



Connect, engage, empower

# Plek Employee Empowerment

**Data Processing Agreement**  
**Version 2.0**  
**March 2024**



# Data Processing Agreement

*Version March 2024*

<b>1. Definitions.....</b>	<b>3</b>
<b>1. Subject matter of this Processing Agreement.....</b>	<b>5</b>
<b>2. Formation, duration and termination of this Data Processing Agreement.....</b>	<b>5</b>
<b>Appendix 1: Processing of Personal Data.....</b>	<b>8</b>
<b>Appendix 2: Appropriate technical and organizational measures.....</b>	<b>9</b>
<b>Appendix 3: Sub-processors.....</b>	<b>9</b>
<b>Appendix 4.....</b>	<b>10</b>



This Data Processing Agreement is an integral part of the service agreement between the Client Organization and Plek for the use of online services and sets forth the agreements regarding the processing of personal data. By signing this agreement, the Client Organization (the "Controller") enters into this Data Processing Agreement with Plek (the "Processor").

### Signing the Data Processing Agreement

This Data Processing Agreement consists of two parts: the main agreement and 4 appendices.

1. Plek as the Processor has already signed this Data Processing Agreement.
2. To sign this Data Processing Agreement, the Client Organization must:
3. Complete and sign the information on page 9.
  - a. Fill in the information in Appendix 4.
  - b. Send the completed and signed Data Processing Agreement via email, stating the formal Client name and Contract number, to: [support@plek.co](mailto:support@plek.co).
4. From the moment a correctly and fully completed and signed agreement is received at this email address, this Data Processing Agreement is legally binding.

### Applicability of the Data Processing Agreement

If the Client Organization signing this Data Processing Agreement has a valid Service Agreement with Plek, then this Data Processing Agreement forms an appendix to that Service Agreement. The Client Organization acts as the Controller, and Plek acts as the Processor in the context of this Data Processing Agreement.

If the Client Organization signing this Data Processing Agreement is not a party to a valid Service Agreement between Plek and the Client Organization, then this Data Processing Agreement is not applicable and not legally binding. If such a Client Organization has procured Plek through an authorized reseller, then the Client Organization should contact this reseller to discuss whether changes to the agreement with this reseller are required.

This Data Processing Agreement does not replace any existing Data Processing Agreements or additional agreements concerning the processing of personal data that have already been included in the Service Agreement between the Client Organization and Plek, unless the Parties agree otherwise in writing.

## 1. Definitions

In this agreement, a number of terms are used, the meanings of which are clarified below. The mentioned terms are capitalized in this agreement. Often, the definition of the term from privacy laws and regulations is used in the list below:

**Personal data:** All information about an identified or identifiable natural person ("the Data Subject") that is processed within the scope of the "Underlying Assignment"; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

**Data subject:** The person to whom Personal Data relates.

**Processing / To Process:** An operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Processor:	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller, without being subject to the direct authority of the Controller.
Controller:	A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data breach / Personal data breach:	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed which may, in reality or potentially, lead to damage.
Data breach reporting obligation:	The obligation to report Data Breaches to the Personal Data Authority and (in some cases) to the Data Subject(s).
Sub-processor:	Another processor engaged by the Processor to carry out specific processing activities on behalf of the Controller.
Employees	Individuals who are employed by the Processor or the Controller, whether in an employment relationship or temporarily hired.
Third parties:	Others than the Processor and the Controller.
Special Categories of Personal Data:	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, as well as personal data relating to criminal convictions and offences or related security measures.
Sensitive Personal Data:	Personal data where loss or unlawful Processing could lead to (among other things) stigmatization or exclusion of the Data Subject, harm to health, financial loss, or (identity) fraud.  This category of personal data must include, at a minimum. <ul style="list-style-type: none"><li>- Special categories of personal data:</li><li>- Data concerning the financial or economic situation of the Data Subject</li><li>- (Other) data that could lead to stigmatization or exclusion of the Data Subject</li><li>- Usernames, passwords, and other login details</li><li>- Data that could be misused for (identity) fraud</li></ul>
Service agreement:	The agreement regarding the implementation, use, and supportive services of Plek.
AVG	General Data Protection Regulation, including the implementation law of this regulation. The GDPR replaces the Data Protection Act as of May 25, 2018.

## 1. Subject matter of this Processing Agreement

- 1.1. This Data Processing Agreement governs the processing of personal data by the Processor within the scope of the Service Agreement.
- 1.2. The nature and purpose of the processing, the type of personal data, and the categories of personal data, data subjects, and recipients are described in Appendix 1.
- 1.3. The Processor guarantees the implementation of appropriate technical and organizational measures (described in Appendix 2) to ensure that the processing meets the requirements of the Regulation and that the protection of the rights of the data subjects is guaranteed.
- 1.4. The Processor guarantees compliance with the requirements of applicable laws and regulations concerning the processing of personal data.

## 2. Formation, duration and termination of this Data Processing Agreement

- 2.1. This Data Processing Agreement comes into effect on the date it is signed by both parties.
- 2.2. This Data Processing Agreement is part of the Service Agreement and will remain in effect as long as the Service Agreement does. If the Service Agreement ends, this Data Processing Agreement automatically terminates; it cannot be terminated separately.
- 2.3. After the termination of the Service Agreement, the Processor, depending on the choice of the Controller, shall either return all Personal Data to the Controller or delete it. Backups are automatically deleted after one month. The Processor ensures that backups are secured with encryption/passwords in accordance with guidelines.

## 3. Scope of Processing Authority of the Processor

- 3.1. The Processor processes the Personal Data as described in Appendix 1 and solely on the instruction and based on written instructions from the Controller, except where deviating legal provisions applicable to the Controller require otherwise.
- 3.2. If, in the opinion of the Processor, an instruction as referred to in the first paragraph is contrary to a legal provision on data protection, the Processor shall inform the Controller of this prior to processing, unless a legal provision prohibits such notification.
- 3.3. If the Processor is required by law to disclose Personal Data, he shall inform the Controller immediately, and if possible, before the disclosure.
- 3.4. The Plek platform provides the Controller with all the necessary tools to comply with a request from a Data Subject who wishes to exercise their privacy rights. These rights include requests for access, correction, supplementation, deletion or blocking of their data, objecting to the processing of their personal data, and requests for the portability of their own Personal Data.
- 3.5. The Processor shall only process the personal data within the European Union and ensures that no processing activity takes place outside the European Union, except with the express written approval of the Controller.
- 3.6. The Processor shall not allow the personal data to be processed by a Sub-processor without the express written permission of the Controller. This consent will only be given on the condition that a written agreement is signed between the Processor and the

Sub-processor, which at a minimum guarantees that the Sub-processor commits to complying with the same agreements that apply to the Processor under this agreement.

- 3.7. The Processor shall provide all information necessary to demonstrate that the obligations of this Data Processing Agreement have been and are being fulfilled.

## **4. Security of Processing**

- 4.1. Appendix 2 outlines the appropriate technical and organizational measures taken by the Processor.
- 4.2. These measures ensure an appropriate level of security, considering the nature of the Personal Data processed by the Processor and the current state of technology.
- 4.3. The Controller has the right to, at its own expense, conduct investigations into the security measures implemented by the Processor and their compliance. The Processor is required to reasonably cooperate with such investigations (Article 28 GDPR).

## **5. Data breaches**

- 5.1. The Processor implements measures to reasonably ensure that a security breach is detected as promptly as possible.
- 5.2. As soon as the Processor discovers a Data Breach or otherwise becomes aware of it, the Processor will immediately take all necessary steps to correct the security deficiencies that led to the Data Breach and to mitigate its effects. The Processor will also cooperate with the Controller to investigate the cause of the Data Breach and take any measures the Controller deems necessary to prevent a similar incident.
- 5.3. If a security breach occurs, the Processor must notify the Controller within 48 hours. The notification must at least include the nature of the breach, the (possible) consequences of the breach, and the measures taken to mitigate the adverse effects of the breach.
- 5.4. The Processor will provide further information to the Controller upon request, at the Controller's first request.
- 5.5. The Controller will assess whether there is a security breach that leads to a substantial chance of serious adverse effects or has serious adverse effects on the protection of Personal Data. In such a case, the Controller will notify the Personal Data Authority.

## **6. Audit**

- 6.1. The Controller has the right to conduct an audit of the Processor no more than once every twelve months to assess the extent to which the Processor is complying with the obligations set forth in this Data Processing Agreement. The audit will be conducted by an independent third party and will take place at a time agreed upon by both the Controller and the Processor. The Controller bears the costs of the audit.
- 6.2. Upon a request from the Controller to conduct an audit, the Processor may choose to provide an audit report prepared by an independent auditor that demonstrates the Processor's compliance with its obligations under this Data Processing Agreement. If such a report is provided, the Controller loses its right to conduct an audit at the Processor for twelve months.

## **7. confidentiality**

- 7.1. The Processor shall keep the Personal Data provided by the Controller confidential, unless a legal obligation necessitates disclosure.
- 7.2. The Processor will ensure that its Employees and Sub-processors also adhere to this confidentiality obligation by incorporating a duty of confidentiality into their (employment) contracts.

## 8. Liability

- 8.1. The Processor is liable to the Controller for any damage incurred by Third Parties and/or the Controller caused by the Processor's non-compliance with the provisions of this agreement and/or applicable laws and regulations. Damage also includes any administrative fines imposed on the Controller by a regulatory authority in connection with the Processor's processing activities and/or a security breach.
- 8.2. The Processor is excluded from liability if the damage results from negligence on the part of the Controller, such as the provision of Personal Data through insecure channels (such as email or an unsecured Excel list) or unauthorized access to Plek.
- 8.3. Liability for breaches involving Special and Sensitive Personal Data, except for profile photos, is excluded. The Controller is responsible for ensuring that such data are not shared on Plek.

## 9. Applicability of law and dispute resolution

- 9.1. This Data Processing Agreement is part of the Service Agreement. Therefore, all rights and obligations from the Service Agreement also apply to the Data Processing Agreement.
- 9.2. In the event of any contradictions between the provisions in the Data Processing Agreement and the Service Agreement, the provisions of this Data Processing Agreement will prevail.
- 9.3. Deviations from this Data Processing Agreement are only valid when the Parties agree in writing.
- 9.4. Dutch law applies to this agreement and its execution.
- 9.5. All legal disputes that may arise between the parties in connection with this agreement will be submitted to the competent court in the district where the Controller is located.

Thus agreed and drawn up in duplicate,

**On behalf of the Controller**

Statutory name: \_\_\_\_\_

Address: \_\_\_\_\_

Place: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

**On behalf of Processor**

Plek Group BV

Rokin 81

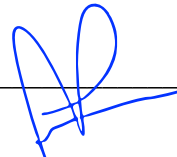
1012 KL, Amsterdam

Andy Verstelle

CEO

April 17, 2024

\_\_\_\_\_



## Appendix 1: Processing of Personal Data

### Types of Personal Data Processed by the Processor:

- Personal and work-related data of employees of the Controller who have been provided an account and who fill out their profile. The precise list of fields was selected by the Controller during the implementation phase of Plek. Only the first and last name fields are mandatory.
- Personal and work-related data of external stakeholders of the Controller who are provided an account upon invitation and who fill out their profile. The precise list of fields was selected by the Controller during the implementation phase of Plek. Only the first and last name fields are mandatory.
- Personal data voluntarily provided (text and/or image), processed in contributions within a community.
- Statistical information about the use of the Plek application.
- Logging of IP address and technical usage information for security and optimization purposes.

### Processing Activities:

The Processor carries out the following processing activities:

- Optionally imports fields from ADFS, supplemented with one or more freely fillable fields;
- Provides the employees of the Controller with the ability to fill out their profile based on these fields;
- Also provides external stakeholders of the Controller, who gain access by invitation, with the ability to fill out their profile;
- Offers employees of the Controller and connected stakeholders of the Controller the opportunity to engage in dialogue with each other.

### Purpose of the Processing:

Plek provides, with its social platform, the opportunity to form communities where users can:

- Find colleagues and communicate with each other;
- Exchange knowledge, ideas, and news;
- Share, evaluate, and comment on plans, designs, and documents;
- Collaborate and exchange thoughts on various topics.



## Appendix 2: Appropriate technical and organizational measures

### Organization and Assessment:

- The Processor's network and the OTAP server infrastructure are managed by a hosting company certified according to ISO27001, ISO9001, and NEN7510 standards.
- The information security policy and its implementation within the Processor's organization are annually assessed against the requirements of ISO27001 and Rijksrichtlijnen BIR2017 BBN2; an in-control statement (ICV) is issued annually.
- The Processor's team is well-informed and operates according to a defined and documented information security policy within an Information Security Management System (ISMS). This policy is implemented in accordance with ISO27001 / BIR2017.
- Any technical vulnerabilities are regularly remedied by patching software or ad hoc in the event of an acute threat.

### Hosting:

- The Processor's platform runs on a redundant, secure private cloud or, if agreed, on-premise at the Controller's location.
- All servers and relevant facilities are located in the Netherlands (out of reach of the Patriot Act).

### Application Security and Data Traffic:

- The architecture is designed to address vulnerabilities in the OWASP top-10 and other vulnerabilities.
- Access security with 2-factor authentication is optionally adjustable per role.
- All data traffic with the Processor, its employees, and participating externals is encrypted over SSL/TLS connections (https).
- The Processor's database servers are only accessible from application servers.
- All channels and groups have properties to determine who can view, add, or modify content.
- Various roles are defined, such as Admin, Content Manager, and User. Admins can grant access to other Admins, Content Managers, and Users.
- The chat function supports end-to-end encryption.
- All changes are logged in the version history.

### Logging, Monitoring, and Reporting:

- The Processor and its hosting partner continuously register and monitor all network activity.
- The Processor informs the Controller about information security through Incident Reporting.
- Statistics are optionally anonymized.

## Appendix 3: Sub-processors

For the provision of the Service, the Processor collaborates with the list of Sub-processors below

Sub-processor	Type	Country	Certification
TRUE B.V.	Hosting	The Netherlands	ISO27001 ISO 9001 NEN 7510

## Appendix 4

Contact details of the Responsible Data Protection Officer

Name: \_\_\_\_\_

Function: \_\_\_\_\_

E-mail address: \_\_\_\_\_

Telephone: \_\_\_\_\_