

## Data Processing Agreement

---

Between

(....)  
hereinafter "Client" or "Controller"

And

(Prodware)  
hereinafter "Prodware" or "Processor"

## Table of contents

Data Processing Agreement.....	1
1. Purpose.....	3
2. Definitions .....	3
3. Contractual documents.....	3
4. Duration of the assignment/notice of termination.....	3
5. Description of the processing being subcontracted out.....	4
6. Place of data processing .....	4
7. Technical and organisational measures .....	4
8. Rectification, blocking and erasure of data.....	4
9. Processor's obligations with respect to the controller .....	5
10. Subcontracting.....	5
11. Data subjects' right to information .....	6
12. Notification of personal data breaches .....	6
13. Assistance under article 35-36 GDPR.....	6
14. Security measures .....	6
15. The Data Protection Officer.....	6
16. Audit.....	7
17. Controller's obligations with respect to the Processor .....	7
18. Liability .....	7
19. Erasure of data and return of data carriers .....	8
20. Final provisions.....	8
Annex 1: Personal data.....	9
Annex 2: Technical and organisational measures In accordance with Art. 32 GDPR.....	10
Annex 3: Contact details of the parties .....	13

## 1. Purpose

1. The Client and Prodware have entered into one or several contracts for the provision of IT services (hereinafter "the Main Contracts" ). As Prodware may have access to personal data in rendering these services or needs such access in order to perform the assignment, the Client as Controller, and Prodware as Processor, require a contractual agreement (hereinafter "the Amendment") concerning the processing carried out on behalf of The Client, pursuant to Art. (28) (3) sentence 1 of the General Data Protection Regulation (GDPR).
2. The purpose of these clauses is to define the conditions in which the Processor undertakes to carry out, on the Controller's behalf, the personal data processing operations defined below.
3. As part of their contractual relations, the Parties shall undertake to comply with the applicable regulations on personal data processing and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from 25 May 2018 (hereinafter "the General Data Protection Regulation").

This Data Processing Agreement applies to the separate signed Main Contracts between Prodware and the Client, which purposes belong to the range of the following services:

- Implementation, development, migration, outsourcing, and/or intellectual services
- Hosting services
- Licence and Hardware
- Support and Maintenance services

## 2. Definitions

The concepts and terms contained in this Data Processing Agreement relating to personal data processing shall have the same meaning as stipulated in the GDPR.

## 3. Contractual documents

This Amendment and its Annexes constitute the entire Data Processing Agreement between the Parties. It replaces all previous agreements relating to its object. Any prior agreements between the Parties relating to personal data, are not binding on the Parties.

The contractual documents must be interpreted as forming a coherent and inseparable whole, with each of them complementing and being explicit in both technical and legal terms. In the case of a divergence between these documents, the decreasing order of priority is defined as follows:

- This document,
- Annex 1 Personal Data
- Annex 2 Technical and organisational measures In accordance with Art. 32 GDPR
- Annex 3 Contact details of the parties

Some of the contractual documents may be amended or enriched during the fulfilment of the Amendment. In any event, these amendments or enrichments must be covered by an amendment signed by the Parties. No modifications may be made to the Amendment and its Annexes without a document signed by both Parties.

## 4. Duration of the assignment/notice of termination

1. The duration of the assignment, (term of the contract) depends on the duration of the service agreement under the Main Contracts.

2. The termination of this Amendment therefore depends on the provisions concerning the duration and the termination of the Main Contracts. Notice to terminate the Main Contracts shall also have the effect of terminating this Amendment.
3. Furthermore, the premature termination of this Amendment without notice shall be permissible in the event of a serious breach of statutory or contractual data protection provisions, insofar as the Contracting Party in question cannot reasonably be expected to continue this Amendment.
4. The parties acknowledge that the termination of the Amendment at any time and for any reason, does not exempt them from their obligations relating to the collection, processing and use of personal data on behalf of another.

## 5. Description of the processing being subcontracted out

1. The Processor is authorised to process, on behalf of the controller, the necessary personal data for providing the service(s) covered by the Main Contracts.
2. The nature of operations carried out on the data is the one described in Main Contracts.
3. The purpose(s) of the processing is (are) the one described in the Main Contracts.
4. Categories of personal data are described in Annex 1
5. To perform the service covered herein, the controller shall provide the Processor with all the necessary information

## 6. Place of data processing

The data shall be processed by the Processor only in the territory of the European Economic Area , or in a member state of the European Economic Area.

1. Every transfer of personal data to a third country or to international organisations shall require the Client's prior agreement, and will be only permitted if the special conditions set out in Art. 44 to 50 GDPR have been fulfilled.
2. The Processor may not transfer personal data to a third country or an international organisation unless it has provided appropriate safeguards, including the signing of Standard Contractual Clauses between the controller and the recipient of the personal data in the third country, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
3. Therefore, by signing this Data processing agreement, the Customer as data exporter, explicitly gives to Prodware a clear and general mandate to sign, in his name and on his behalf, the 2010 standard contractual clauses with the data importer, which is a Prodware's non-EEA-based sub-processor.

## 7. Technical and organisational measures

1. Prodware shall take suitable technical and organisational measures to ensure a level of security appropriate to the risk, and must maintain these measures for the duration of the contract. Prodware guarantees that it has carried out the technical and organisational measures specified in **Annex 2** to this agreement.
2. The technical and organisational measures are subject to the current state of technology and technical progress. In this regard, Prodware is permitted to implement adequate alternative measures. These measures may not fall below the level of security of the stipulated measures. Material changes must be documented.

## 8. Rectification, blocking and erasure of data

1. Prodware shall only rectify, erase or block data processed on behalf of another, if instructed to do so by the Client's written request. Copies may only be made with the Client's prior agreement. However, this does not include copies that are necessary to ensure proper data processing and for the proper provision of the services in accordance with the Main Contracts, nor copies that are necessary in order to comply with the statutory retention requirements.

2. If a data subject should contact Prodware directly for the purpose of rectifying or erasing their data, Prodware shall pass on this request to the Client without delay.
3. These two commitments are applicable solely where the hosting of the customer's personal data is provided by Prodware.
4. GDPR activities that requires additional Prodware services can be provided at the tariff conditions in effect at the time of the request.

## 9. Processor's obligations with respect to the controller

The Processor shall undertake to:

1. process the data solely for the purpose(s) subject to the sub-contracting
2. process the data in accordance with the documented instructions from the controller appended hereto. Where the Processor considers that, an instruction infringes the General Data Protection Regulation or of any other legal provision of the Union or of Member States bearing on data protection, it shall immediately inform the controller thereof. Moreover, where the Processor is obliged to transfer personal data to a third country or an international organisation, under Union law or Member State law to which the Processor is subject, the Processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest
3. guarantee the confidentiality of personal data processed hereunder
4. take into consideration, in terms of its tools, products, applications or services, the principles of data protection by design and by default
5. ensure that the persons authorised to process the personal data hereunder:
  - a. have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
  - b. receive the appropriate personal data protection training

Compliance with approved codes of conduct in accordance with Art. 40 of the General data protection regulation, or an approved certification mechanism in accordance with Art. 42 of the General data protection regulation may be used as proof of sufficient guarantees within the meaning of Art. 28 of the General data protection regulation.

## 10. Subcontracting

Insofar as Prodware wishes to include Sub-Processor in the processing or Use of the Client's personal data, the following conditions shall apply:

1. The Processor may engage another Processor (hereinafter "the Sub-Processor") to conduct specific processing activities. In this case, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Sub-processors either via an email, either through the Prodware GDPR portal (<https://gdpr.prodwaregroup.com/fr>). This website is available via Internet and proposes an automatic notification mechanism in case of update if the Controller logs in.
2. This information must clearly indicate which processing activities are being Sub-contracted out, the name and contact details of the Sub-Processor and the effective dates of the Subcontract.
3. By signing this Amendment, the Controller approves the Sub-processors which were defined by the Processor.
4. The Controller has seven days from the date on which it receives said information to object thereto.
5. The Sub-Processor is obliged to comply with the obligations hereunder on behalf of and on instructions from the controller.
6. It is the initial Processor's responsibility to ensure that the Sub-Processor provides the same sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of the General Data Protection Regulation.

7. Where the Sub-Processor fails to fulfil its data protection obligations, the initial Processor remains fully liable with regard to the controller for the Sub-Processor's performance of its obligations.
8. Services that Prodware commissions from third parties as supplementary work in support of the assignment shall not be regarded as sub-contracting within the meaning of this provision. This includes such services as telecommunication services, maintenance and user services, cleaners, auditors or the removal of data carriers. However, Prodware must form appropriate and lawful contractual agreements and take control measures in order to guarantee the protection and security of the Client's data in the case of supplementary work by third parties.

### **11. Data subjects' right to information**

It is the Controller's responsibility to inform the data subjects concerned by the processing operations at the time data are being collected.

The Processor shall assist the Controller, insofar as this is possible, for the fulfilment of its obligation to respond to requests for exercising the data subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling).

Where the data subjects submit requests to the Processor to exercise their rights, the Processor must forward these requests as soon as they are received by email to a contact designated by the Controller.

GDPR activities that requires additional Prodware services can be provided at the tariff conditions in effect at the time of the request.

### **12. Notification of personal data breaches**

1. The Processor shall notify the Controller of any personal data breach not later than 48 hours after having become aware of it and via an email sent to the customer's contact defined in **Annex 3**.
2. Said notification shall be sent along with any necessary documentation to enable the Controller, where necessary, to notify this breach to the competent supervisory authority.

### **13. Assistance under article 35-36 GDPR**

1. Processor shall provide Controller with reasonable assistance needed to fulfil Customer's obligation under article 35 of the GDPR to carry out a data protection impact assessment related to Customer's use of the services, to the extent Customer does not otherwise have access to the relevant information, and to the extent, such information is available to Processor.
2. Processor shall provide reasonable assistance to Controller in the cooperation or prior consultation with the Supervisory Authority, to the extent required under article 36 of the GDPR.
3. This assistance will be provided at the tariff conditions in effect at the time of the request.

### **14. Security measures**

The Processor undertakes to process the personal data covered by the contract in such a way as to guarantee appropriate security and confidentiality. The details of the implemented security measures are given in **Annex 2**.

### **15. The Data Protection Officer**

The Processor has designated a data protection officer in accordance with article 37 of the GDPR. The name and contact details of the the DPO will be communicated in Annex 3..

## 16. Audit

1. The Processor will provide the Controller with all necessary information to prove compliance with the obligations set out in this Article and to allow and give reasonable support to audits, including inspections which shall be carried out by the Controller or a third party auditor commissioned by the Controller. Any third party auditor shall be expressly approved by Prodware.
2. In addition to the parties agree that the on-site audits (described in Clause 9 and Clause 17 of this Amendment) shall be carried out in accordance with the following specifications:
3. Following any notice by Client to Prodware of an actual or reasonably suspected unauthorized disclosure of Personal Data, upon Controller's reasonable belief that Processor is in breach of its obligations in respect of protection of Personal Data under this Amendment, or if such on-site audit is required by Controller's Supervisory Authority, Controller may contact Processor to request an on-site audit relevant to the protection of Personal Data.
4. Any such request shall occur no more than once annually, save in the event of an actual or reasonably suspected unauthorised access to Personal Data. Client shall reimburse Processor for any time expended for any such on-site audit at the Processor Group's then-current professional services rates, which shall be made available to Client upon request. Before the commencement of any such on-site audit, Client and Processor shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Client shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Processor.
5. Client shall promptly notify Processor with information regarding any non-compliance discovered during the course of an audit.

## 17. Controller's obligations with respect to the Processor

In accordance with Art. 5 (2) GDPR, the Client as Controller shall be responsible for compliance with the principles set out in Art. 5 (1) GDPR governing the processing of Personal Data (accountability).

The Client, as the owner of the data and the owner of all possible rights, shall comply with the following obligations :

1. The Client shall provide Prodware with the data that it needs for the provision of the services under the Main Contracts in good time and shall also be responsible for the quality of the data.
2. The Client shall document, in writing, any instruction bearing on the processing of data by the Processor.
3. The Client shall immediately notify Prodware of any errors or irregularities that it ascertains in relation to data protection provisions or its instructions when examining the results of the assignment.
4. The Client shall make sure that, before and during the processing, the Processor complies with the obligations set forth in the general data protection regulation.
5. The Client shall supervise the processing, including by conducting audits and inspections with the Processor. The person authorised to issue instructions on the part of the Client, the recipient of instructions on the part of Prodware and the responsible data protection officers, insofar as their appointment is required by law, are listed in **Annex 3**. In the event of a change in the responsible contact, the other Contracting Party must be notified of the name of the successor in writing without delay, providing the contact data.

## 18. Liability

1. The following liability clauses only concern the contractual relationship between the Client and Prodware. They do not represent a disclaimer with regard to the rights of the data subjects under Art. 82 (1) GDPR.
2. Prodware and its legal representatives or agents shall not be liable in the case of negligence. However, this disclaimer in relation to negligence shall not apply in the case of the breach of a fundamental contractual obligation. This Data Processing Agreement's Fundamental contractual obligations are obligations on the part of Prodware whose fulfilment is essential for the proper

- performance of this Data Processing Agreement, and obligations whose breach would jeopardise the achievement of the contractual purpose as set in article 1 of the Data Processing Agreement.
3. If and to the extent that Prodware or its legal representatives and agents are liable for negligence, liability shall be limited to the direct damages in the case of damages to property and financial loss. Liability for indirect or non-consequential damages shall be excluded.
  4. In any case, the amount of the compensation to be paid by if it is found to be liable, for all reasons taken together, may not exceed the total sum actually received by Prodware under the Main Contracts in the year in which the incident occurs.
  5. In the event of loss or deterioration of Data or files of the Client, and if the destruction/deterioration observed is due to Prodware, its liability will be limited to the reinstallation of the last back-up done by the Client.
  6. All the Client's claims for damages against Prodware shall become statute-barred two years after the event of damage. This shall not apply to claims in tort or due to an intentional infliction of damage.

### **19. Erasure of data and return of data carriers**

At the end of the service bearing on the processing of such data, the Processor undertakes to:

At the Parties' choosing:

1. destroy all personal data, or
2. return all personal data to the Controller, or
3. return the personal data to another Processor designated by the Controller

Together with said return, all existing copies in the Processor's information systems must be destroyed. Once destroyed, if asked to do so by the Client's written request, the Processor shall demonstrate, in writing, that this destruction has taken place.

Documents that serve to corroborate due and contractually compliant data processing or statutory retention periods shall also be retained by Prodware even after termination of the Amendment pursuant to the relevant retention periods.

GDPR activities that requires additional Prodware services can be provided at the tariff conditions in effect at the time of the request.

### **20. Final provisions**

1. If individual provisions of this Amendment should be or become ineffective, this shall not affect its remaining provisions. The Parties undertake to replace the ineffective provisions with a legally valid provision that comes closest to the purpose of the ineffective provisions.
2. In the event of contradictions between this Amendment and any other agreements between the Parties, especially the Main Contracts, the provisions of this Amendment shall take precedence.
3. Ancillary agreements, amendments and additions to this Amendment must be made in writing. This also applies to the amendment of this requirement for written form.
4. This Amendment and all transactions carried out in performing this Amendment shall be governed by local law and, insofar as applicable, the General Data Protection Regulation.
5. The Parties agree to submit to the exclusive jurisdiction of the court of local jurisdiction any claim or dispute arising from this Amendment.



## Annex 1: Personal data

---

Categories of personal data are:

- ✓ Civil status (identity, identification data, images, etc.)
- ✓ Personal life (lifestyle, family situation, etc.)
- ✓ Professional life (CV, vocational training, awards, etc.)
- ✓ Economic and financial information (income, financial situation, tax situation, etc.)
- ✓ Connection data (IP address, logs, etc.)
- ✓ Special categories of data:
  - Social security number

Categories of data subjects

- ✓ The Client's customers/prospects
- ✓ The Client's employees
- ✓ The Client's suppliers/service providers
- ✓ The Client's candidates
- ✓ The Client's partners

## **Annex 2: Technical and organisational measures In accordance with Art. 32 GDPR**

The contractor has implemented a comprehensive data backup concept that contains the necessary precautions in terms of construction, personnel, organisation and technology to ensure the safety of the objects and the data stock as well as undisturbed operation in an optimal manner.

The following technical and organisational measures have been taken:

a) Admission control:

Measures to prevent unauthorised persons from gaining access to the data processing equipment used to process personal data.

<b>Imple-mented</b>	<b>Measure</b>
Y	Access control guidelines and regulations
Y	Security areas are clearly defined
Y	Appropriate implementation of measures to secure the buildings
Y	Appropriate implementation of measures to secure Datacenter Access
Y	Security also outside working hours by alarm system and/or plant security
Y	Access only for authorized persons (company employees and external persons)
Y	Regulation for external parties
Y	Use of security badges
Y	Key Management
Y	Implementation of locks
Y	External staff is accompanied by Prodware staff

b) Access control:

Measures and procedures to prevent unauthorised persons from using the data processing equipment.

<b>Imple-mented</b>	<b>Measure</b>
Y	Regulation of user authorizations (administration incl. assignment of rights, assignment of special rights, revocation of authorizations, regular reviews).
Y	Password policy (secure passwords, regular changes, regular reviews).
Y	Use of encryption routines for mobile data carriers (incl. notebooks, USB sticks)
Y	Remote user authentication (cryptographic techniques, hardware identification, VPN solutions)
Y	Obligation to maintain data secrecy in accordance with Art. 28 Para. 3 lit. b GDPR
Y	Role based authorization
Y	Controlled destruction of data carriers
Y	Regular security audit

c) Access monitoring:

Measures to ensure that those authorised for data processing can only access the personal data subject to their access authorisation.

Imple-mented	Measure
Y	Control of access authorization (differentiated authorizations via profiles, roles, time limit)
Y	Provision of appropriate authentication technologies
Y	Security Logs (ex: unsuccessful and successful authentication attempts).
Y	Guidelines for the pseudonymization/anonymization of personal data

d) Transfer control:

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission, transport or storage on data carriers.

Imple-mented	Measure
Y	Guidelines for the exchange of information of all kinds
Y	Encryption during data transmission (network encryption, TLS)
Y	Logging during the transmission of data
Y	Method for detecting and protecting malware
Y	Access Control
Y	Encryption of data carriers before transport
Y	Handover of data carriers to authorized persons only
Y	Controlled destruction of data carriers

e) Input control:

Measures to ensure authenticated entry of personal data.

Imple-mented	Measure
Y	Acces control
Y	Data security policy
Y	Process, program and workflow organization

f) Order control:

Measures to ensure that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions.

Imple-mented	Measure
Y	Contract in writing with determination of the instructions
Y	Formalized order placement
Y	Careful selection of the subcontractor
Y	Monitoring the proper execution of the contract
Y	Separation of duty

g) Availability control:

Measures to ensure that personal data is protected against accidental destruction or loss.

Imple-mented	Measure
Y	Controlled process to ensure business operations (BCM)/IT-SCM
Y	contingency plans
Y	Regular back-ups according to backup plan
Y	Protection of systems against database failure, service level agreements with IT service providers
	Mirroring of data according to the contract SLA
Y	Antivirus/Firewall
Y	Redundant hardware

h) Separation control:

Measures to ensure that data collected for different purposes can be processed separately.

Imple-mented	Measure
Y	Client separation
Y	Functional separations

i) Procedures for periodic review and evaluation

Procedures for regular review, evaluation and evaluation of the effectiveness of technical and organisational measures

Imple-mented	Measure
Y	Data Protection Management
Y	Incident response management

**Annex 3: Contact details of the parties**

---

**1. Parties entitled to issue instructions and recipients of instructions**

Client

Name	Telephone	Email

Prodware

Name	Telephone	Email
As specified on the Prodware GDPR Portal ( <a href="https://gdpr.prodwaregroup.com/fr">https://gdpr.prodwaregroup.com/fr</a> )		

**2. Client's Data Protection Officer (or responsible)**

Name	Telephone	Email

**3. Prodware's Data Protection Officer**

Name	Telephone	Email
As specified on the Prodware GDPR Portal ( <a href="https://gdpr.prodwaregroup.com/fr">https://gdpr.prodwaregroup.com/fr</a> )		

**Place/date****Place/date****Client****Prodware**