Data Processing Agreement

Version 2.1

Version:	2.1
Last changed:	September 2022

Contents

Standard Clauses for Data Processing

Version: September 2022

These standard clauses and its annexes constitute the data processing agreement ("DPA") which forms an integral part of the Agreement.

Article 1. Definitions

The following terms have the following meanings ascribed to them in this Data Processing Agreement and in the Agreement:

1.1 Dutch Data Protection Authority (AP): the regulatory agency outlined 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 Subject: a natural person who can be identified, directly or indirectly.

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

1.6 Agreement: the agreement concluded between the Client and the Data Processor, on whose basis the ICT supplier provides services and/or products to the Client, the data processing agreement being part of this agreement.

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

1.8 Data Processing Agreement: the present Standard Clauses for Data Processing and its annexes within the meaning of Article 28.3 of the GDPR.

1.9 Controller: the party who determines the purpose and means of the processing.

Article 2. General provisions

2.1 The details of the processing activities to be carried out by the Data Processor under the Agreement and, the special categories of Personal Data where applicable, are specified in Annex 1.

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

2.3 The technical and organizational measures in Annex 2, may be adapted from time to time to changing circumstances by the Data Processor. The Data Processor will notify the Client in the event of significant revisions. If the Client cannot reasonably agree to the revisions, the Client will 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.

2.4 The Data Processor will process the Personal Data on behalf of the Client, in accordance with instructions provided by the Client and accepted by the Data Processor.

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

2.6 The Data Processor will serve as the processor within the meaning of the GDPR and will therefore not have control over the purpose and means of processing the Personal Data, and will not make any decisions on the use of the Personal Data and other such matters.

2.7 The Data Processor will give effect to the GDPR as laid down in the present Standard Clauses for Data Processing and the Agreement. It is up to the Client to judge, on the basis of this information, whether the Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organizational measures so as to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.8 The Client will guarantee to the 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.

2.9 Administrative fines imposed on the Client by the Dutch Data Protection Authority will not be able to be recouped from the Data Processor, except in the event of willful misconduct or gross negligence on the part of the Data Processor's management team.

Article 3. Security

3.1 The Data Processor will implement the technical and organizational security measures outlined in Annex 2. In implementing the technical and organizational security measures, the Data Processor will 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 operations and the intended use of its products and services, the risks inherent in processing the data and risks of various degrees of likelihood and severity to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of the Data Processor's products and services.

3.2 Unless explicitly stated otherwise, the product or service provided by the Data Processor will not be equipped to process special categories of Personal Data or data relating to criminal convictions and offences.

3.3 The Data Processor seeks to ensure that the security measures it will implement are appropriate for the manner in which the Data Processor intends to use the product or service.

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

3.5 The Data Processor will be entitled to adjust the security measures it has implemented if it feels that such is necessary for a continued provision of an appropriate level of security. The Data Processor will record any significant adjustments it chooses to make, e.g. in a revised technical and organizational measures document, and will notify the Client of said adjustments where relevant.

3.6 The Client may request the Data Processor to implement further security measures. The Data Processor will not be obliged to honor such requests to adjust its security measures. If the Data Processor makes any adjustments to its security measures at the Client's request, the Data Processor will be allowed to invoice the Client for the costs associated with said adjustments. The Data Processor will not be required to actually implement these security measures until both Parties have agreed in writing and signed off on the security measures requested by the Client.

Article 4. Data breaches

4.1 The Data Processor does not guarantee that its security measures will be effective under all conditions. If the Data Processor discovers a data breach within the meaning of Article 4.12 of the GDPR, it will notify the Client without undue delay. The "Data Breach Protocol" section of Annex 2 outlines the way in which the Data Processor will notify the 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 the Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (the Client or its customer) will 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. The 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, the Data Processor will provide more information on the data breach and will help the Client meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information.

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

Article 5. Confidentiality

5.1 The Data Processor will ensure that the persons processing Personal Data under its responsibility are subject to a duty of confidentiality.

5.2 The Data Processor will be entitled to furnish third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or legal order to do so issued by a government agency.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by the Data Processor to the Client, and any and all information provided by the Data Processor to the Client which gives effect to the technical and organizational security measures included in Annex 2 are confidential and will be treated as such by the Client and will only be disclosed to authorized employees of the Client. The Client will ensure that its employees comply with the requirements outlined 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 and will enter into force at the time of the conclusion of the Agreement and will remain effective until terminated.

6.2 This Data Processing Agreement will end by operation of law when the Agreement or any new or subsequent agreement between the parties is terminated.

6.3 If the data processing agreement is terminated, the Data Processor will delete all Personal Data it currently stores and which it has obtained from the Client within the timeframe laid down in Annex 2, in such a way that the Personal Data will no longer be able to be used and will have been rendered inaccessible. Alternatively, if such has been agreed, the Data Processor will return the Personal Data to the Client in a machine-readable format.

6.4 If the Data Processor incurs any costs associated with the provisions of Article 6.3, it will be entitled to invoice the Client for said costs.

6.5 The provisions of Article 6.3 do not apply if the Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such cases, the Data Processor will 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 will not apply if the 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, the Data Processor will cooperate with reasonable requests made by the Client relating to Data Subjects claiming alleged rights from the Client. If the Data Processor is directly approached by a Data Subject, it will refer the Data Subject to the Client where possible.

7.2 If the 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, the Data Processor will cooperate with such, following a reasonable request to do so.

7.3 In addition, at the Client's request, the Data Processor will 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, the Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, the Client will be entitled to have an audit performed (at its own expense) not more than once every year by an independent, fully certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The audit will be limited to verifying that the Data Processor is complying with the arrangements made regarding the processing of the Personal Data as laid down in the present Data Processing Agreement. The expert will be subject to a duty of confidentiality with regard to his/her findings and will only notify the Client of matters which cause the Data Processor to fail to comply with its obligations under the Data Processing Agreement. The expert will furnish the Data Processor with a copy of his/her report. The Data Processor will be entitled to reject an audit or instruction issued by the expert if it feels that 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.

7.4 The parties will consult each other on the findings of the report at their earliest convenience. The parties will implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. The Data Processor will implement the proposed measures for improvement insofar as it feels these 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.

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

Article 8. Sub-processors

8.1 The Data Processor has outlined in Annex 3 whether the Data Processor uses any third parties (sub-processors) to help it process the Personal Data, and if so, which third parties.

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

8.3 The Data Processor will notify the Client if there is a change with regard to the third parties hired by the Data Processor, e.g. through a revised Annex 3. The Client will be entitled to object to the aforementioned change implemented by the Data Processor. The Data Processor will ensure that any third parties it hires will commit to ensuring the same level of Personal Data protection as the security level the Data Processor is bound to provide to the Client pursuant to Annex 2.

Article 9. Other provisions

9.1 This DPA applies to the PayByLink system as provided by the Data Processor.

9.2 These DPA constitutes an integral part of the Agreement. Therefore, any and all rights and requirements arising from the Agreement, including any general terms and conditions and/or limitations of liability which may apply, will also apply to the Data Processing Agreement.

9.3 This DPA is drafted by PayByLink BV, Veenweg 158-B, 3641 SM, Mijdrecht (The Netherlands). If there are any queries about this Data Processing Agreement or data protection in general, please contact the CTO: Mr. Sjoerd Bakker by mail; info@paybylink.com or by phone: +31 (0)20 - 214 80 00.

Annex 1

Details of processing of Personal Data

A.1. Categories of Personal Data

Personal data relating to individuals provided to the Data Processor via the services and processed on behalf of and at the directions of the Controller, can pertain to the following categories of data, as applicable and depending on the services provided under the main agreement:

- **User data**
  1. **Users:** gender, first name, middle, last name, mail address, phone number, mobile number, address, postal code, city, country
  2. the Data Processor services can be used by a Client to upload any type of information / document, which may contain Personal Data.
- **Account data**
  1. **Payments:** order id, description, gender, client name, company name, mail address, phone number, sms text, mail text
  2. **Payment attachments as supplied by the client**
  3. **Mandates:** order id, description, gender, first name, last name, company name, company number, mail address, phone number, address, postal code, city, country, sms text, mail text
  4. **Direct Collect-data:** in case of an automatic payment creation in case of a failed direct collect: order id, description, gender, client name, company name, mail address, phone number, sms text, mail text
  5. **History info:** mail address, phone number, call back information
  6. **Mail messages:** all the sent mails are logged in the system and can therefor contain privacy sensitive information
  7. **SMS messages:** all the sent sms messages are logged in the system and can therefor contain privacy sensitive information
  8. **(API) Parameters:** all payment-, mandate- and direct collect parameters that are supplied to the system from an external source can contain privacy sensitive information
  9. **API Logging:** all the API calls are logged and can contain privacy sensitive information
  10. **Call back information:** call backs can be performed per e-mail or to external system and can contain privacy sensitive information
  11. **Payment Service Provider Payment attempts:** (partial) card or bank account number, raw response data as received from payment service provider is logged and can contain privacy sensitive information
- **Historical data**
  1. **Change history:** all the changes to the above information holders in the systems are logged, this change history information can contain privacy sensitive information

A.2. Special Category of Personal Data

By definition, the service is not intended and not developed to process “special category Personal Data” as specified in Article 9 GDRP. However, it is possible that users upload special category Personal Data for the use of the service (such as for example a photo on an identity card). Clients are specifically reminded that it could be that they upload special category Personal Data and that they remain responsible for this data. For the avoidance of doubt, Processor will in any case ensure that the users provides their prior consent to the processing of this special category of Personal Data.

A.3. Processing operations (nature and purpose of processing):

The specific processing activities to be carried out by the Processor can be, as applicable and depending on the services provided under the main agreement:

Services:

- sending payment/contract/mandate/authentication requests from the Client to consumers and/or companies for goods and / or services ordered from such user via electronic communications, including but not limited to email and sms;
- submitting reports, invoices and overviews of payments/contracts/mandates as to any processed requests to the Client;
- via an online portal an/or API and/or (s)-FTP.

A.4. Subject matter and duration of the processing of Personal Data

The subject matter of the Processing of Personal Data of the above category of data subjects concerns data that is entered by a client through the PayByLink services pursuant to the Agreement. Processor will process any Personal Data during the term of the Agreement and until the later of:

(i) 15 days after the date of cessation of any services involving the processing of Personal Data,

(ii) (ii) the expiration of any continuing obligations of Processor to retain Personal Data under the Agreement, and

(iii) (iii) the expiration of the time period for which Personal Data is maintained pursuant to applicable disaster recovery and/or data retention practices for the services.

Annex 2

Technical and Organizational Measures

B.1. The Data Processor has implemented the following security measures to protect its product or service:

i. Only authenticated users can logon to the system
ii. Only authorized users can see confidential information
iii. When users are deleted, all the user-data as described in Annex 1 Article A.1. will be anonymized in such a way that it can never be led back to the original data or user in any kind
iv. Users must change their password every 60 days. A new password must comply to the following rules and must:
   a. differ from the last 5 passwords and be different than the mail address of the user
   b. at least be 15 characters long and at least contain one uppercase letter (A, B, C, etc.)
   c. at least contain one lowercase letter (a, b, c, etc.)
   d. at least contain one special character (1, 2, !, #, @ etc.) except < or >
v. All data from the past remains available in the system. In the PayByLink back office (Maintenance – Entity info – Data Protection), Client can choose to anonymize data (as described in Annex 1 Article A.1.) after x months. Once this data has been anonymized, this information is permanently masked in the system (and accordingly will be masked in the back-ups after 30 days).
vi. Manual changes or deletions are final after 30 days.
vii. In case of an incident, data is available within any point of time in the past 30 days

B.2. The Data Processor will process the Personal Data provided by its clients:

within the European Economic Area (EEA).

B.3. Microsoft Azure, as Data Processor of PayByLink conforms to the principles of the following Information Security Management System (ISMS):

- ISO 27001
- PCI/DSSData leak protocol

B.4. In the unfortunate event that something goes wrong, the data processor will follow the following Data Breach Protocol to ensure that clients are notified of incidents:

- The Client is connected by DataProcessor within 24 hours after the event was discovered
- A detailed report of the leaked data is supplied to the Client

Data Processor will report any incidents to the Data Controller pursuant to article 33 GDPR.

B.5. The data processor will support its clients in the following way when they receive requests from data subjects:

- PayByLink offers the following functionality to Clients:
    - i. **To see what is known of the client** by showing a user overview page
    - ii. **To initiate a change** by offering a form that can be entered by the user and that will be processed by Data Processor within 30 days
    - iii. **To initiate a deletion of a client user** by offering a form that can be entered by the Client. After an explicit confirmation (twice) the data can ask to be removed from the system. This is performed within 30 days
        1. The user data will be anonymized
        2. An explicit warning will be shown to the user prior to this action
        3. After the user is anonymized, he/she won't be able to log on
    - iv. **To initiate a deletion of an account** by offering a form that can be entered by the user and that, after verification of the authorizations of the user, will be processed by Data Processor within 30 days
    - v. **To initiate a deletion of a license and all the underlying accounts** by offering a form that can be entered by the user and that, after verification of the authorizations of the user, will be processed by PayByLink within 30 days
    - vi. **To set an automatically deletion period** where the user can tell within what period of time **account data**, as mentioned in Annex 1 Article A.1., must be removed and/or anonymized
    - vii. **To anonymize customer data** that can be used to anonymize specific transactions within the PayByLink system with sensitive customer data
- **For all the items and actions as mentioned above, the law applies as well.** If the law states that Data Processor cannot delete financial data, this data is remained (and anonymized) within the system.

B.6. Once an Agreement with a Client has been terminated, the Data Processor will delete the Personal Data it processes on behalf of the Client within three months, in such a manner that they will no longer be able to be used and will be rendered inaccessible. Within this period of time, a Client with sufficient authorizations can download the data from the system to an Excel document and store this on his/her own device. Data Processor cannot be held responsible for the data once its' downloaded by the client

Annex 3

Sub processors

C.1. The data processor uses the following sub-processors:

- **Microsoft Azure (**all data is described in Annex 1 Article A.1.**)**
  Microsoft refers to their 'Online Services Terms', attachment 4, that can be found on this location: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46
- **SendGrid (only mail addresses, as described here: https://sendgrid.com/resource/general-data-protection-regulation/)**
  Please note that SendGrid does not – and does not currently have plans to – use servers or data centers in the European Union to process email. Thus, SendGrid cannot restrict data to the EU. However, neither current EU law nor the GDPR require this. Instead, what is required is that SendGrid must provide "appropriate safeguards" for data that it hosts and processes on its US servers (see Art 46 of the GDPR: https://gdpr-info.eu/art-46-gdpr/).
  PayByLink has signed a Data Processing Addendum (DPA) with SendGrid to provide such adequate safeguards, which includes provisions for when GDPR goes into effect. This can be send on request.
- **Spryng (SMS provider)**
  Spryng is a SMS provider in Europe that is both ISO 27001 and NEN 7510 certified.
  The virtual private clouds from Spryng are located in Frankfurt, so all data stays within the EU.
  https://www.spryng.nl/en/security/
- **SuperOffice Benelux (CRM platform)**
  SuperOffice is a modern CRM. Data stored in SuperOffice CRM Online is protected by a ISO 27001 certified Information Security Management System. All data is stored in Europe.
  https://www.superoffice.com/features/gdpr/