
- Logging and reports on data-deletion
- Logging and reports on changes to data
- Defined processes for incident monitoring, including automated incident alarms and incident management, including post-mortems and root cause analyses for critical incidents.

## **3. Availability and Resilience (Art. 32 para. 1 lit. c GDPR)**

#### **Availability Control / Rapid Recoverability:**

**Purpose:** To ensure that personal data is protected against accidental destruction or loss.

**Measures:**

- Defined procedure for Backups, including secure encrypted storage in different physical locations and regular restoration tests
- Use of protection programs (virus protection, firewall, SPAM filter)
- The Fullview database provides an availability of at least 99,9 % which is safeguarded by a corresponding service level agreement with the subcontractor.

**Measures of third party service providers:**

Fullview is hosting its solution exclusively on high-security AWS servers in Germany. The data centers have ISO 27001 certification. For an overview of security measures, visit <https://aws.amazon.com/de/compliance/data-center/controls/>

#### **4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR, Art. 28 GDPR)**

#### **Organization Control**

**Purpose:** To design the organization in such a way that it meets requirements of data protection.

**Measures:**

- All employees have been obligated in writing to maintain data secrecy and have been instructed accordingly
- All employees are trained regularly (at least once a year) on data protection in the workplace
- Auditing by the data protection officer(s) is carried out on a regular basis.
- There is a procedure for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR) in the form of an integrated management system (IMS). The IMS includes a data protection management system and an information security management system oriented towards ISO/IEC 27001:2013
- Risk Management Process

**Measures of third party service providers:**

Fullview is hosting its solution exclusively on high-security AWS servers in Germany. The data centers have ISO 27001 certification. For an overview of security measures, visit <https://aws.amazon.com/de/compliance/data-center/controls/>

#### **Supplier Management**

**Purpose:** To ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

**Measures:**

- Fullview has appointed a data protection officer and ensures through the data protection organization that he is appropriately and effectively integrated into the relevant operational processes.
- Data Processing Agreements are in place with all relevant subcontractors.
- A Supplier Risk Management process is in place to regularly review the security measures of service providers.

**5. Data protection-friendly default settings (Privacy by Design / Privacy by Default) according to Art. 25 GDPR**

**Purpose:** To comply with the Privacy by Design/Privacy by Default regulations.

**Measures:**

- As a Processor, we process customers personal data as necessary for providing our services.
- Consultation of the data protection officer takes place during the development of software features.