Data Processing

Agreement DotPDF.io

Comprised of:

Deel 1. Data Pro statement

Deel 2. Standard Clauses for Data processing

Part 1: Data Pro Statement

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

General information

1. **This Data Pro Statement was drawn up by the following Data Processor:**
   Menzit B.V. office located at Zonneoordlaan 17, 6718 TK, Ede

   If you have any queries about this Data Pro Statement or data protection in general, please contact:
   Harm Zeinstra at privacy@dotpdf.io

2. **This Data Pro Statement will go into effect on May 2nd 2024**
   We regularly revise the security measures described in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we shall notify you of the revised versions through our regular channels.

3. **This Data Pro Statement applies to the following products and services provided by data processor**
   DotPDF SaaS, DotPDF Hosted, DotPDF On-prem

4. **Description of DotPDF**
   DotPDF empowers businesses to effortlessly transform their HTML data into professional-looking PDF documents. With its versatile functionality, DotPDF caters to a wide range of applications, making it an invaluable tool for software developers seeking a robust and reliable solution.

5. **Intended use DotPDF was designed and built to process the following types of data:**
   DotPDF recognizes the sensitivity of data and is committed to safeguarding your privacy. While the software is capable of processing (special) personal data, the decision to do so rests entirely with the client. DotPDF ensures that data remains secure and adheres to the highest data privacy standards

   DotPDF offers three deployment options to suit your specific requirements:

   - DotPDF SaaS: In this cloud-based model, DotPDF manages the servers, providing a hassle-free experience. Multiple SaaS clients share these servers, ensuring efficient resource utilisation.
   - DotPDF Dedicated: For those seeking a dedicated server environment, DotPDF sets up a server exclusively for the client's use.
   - DotPDF Self-Managed: If you prefer complete control over your data and server infrastructure, DotPDF's self-managed option allows you to deploy the software on your preferred servers.

   When this product/service was designed, the possibility that it would be used to process special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government was taken into account.

   It is up to client to determine whether or not it shall use the aforementioned product or service to process such data.

6. **When data processor designed the product or service, it applied a privacy-by-design approach in the following manner:**
   DotPDF integrates privacy considerations throughout the entire design and development process of the DotPDF service. Proactive measures are taken to minimise the collection, processing and storage of (personal) data, ensuring data security and privacy from the very beginning.
   A non-exhaustive list of examples:

   - Implementing data minimization techniques to collect only the necessary data.

- Building security features like encryption and access controls.
- Deletion of HTML and PDF data as soon as possible

7. **Data processor uses the Data Processing Standard Clauses for data processing, which are attached to the Agreement as an addendum.**

8. **The data processor shall process the personal data provided by its clients within/ the EU/EEA.**

    - Google Cloud Platform: resources hosted in europe-west4 region
    - MongoDB Atlas: resources hosted in GCP europe-west1 region
    - Sinch: GCP europe-west1 and europe-west3 region
    - Atlassian: EU region
    - Stripe Payments Europe: Europe

9. **Once an agreement with a client has been terminated, data processor shall delete personal data it processes on behalf of client within three months, in such a manner that they shall no longer be able to be used and shall be rendered inaccessible.**

Security policy

Data processor has implemented the following security measures to protect its product or service

- The different server elements only have access to the portion of the database that they need to access.
- The different server elements only have rights to the portion of the database that they need to operate in (read/writes).
- Database access is restricted to various inhouse IP addresses.
- Sensitive environment variables are masked and fenced off.
- The API is protected by API keys and every request to fetch data needs a unique hash made for that specific piece of data.
- HTML and PDF data is removed from all servers as soon as possible. This data is only accessible by the server itself as it is located inside the container and not accessible from the outside other than by the protected API.
- When requests are done by IP instead of an API key, IP will be hashed and stored for licensing, overflowing, abuse detection purposes.
- No further personal data will be stored although the mentioned systems.

Furthermore

- DotPDF is a registered trademark to prevent abuse and misuse of the name.
- Access to servers and repositories is restricted and closely monitored through various logging tools.
- Regularly patch and update software to address known security vulnerabilities.
- All request data must implement a secure protocol.
- Developers are trained in secure coding practices to avoid common coding errors that can be exploited by attackers.
- Code is peer reviewed before added to any source code that could potentially reach client.
- Proactively identify and mitigate potential security threats throughout the development lifecycle.
- Computers and offices are locked whenever no authorised person is around to operate that computer.
- Access control is done with MFA factors in place.
- When an incident should occur, client is notified and updated frequently to ensure transparency of the process. This with the knowledge that resources will be available to address the incident as soon as possible.
- Tests are done to ensure security of mentioned systems and products.
- Database and server backups are in place in case of an attack of any sort that would disrupt main servers and/or databases.
- For external responsible disclosures there is a secured mailing available.

10. **Data processor conforms to the principles of the following Information Security Management System (ISMS):**
    - ASVS
    - OWASP

Data breach protocol

11. **In the unfortunate event something does go wrong, data processor shall follow the following data breach protocol to ensure that clients are notified of incidents:**

Detection and Initial Response

- **Incident Response Team (IRT) Activation:** Upon detecting a potential data breach, the designated IRT lead or security officer initiates the response process.
- **Containment:** Immediately isolate affected systems or services to prevent further unauthorised access or data loss.
- **Documentation:** Document the date, time, and nature of the breach, along with any initial observations or evidence.

Assessment and Investigation

- **Scope and Severity:** Conduct a thorough investigation to determine the scope and severity of the breach, including the type of data compromised and potential impact on client.
- **Root Cause Analysis:** Identify the root cause of the breach and assess any vulnerabilities or weaknesses that may have been exploited.
- **Evidence Preservation:** Preserve evidence for forensic analysis if necessary, while ensuring compliance with legal and regulatory requirements.

Notification and Communication

- **Stakeholder Alert:** Notify key stakeholders, including senior management, legal counsel, IT security personnel, and relevant regulatory authorities, as required by applicable laws and regulations.
- **Customer Communication:** Communicate transparently and promptly with affected clients about the breach, its potential impact, and any steps they should take to protect themselves (e.g., changing passwords).
- **Dedicated Channel:** Provide regular updates and establish a dedicated communication channel for inquiries and support.

Containment and Mitigation

- **Immediate Measures:** Implement immediate measures to contain the breach and prevent further unauthorised access or data loss.
- **Vulnerability Patching:** Deploy security patches, updates, or remediation measures to address any vulnerabilities or weaknesses identified during the investigation.
- **Enhanced Security:** Review and enhance security controls and protocols to mitigate the risk of similar incidents in the future.

Response Coordination and Collaboration

- **Internal Teams:** Coordinate with internal teams, such as customer support, engineering, and legal, to facilitate the response effort.
- **External Partners:** Collaborate with external partners, such as cloud service providers or third-party vendors, to address any shared responsibilities or dependencies.
- **Law Enforcement:** Engage with law enforcement agencies or regulatory bodies as needed to report the breach and comply with legal obligations.

Documentation and Reporting

- **Detailed Records:** Maintain detailed records of all actions taken during the breach response, including communications, decisions, and remediation efforts.
- **Incident Report:** Prepare a comprehensive incident report summarising the breach, response activities, lessons learned, and recommendations for improving security posture.
- **Policy Review:** Review and update relevant policies, procedures, and security controls based on insights gained from the incident.

Review and Continuous Improvement

- **Post-Incident Review:** Conduct a post-incident review to evaluate the effectiveness of the response effort and identify areas for improvement.
- **Corrective Actions:** Implement corrective actions and enhancements to strengthen security posture and resilience against future incidents.
- **Security Awareness:** Provide ongoing training and awareness to employees and stakeholders to promote a culture of security and vigilance.

Additional regular actions for faster reaction time

- **Regular Training:** Training of a team on data breach response procedures to ensure a swift and coordinated response.
- **Data Backups:** Maintain secure and up-to-date backups of data to facilitate recovery in case of a breach.

By following this comprehensive protocol, the product will be better prepared to handle a data breach. Specific actions may need to be adjusted based on the nature of the incident.

Part 2: Standard Clauses for Data Processing

Version: November 2019

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in its capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: a statement issued by the Data Processor in which it provides information such as the intended use of its products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor to meet its requirements under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.

2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written instructions provided by Client and accepted by Data Processor.

2.4 Client or its customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 Client shall guarantee Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in its Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of its products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures it shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures it has implemented if to its discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust its security measures. If Data Processor makes any adjustments to its security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing. .

Article 4. Data breaches

4.1 Data Processor does not guarantee that its security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, it shall notify

Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or its customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or its customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, it is entitled to invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that its employees comply with the requirements described in this article.

Article 6. Term and termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data it currently stores and which it has obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, it shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, it shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor shall be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.4 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at its own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with its obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to its discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.

7.5 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to its discretion such are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.

7.6 Data Processor shall be entitled to invoice Client for any costs it incurs in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (subprocessors) to help it process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet its obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes . Data Processor shall ensure that any third parties it hires shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.