

Data Processing Agreement

Recticals

This Data Processing Agreement (hereinafter: "Processing Agreement") is an annex to the General Terms and Conditions of Payflip. The General Terms and Conditions and the Processing Agreement together form part of the Agreement between the Customer and Payflip.

By means of this Processing Agreement, the Parties wish to record in writing their mutual agreements regarding (i) the management, security and/or Processing of such Personal Data and (ii) the obligation of the Parties to comply with Privacy Legislation.

Article 1: definitions

In this Processing Agreement, the following terms (when written with a capital letter) have the meaning described in this Article: "Agreement", "Customer", "Party"/"Parties", "Services", "Payflip", "Term", "Confidential Information", "GDPR", "Benefit Provider", "Employee" and "Tool" have the meaning given to them in the General Terms and Conditions.

"Controller", "Data Subject", "Personal Data Breach", "Third Party", "Data Protection Impact Assessment", "Supervisory Authority", "Processor" and "Process/Processing" have the meaning given to them in the Privacy Legislation.

"Personal Data": all personal data, as defined in Article 4(1) of the GDPR, for which the Customer is responsible as Controller and which Payflip expects to Process on behalf of the Customer in the context of providing its Services, a non-exhaustive list of which can be found in Annex 1.

"Sub-processor": any Processor engaged by Payflip as a subcontractor and authorized to, in the context of this Processing Agreement, obtain logical access to certain Personal Data and process it with a view to providing (parts of) the Services or technical support, and who undertakes to process this Personal Data exclusively for and on behalf of the Controller in accordance with this Processing Agreement.

"Substantial Sub-processor": a Sub-processor that forms an essential and indispensable part of the Services, by structurally Processing Personal Data in the context of the Services. This includes in particular (but not exclusively) suppliers involved in hosting, database management, providing essential or built-in functionalities and customer support. Sub-processors that only incidentally, supplementarily or to a very limited extent Process Personal Data via Payflip, or that are not necessarily connected to the core functionality of the Tool and/or the Services, are expressly not considered Substantial Sub-processors.

This Processing Agreement contains the following annexes:

- **Annex I:** Overview of (i) the Personal Data that the Parties expect to be processed by Payflip in the context of the Services, (ii) the categories of Data Subjects to whom the Personal Data relates, (iii) the intended use (i.e., the manner(s) of Processing) of the Personal Data and (iv) the agreed purposes and means of that Processing.
- **Annex II:** Overview and description of the technical and organizational security measures that Payflip has taken in the context of this Processing Agreement.
- **Annex III:** Overview of the various Substantial Sub-processors that Payflip uses.

Article 2: capacity of parties

2.1 For the provision of the Services, Payflip processes the Personal Data listed in Annex I. The Customer acts as Controller within the meaning of the Privacy Legislation and entrusts the processing of this Personal Data to Payflip, which processes it in the name and on behalf of the Customer as Processor.

2.2 This Processing Agreement relates exclusively to Payflip's role as Processor. For information about the processing of Personal Data by Payflip in its role as Controller, we refer to the Privacy Statement.

2.3 The Customer and Payflip are referred to for the remainder of this Processing Agreement as the "CONTROLLER" and the "PROCESSOR" respectively.

Article 3: mutual obligations

3.1 Both Parties expressly undertake to comply with the provisions of the Privacy Legislation and not to do or omit anything that could cause the other Party to violate the Privacy Legislation. Both Parties undertake to take appropriate measures to ensure that the Personal Data is not misused or obtained by an unauthorized Third Party.

3.2 The PROCESSOR will Process the Personal Data in a proper and careful manner, in accordance with the Privacy Legislation, the provisions of this Processing Agreement and the written instructions of the CONTROLLER. More specifically, when performing the Services, the PROCESSOR will make all its know-how available to perform the Services according to the rules of the art, as befits a specialized and 'good' Processor.

3.3 The CONTROLLER is the owner of and fully responsible for the Processing of the Personal Data, including the nature and purpose of the Processing, the proportionality, the retention periods, and the accuracy, quality and lawfulness of the Personal Data and the manner in which it has acquired such Personal Data. This responsibility and control never rest with Payflip.

Article 4: duration of processing

4.1 This Processing Agreement remains in force as long as the PROCESSOR processes Personal Data in the name and on behalf of the CONTROLLER as part of the Agreement. When the Agreement ends, this Processing Agreement also ends.

4.2 In the event of a breach of this Agreement or the applicable provisions of the Privacy Legislation by the PROCESSOR, the CONTROLLER may instruct the PROCESSOR to immediately cease Processing the Personal Data.

4.3 The PROCESSOR does not retain Personal Data longer than necessary for the performance of the Services.

(i) During the term of the Agreement, the PROCESSOR pseudonymizes or anonymizes Personal Data as soon as it is no longer relevant for the performance of the Services. At the request of the CONTROLLER or the Data Subject, the PROCESSOR permanently deletes the relevant Personal Data.

(ii) After the end of the Agreement, the PROCESSOR deletes all Personal Data within thirty (30) calendar days, or earlier if the Customer so requests. If applicable law requires longer retention, the PROCESSOR may retain the Personal Data as long as legally necessary. Backup copies containing Personal Data may be retained for a maximum of one (1) year. Upon express request of the CONTROLLER, the PROCESSOR can return the Personal Data to the CONTROLLER by means of an export. This export takes place according to the modalities as described in the General Terms and Conditions.

Article 5: assistance to controller

5.1 **Compliance with legislation.** Taking into account the nature of the Processing and the information available to it, the PROCESSOR provides the CONTROLLER with assistance in complying with the obligations pursuant to Articles 32 to 36 of the GDPR.

5.2 **Personal Data Breach.** In the event of a Personal Data Breach relating to the subject of the Processing of this Agreement, the PROCESSOR informs the CONTROLLER without delay, as soon as it becomes aware of a Personal Data Breach.

This notification contains at least the following information:

- The nature of the Personal Data Breach;
- The categories of Personal Data to which the Personal Data Breach relates;
- The categories of Data Subjects concerned and, approximately, the number of Data Subjects concerned;
- The categories of personal data records concerned and, approximately, their number;
- The likely consequences of the Personal Data Breach;
- Measures proposed or taken to address the Personal Data Breach, including, where appropriate, measures to limit any adverse consequences thereof.

5.3 If the PROCESSOR uses a Sub-processor, the PROCESSOR will require the Sub-processor to provide it with the same information if a Personal Data Breach occurs at the Sub-processor. The PROCESSOR immediately passes on to the CONTROLLER the information it receives from the Sub-processor.

5.4 The PROCESSOR and its Sub-processor(s) designate among their Employees a person who is a single point of contact and who is responsible for all communication between the PROCESSOR, the Sub-processor(s) and the CONTROLLER in the event of an incident that has led or may lead to an accidental or unlawful destruction or loss, unauthorized access, alteration or disclosure of Personal Data processed on behalf of the CONTROLLER.

5.5 Only the CONTROLLER decides, at its own discretion and in accordance with the Privacy Legislation, whether Data Subjects whose Personal Data are affected by a Personal Data Breach are informed thereof. It is the responsibility of the CONTROLLER to notify the Supervisory Authority of a Personal Data Breach.

5.6 The Parties, and if applicable the Sub-processor(s), ensure that they cooperate in good faith to limit the possible adverse consequences of a Personal Data Breach.

5.7 Data Protection Impact Assessment (DPIA). In addition, the PROCESSOR provides assistance to the CONTROLLER when it conducts a Data Protection Impact Assessment in accordance with Article 35 of the GDPR.

Article 6: information obligations

6.1 The PROCESSOR will at any time upon request of the CONTROLLER (however, with such a request the PROCESSOR must be given a reasonable period to comply with the request), provide the CONTROLLER with all information it needs and at least the information established by the provisions of this clause:

- All relevant data about its own business structure as well as accurate and updated identification data about all entities of the PROCESSOR involved in the processing of Personal Data, including the location of their head office;
- The aspects of the processing for which the services of the Sub-processor are or wish to be used and the identification data of a Sub-processor including the location of its head office. The PROCESSOR provides the CONTROLLER with the agreement with the Sub-processor(s) that relates to or is relevant to the processing of Personal Data, unless such agreement with the Sub-processor(s) contains Confidential Information, in which case it may remove such Confidential Information;
- Geographic data about the processing locations, including backup facilities and data destruction facilities.
- The physical, organizational, technical and logical security measures taken by the PROCESSOR and its Sub-processor(s), as specified in Article 11 of this Agreement.

Article 7: obligations of the processor

7.1 The PROCESSOR treats immediately or within a reasonable period (depending on the legal obligations specified in the GDPR) and properly all reasonable requests of the CONTROLLER regarding the processing of Personal Data related to this Agreement.

7.2 The PROCESSOR ensures that there are no obligations arising from applicable legislation that make it impossible for it to comply with the obligations of this Agreement.

7.3 The PROCESSOR undertakes to process Personal Data only for the purpose of performing the Services and to meet the responsibilities of this Agreement in accordance with the written instructions of the CONTROLLER. The PROCESSOR may and will only process the Personal Data listed in Annex 1, in accordance with the Processing activities agreed therein and exclusively for the purposes specified therein, unless legislation expressly provides otherwise, in which case the PROCESSOR immediately informs the CONTROLLER thereof.

7.4 The CONTROLLER may unilaterally make limited changes to the instructions. The PROCESSOR is consulted before significant changes to the instructions are made. Both Parties must agree to changes that affect the main provisions of the Agreement. The PROCESSOR may refuse to follow the instructions of the CONTROLLER if the PROCESSOR reasonably judges that the instructions may be contrary to the Privacy Legislation (cf. art. 8.3) or other mandatory legislation (cf. Article 8.5), in which case the PROCESSOR immediately informs the CONTROLLER thereof.

7.5 The PROCESSOR ensures that access to, inspection, processing and provision of Personal Data only occurs in accordance with the principle of proportionality and the 'need-to-know' principle (i.e., that data is only provided to persons who need the Personal Data to perform the Services).

7.6 The PROCESSOR undertakes to provide Personal Data only to the Employees of the CONTROLLER who need the Personal Data to comply with the obligations of this Agreement and ensures that the relevant Employee commits to confidentiality or is bound by a legal confidentiality obligation, unless such provision is provided for under the Main Agreement.

Article 8: obligations of the controller

8.1 The CONTROLLER provides all necessary assistance to the PROCESSOR and cooperates with it in good faith to ensure that every

Processing of Personal Data complies with the provisions of the GDPR, in particular the principles relating to the Processing of Personal Data.

8.2 The CONTROLLER agrees with the PROCESSOR on appropriate communication channels to ensure that the instructions, guidelines and other communications regarding Personal Data Processed by the PROCESSOR on behalf of the CONTROLLER are properly received by the Parties. The CONTROLLER informs the PROCESSOR of the identity of the person who is the single point of contact of the CONTROLLER with whom the PROCESSOR should contact in application of this Article 8.2.

8.3 The CONTROLLER will make best efforts to give only instructions, guidelines or communications to the PROCESSOR that comply with the provisions of the GDPR.

8.4 The CONTROLLER provides the PROCESSOR and/or its Sub-processor(s) with the necessary assistance to the extent that a request, order, investigation or summons from a competent national government authority (such as a Supervisory Authority) or judicial authority relates to the Processing of Personal Data for which the CONTROLLER is responsible and the intervention of the CONTROLLER is necessary to comply therewith.

8.5 The CONTROLLER will make best efforts not to give instructions, guidelines or requests to the PROCESSOR that would cause the PROCESSOR and/or its Sub-processor(s) to violate obligations imposed by applicable mandatory national legislation applicable to the PROCESSOR and/or its Sub-processor(s).

8.6 The CONTROLLER ensures that it cooperates in good faith with the PROCESSOR to limit the adverse effects of a security incident that affects the Personal Data processed on behalf of the CONTROLLER by the PROCESSOR and/or its Sub-processor(s).

Article 9: use of sub-processors

9.1 The PROCESSOR may only appoint Substantial Sub-processors with prior written consent of the CONTROLLER to perform specific processing of Personal Data on behalf of the CONTROLLER. By signing this Processing Agreement, the CONTROLLER hereby agrees to the list of Substantial Sub-processors as listed in Annex 1 of this Agreement.

9.2 The PROCESSOR informs the CONTROLLER in writing of any intended change (addition or replacement; not: removal) of Substantial Sub-processors, whereby the CONTROLLER is given the opportunity to make a reasoned objection to such changes within a period of ten (10) calendar days.

9.3 If the CONTROLLER, in accordance with Article 9.2, makes a reasoned objection to the appointment of a new Substantial Sub-processor, and this objection is not deemed unreasonable or unfounded, the PROCESSOR will make all reasonable efforts in consultation with the CONTROLLER to find an appropriate solution. If no solution can be found, the Customer has the right to terminate the Agreement, insofar as the Services concerned cannot be provided without using the disputed Substantial Sub-processor.

9.4 The PROCESSOR ensures that its (Substantial) Sub-processors are bound by the same obligations regarding the Personal Data as those that bind the PROCESSOR under this Agreement.

9.5 The PROCESSOR will accurately and immediately communicate the purposes established by the CONTROLLER and the instructions given to the (Substantial) Sub-processor(s) when and where these purposes and instructions relate to the part of the processing in which the (Substantial) Sub-processor(s) is (are) involved.

Article 10: rights of data subjects

10.1 Taking into account the nature of the processing, the PROCESSOR provides the CONTROLLER with assistance by means of appropriate technical and organizational measures, to the extent possible, in fulfilling its duty to respond to requests to exercise the rights of the Data Subject established in Chapter III of the GDPR;

10.2 The following conditions apply to any request from Data Subjects regarding their rights concerning the Processing by the PROCESSOR and/or its Sub-processors of Personal Data relating to them:

- The PROCESSOR will make best efforts to notify the CONTROLLER immediately of any request from a Data Subject regarding Personal Data that the PROCESSOR and/or its Sub-processor(s) process on behalf of the CONTROLLER, without responding to such request unless the CONTROLLER expressly gives permission to do so;
- The PROCESSOR immediately complies with and requires its Sub-processor(s) to immediately comply with any request from the CONTROLLER so that the CONTROLLER can respond to a

request from the Data Subject who wishes to exercise one of its rights;

- The PROCESSOR ensures that both itself and its Sub-processor(s) have the required technical and organizational capabilities to block access to Personal Data and physically destroy the data without any possibility of retrieving it if and when the CONTROLLER makes such a request.
- The PROCESSOR provides upon simple request of the CONTROLLER on the basis of best efforts all necessary assistance and all required information that the CONTROLLER needs to defend its interests in any form of procedure – judicial procedure, arbitration or other – instituted against the CONTROLLER or its Employee due to a violation of the fundamental rights to privacy and the protection of Personal Data of the Data Subjects.

Article 11: security measures

11.1 During the term of this Agreement, the PROCESSOR implements and maintains appropriate technical and organizational measures in such a way that the processing meets the requirements of the GDPR and the protection of the rights of the Data Subject is guaranteed. The PROCESSOR will, among other things, take technical and organizational measures to protect (i) the Personal Data, including security against careless, improper, unauthorized or unlawful use and/or Processing and against unintentional loss, destruction or damage, and (ii) the confidentiality and integrity of the Personal Data, as set out in Annex 2.

11.2 The PROCESSOR will more specifically take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR.

11.3 In assessing the appropriate level of security, particular account was taken of the processing risks, especially as a result of the destruction, loss, alteration or unauthorized disclosure of, or unauthorized access to transmitted, stored or otherwise processed Personal Data, whether accidental or unlawful.

11.4 The CONTROLLER reserves the right to suspend and/or terminate the Agreement when the PROCESSOR can no longer provide technical and organizational measures appropriate to the processing risk.

Article 12: audit

12.1 The PROCESSOR acknowledges that the CONTROLLER is under the supervision of one/several Supervisory Authority(ies). The PROCESSOR acknowledges that any relevant Supervisory Authority has the right to conduct an audit at any time and in any case during the PROCESSOR's normal business hours, during the term of this Agreement to assess whether the PROCESSOR complies with the Privacy Legislation and the provisions of this Agreement. The PROCESSOR will provide the necessary cooperation.

12.2 The CONTROLLER has the right to verify or have verified the PROCESSOR's compliance with this Processing Agreement and the applicable Privacy Legislation. Such an audit may take place a maximum of once (1) per Term, unless there are valid reasons to conduct an additional audit (such as suspicion of an unreported Personal Data Breach, an ongoing investigation by a Supervisory Authority or serious suspicions of fraud). The CONTROLLER notifies the PROCESSOR in writing at least thirty (30) days in advance of its intention to conduct an audit. The notification states the name of the auditor, as well as the purpose and scope of the audit.

12.3 The PROCESSOR makes available to the CONTROLLER in the context of the Agreement all reasonable information to demonstrate that it complies with its obligations under this Agreement or the Privacy Legislation. If the information and reports provided by the PROCESSOR pursuant to this Article are insufficient to enable the CONTROLLER to demonstrate compliance with the obligations under the Privacy Legislation, the PROCESSOR and the CONTROLLER meet to agree on the operational, security and financial conditions of a technical on-site inspection. The conditions of this inspection may in no case prejudice the security of the PROCESSOR's other customers.

12.4 Upon written request of the CONTROLLER, the PROCESSOR provides the CONTROLLER, an independent third party, a certified auditor or an auditor appointed by the CONTROLLER or the relevant Supervisory Authority, access to the relevant parts of the PROCESSOR's administration and to all information and locations relevant to the PROCESSOR (and to those of its agents, subsidiaries and subcontractors) to determine whether the PROCESSOR complies with the Privacy Legislation and the provisions of this Agreement. Upon request of the PROCESSOR, the parties concerned enter into a confidentiality agreement.

12.5 The CONTROLLER ensures that the audit is conducted in a manner

that disrupts the PROCESSOR's business operations and service to its customers as little as possible. The audit takes place during the PROCESSOR's normal business hours and under conditions of strict confidentiality.

12.6 If the PROCESSOR and the CONTROLLER agree on a material deficiency in compliance with the Privacy Legislation and/or the Agreement, as shown by the audit, the PROCESSOR remedies this deficiency as quickly as possible. The Parties may agree to draw up a plan, including a timeline for its implementation, to remedy the deficiencies revealed during the audit.

12.7 The CONTROLLER bears the costs of any audit carried out within the meaning of this Article, unless the audit shows that the PROCESSOR has manifestly not complied with the Privacy Legislation and/or the provisions of this Agreement, in which case the PROCESSOR bears the costs of such audit.

Article 13: transfer to third parties

13.1 The transfer of Personal Data to Third Parties in any way is prohibited, unless it is legally required or the PROCESSOR has received the express consent of the CONTROLLER to do so. If a legal obligation applies to the transfer to Third Parties of Personal Data covered by this Agreement, the PROCESSOR informs the CONTROLLER thereof before the transfer.

13.2 The Controller may instruct the PROCESSOR to transfer Personal Data to third-party service providers (such as Benefit Providers or payroll partners) with whom the CONTROLLER has a separate agreement. This transfer can take place both manually and via technical integrations within the Tool. These third-party service providers are not Sub-processors of the PROCESSOR, but process the Personal Data as independent Controllers or as Processors of the CONTROLLER. The CONTROLLER warrants to the PROCESSOR that it has made appropriate contractual arrangements with such third-party service providers regarding data protection and remains responsible for the relationship with these parties. The role of the PROCESSOR is limited to technically facilitating the data transfer on the instruction of the CONTROLLER.

Article 14: international transfer

14.1. The PROCESSOR may only transfer or store Personal Data in a third country outside the European Economic Area ("EEA") or at an international organization, insofar as this is necessary for the performance of the Agreement and provided this is done in accordance with the applicable Privacy Legislation and the provisions of this Processing Agreement.

14.2. Such a transfer may only take place if one of the following conditions is met:

- a) the third country or international organization has been recognized by the European Commission as a country with an adequate level of protection (adequacy decision); or
- b) the transfer is subject to appropriate safeguards within the meaning of Article 46 GDPR, provided that the data subjects have enforceable rights and effective remedies. These safeguards may include:
 - i. binding corporate rules;
 - ii. standard contractual clauses for data protection as established by the European Commission in Decision 2021/914/EU of 4 June 2021 or any successor thereof;
 - iii. an approved code of conduct or an approved certification mechanism.

14.3. The PROCESSOR informs the CONTROLLER in advance when a change in the list of Substantial Sub-processors (see Article 9.2) leads to a transfer of Personal Data outside the EEA. The CONTROLLER accepts the current list of Substantial Sub-processors and the associated transfers (see Annex 3).

14.4 If the PROCESSOR is required to transfer Personal Data pursuant to applicable Union law or Member State law, the PROCESSOR will notify the CONTROLLER thereof prior to the transfer, unless that legislation prohibits notification for important reasons of general public interest.

Article 15: conduct regarding national government bodies and authorities

15.1 The PROCESSOR immediately notifies the CONTROLLER of any request, order, investigation or summons directed to the PROCESSOR or its Substantial Sub-processor by a competent national government authority or judicial authority that involves the disclosure of Personal Data processed by the PROCESSOR or a Substantial Sub-processor or any data and/or information related to such Processing by the PROCESSOR for and on behalf of the CONTROLLER.

15.2 Without prejudice to Article 15.1 of this Agreement, the PROCES-

SOR ensures that there are no obligations of applicable legislative law that make it impossible for the PROCESSOR to comply with its obligations under this Agreement.

Article 16: liability

16.1 The CONTROLLER involved in the processing is liable for damage caused by Processing that is contrary to the Privacy Legislation and this Agreement. Without prejudice to the General Terms and Conditions, the PROCESSOR is only liable for damage caused by Processing if it has not complied with the obligations of the Privacy Legislation specifically intended for Processors or when it has acted outside or contrary to this Processing Agreement or the lawful instructions of the CONTROLLER.

16.2 The CONTROLLER or the PROCESSOR is exempt from liability pursuant to point 16.1 if it proves that it is in no way responsible for the event that caused the damage.

16.3 Each Party is solely liable for administrative fines or other sanctions imposed on it by a Supervisory Authority, insofar as these are the direct result of a breach of the Privacy Legislation or this Agreement attributable to that Party. Neither Party can recover from the other Party the payment of an administrative fine or sanction resulting from its own breach of the Privacy Legislation or this Processing Agreement.

16.4 When it appears that both the PROCESSOR and the CONTROLLER are responsible for the damage caused by the processing of Personal Data, both Parties are liable and both pay compensation in proportion to their individual share in the responsibility for the damage caused by the processing.

16.5 When both the CONTROLLER and the PROCESSOR are involved in the same processing and they are responsible pursuant to points 16.1 and 16.4 for damage caused by the Processing, both the CONTROLLER and the PROCESSOR are held liable for the full damage, in order to ensure effective compensation of the Data Subject.

16.6 When the CONTROLLER or the PROCESSOR has paid the full compensation for the damage suffered in accordance with point 16.5, that CONTROLLER or that PROCESSOR has the right to recover from the other the part of the compensation corresponding to their share of the responsibility for the damage, in accordance with the conditions of point 16.1 and/or in accordance with the limitation of liability as specified in this Article 16.

16.7 The limitation of liability included in the General Terms and Conditions applies in full to this Processing Agreement. The liability of the PROCESSOR under this Processing Agreement will in no case exceed the limits agreed in the General Terms and Conditions.

Article 17: mediation and jurisdiction

17.1 The PROCESSOR agrees that if the Data Subject brings a claim for damages against it under this Agreement, the PROCESSOR will accept the Data Subject's decision:

- To submit the dispute to an independent person for mediation;
- To submit the dispute to the courts in Belgium.

17.2 The Parties agree that the Data Subject's choice does not prejudice its substantive or procedural rights of redress in accordance with other provisions of applicable national or international legislation.

17.3 Any dispute between the Parties about the terms of this Agreement will be brought before the competent courts as specified in the General Terms and Conditions.

Annex 1: Processing of Personal Data by Payflip

This annex contains an overview of the Personal Data that Payflip expects to Process on behalf of the Customer in the context of the Agreement, as well as the relevant categories of Data Subjects, the manner(s) of Processing Personal Data and the means and purposes of Processing.

1. Categories of Personal Data

Personal Data

- Full name
- Email address (professional or private)
- Signature
- Address
- Telephone number

Employment Data

- Date of entry into service with the company (the Customer)
- Joint committee
- External identifier of the payroll provider of the company (the Customer)
- Employment contract

Salary Data

- Gross monthly salary
- Year-end bonus
- NSSO coefficient (employer and employee)

Bank details (for reimbursement of benefits)

- IBAN
- Name of bank institution

Car data (for mobility budget)

- Leasing price / TCO
- Leasing period
- License plate
- Location data (charging/fuel stations)

Data editable by Employees

Employees can manage or update the following data themselves via the Tool:

- Address
- Preferred language (NL, FR or EN)
- Documents that can be re-uploaded

The Personal Data listed in this overview do not qualify as special categories of Personal Data within the meaning of Article 9 of the GDPR. Payflip processes in its capacity as Processor exclusively identification and employment-related data necessary for the performance of the Services on behalf of the Customer.

This does not alter the fact that certain Personal Data, in particular financial and payroll data (such as salary data, bank account numbers and contractual wage components), are considered sensitive and confidential in practice. Payflip grants these data an appropriately increased level of protection.

Any processing of special categories of Personal Data by the Customer (for example via documents uploaded by Employees) falls outside the intention and responsibility of Payflip and remains entirely under the exclusive responsibility of the Customer as Controller.

2. Categories of Data Subjects

Employees of the Customer who have access to the Tool

3. Purposes of processing

Payflip processes this Personal Data exclusively for the performance of the Services under the Agreement, including among others:

- Managing and implementing benefits or remuneration options offered by the Customer to Employees;
- Supporting the Customer in using the platform and the technical functionalities necessary for the performance of the Services;
- Facilitating data exchange with third-party service providers selected by the Customer, such as payroll partners or benefit providers, on the instruction of the Customer;
- Performing administrative, technical and security-related actions necessary for the performance of the Agreement.

Independent of its role as Processor, Payflip may process limited Personal Data of Employees to generate anonymized and aggregated usage data. This usage data is processed by Payflip as an independent Controller for legitimate business purposes, such as statistical analysis, research, training, product improvement and platform security. In addition, Payflip as Controller is authorized to anonymize and aggregate Customer data entered by the Customer or its Employees in the Tool. This anonymized Customer data is used exclusively for internal purposes, in particular to improve the Services. Both processing activities fall outside the scope of this Processing Agreement and are governed by Payflip's Privacy Statement and the applicable Privacy Legislation.

4. Manner and means of processing

- Manner of processing: electronically via the Tool, including automatic synchronizations with third-party service providers selected by the Customer (e.g., payroll partners, Benefit Providers).
- Means of processing: the Tool, secure servers, backups and document storage within the Tool.
- Security: processing takes place with appropriate technical and organizational measures as described in Annex 2.

Annex 2: Technical and Organizational Measures

This annex describes the technical and organizational measures that Payflip as Processor applies for the processing of Personal Data of the Controller. The measures are intended to ensure the confidentiality, integrity and availability of Personal Data, in accordance with Article 32 GDPR.

1. Security infrastructure

- Personal Data is stored within a secure Microsoft Azure cloud infrastructure within the European Union.
- Databases have replicas for redundancy and availability, so that data loss is prevented and continuity is guaranteed.
- Access to servers and databases is managed via Azure's role-based access controls and authentication.

2. Security of data at rest and in transit

- Personal Data is encrypted at rest (database encryption) and encrypted in transit (TLS/HTTPS).
- Sensitive data such as IBAN, salary information and other confidential data are additionally secured within the database.

3. Access management and authorization

- Payflip employees have access to Personal Data via role-based access control within the platform, where rights are assigned based on operational necessity (least privilege).
- Employees of the Controller only have access to their own data via the rights and invitations set by the Customer.
- Access to production data for development or testing purposes is excluded. Development environments only use synthesized or anonymized data.

4. Authentication and identification

- Logging into the Payflip platform takes place via 256-bit SSL/TLS and is authenticated via Auth0.
- Payflip employees log into their hardware (laptop, phone) with a strong password; optional additional authentication (Touch/Face ID) can be set individually.
- All platform accounts have unique credentials; access to the platform is regulated via internal processes and role management.

5. Software development and code management

- Production data is not available in development or test environments.
- Access to production data is strictly limited to operational processes and necessary support.
- Code is tested in separate development environments without access to live customer data.

6. Cloud and infrastructure security

- Use of cloud-based solutions (Microsoft Azure) reduces the risk of physical theft or unauthorized access.
- Backups are made periodically.
- Backups and replicas are located exclusively within the EU, ensuring continuity and compliance with the GDPR.

7. Monitoring, logging and audit

- Payflip uses logging and monitoring of the infrastructure and provider tools used to record system activities, access and incidents.
- Logs contain information about changes in infrastructure and authentication, with which unauthorized access can be detected.
- Although platform-level logging of all employee actions is limited, operational and infrastructure activities are closely monitored.

8. Incident and notification policy

- Payflip has a documented internal policy for reporting Personal Data Breaches and security incidents, in accordance with GDPR.
- Employees are trained in this policy and required to follow these procedures.
- Relevant incidents are investigated in a timely manner and, if applicable, reported to the Controller.

9. Retention and deletion of data

- After the end of the Agreement, the Processor deletes all Personal Data of the CONTROLLER within thirty (30) calendar days.
- Backups are retained for a maximum of one (1) year after the end of the Agreement.
- Personal Data is also returned to the CONTROLLER upon request via export, in accordance with the procedure as laid down in the General Terms and Conditions.

Annex 3: Substantial Sub-processors

The PROCESSOR is authorized to use the following Substantial Sub-processor(s):

Sub-processor Name	Processing Activity	Category	Data Storage Location	Registered Office
Microsoft Azure	Cloud infrastructure: provides the cloud environment in which our Tool runs.	Infrastructure & hosting	EU	VS
MongoDB	Database provider: manages and stores data within our databases.	Infrastructure & hosting	EU	US
Datadog	Monitoring & log analysis: monitors the performance, logs and operational status of the Tool.	Infrastructure & hosting	EU	US
Netlify	Content Delivery Network (CDN): provides content distribution and fast delivery of web assets to end users.	Infrastructure & hosting	EU	US
Amazon Web Services (AWS)	Adobe PDF document generation: generates PDF documents within the platform.	Functionality	EU	US
Postmark	Email service provider: sends emails to end users, such as notifications or communications.	Functionality	EU	US
Auth0 (Okta)	Identity management: manages user authentication and single sign-on (SSO) for the Tool.	Functionality	EU	US
Dropbox Sign	e-Signature provider: provides an API for employees to sign digital contracts.	Functionality	EU	US
Make	iPaaS & automation service: automates workflows in the context of customer support.	Customer support	EU	US
Intercom	Front-office support messaging system: facilitates communication between end users and the support department.	Customer support	EU	US
Anthropic, PBC	Customer support operations & reporting	AI services	US	US