

Data Processing Agreement

Table of Contents

1. Applicability, formation and version control

2. Definitions

3. Subject matter, duration, nature and purpose of the processing

4. Instructions and responsibilities

5. Security

6. Confidentiality and access

7. Sub-processors

8. Transfers outside the EEA

9. Assistance to the Customer

10. Data Breaches and security incidents

11. Retention periods, return and deletion

12. Audit, information and DPIA

13. Liability and indemnity

14. Order of precedence

15. Amendments

16. Term and termination

17. Governing law and disputes

Annex A. Description of the processing

Annex B. Sub-processor Register

Annex C. Technical and organisational measures

1. Applicability, formation and version control

These Data Processing Terms apply to every Main Agreement under which Salure B.V., trading under the name Salure, processes Personal Data on behalf of the Customer as Processor within the meaning of the GDPR.

The Customer is the Controller, unless the Parties have expressly agreed a different allocation of roles in writing in the Main Agreement. Salure processes Personal Data solely on behalf of the Customer and within the limits of the Main Agreement, these Data Processing Terms and the Customer's other documented instructions.

These Data Processing Terms become part of the Main Agreement when they are declared applicable in a quotation, order confirmation, agreement, order process, service terms or general terms and conditions of Salure. Acceptance of that Main Agreement also constitutes acceptance of these Data Processing Terms.

Salure makes these Data Processing Terms available electronically in a manner that allows the Customer to store them and consult them later. Salure retains each published version and can indicate, upon request, which version applies to a specific Main Agreement.

If no specific version is mentioned in the Main Agreement, the applicable version is the version published or otherwise made available to the Customer by Salure at the time the Main Agreement was formed.

2. Definitions

Term	Meaning
GDPR	Regulation (EU) 2016/679, the General Data Protection Regulation.
Data Subject	The identified or identifiable natural person to whom Personal Data relates.
Data Breach	A breach of security leading accidentally or unlawfully to the destruction, loss, alteration, unauthorised disclosure of or unauthorised access to Personal Data.
Main Agreement	The quotation, order confirmation, agreement, service level agreement or other arrangement between Salure and the Customer under which Salure provides services.
Customer	The party that purchases Salure's services and generally acts as Controller.
Personal Data	Any information relating to an identified or identifiable natural person that Salure processes in the context of the Main Agreement.
Sub-processor	Another processor engaged by Salure to carry out specific processing activities on behalf of the Customer.
Data Processing Terms	These data processing terms, including annexes, which together form the data processing agreement within the meaning of Article 28 GDPR once they have been declared applicable.
Processing	Any operation or set of operations performed on Personal Data, including collection, recording, organisation, structuring, storage, alteration, consultation, use, disclosure, erasure or destruction.

3. Subject matter, duration, nature and purpose of the processing

The subject matter of the Processing is the performance of the Main Agreement and Salure's related services, including payroll administration, activities in AFAS Profit, management and optimisation of administrative

processes, integrations, software development, continuity assurance, customer requests and compliance with applicable laws and regulations.

The duration of the Processing is equal to the duration of the Main Agreement, plus the period required for completion, transfer, deletion, statutory retention periods and normal backup or continuity processes as described in Article 10.

The nature and purpose of the Processing, the categories of Data Subjects and the categories of Personal Data are further described in Annex A. The specific scope is always determined by the services purchased by the Customer under the Main Agreement.

4. Instructions and responsibilities

Salure processes Personal Data solely on the basis of documented instructions from the Customer. Documented instructions include in any event the Main Agreement, these Data Processing Terms, the functional setup of the purchased services and any written or electronically recorded additional instructions from the Customer.

If Salure believes that an instruction conflicts with the GDPR or other applicable privacy legislation, Salure will inform the Customer as soon as possible. Salure is not obliged to carry out an instruction insofar as, in its reasonable opinion, doing so would be unlawful.

The Customer warrants that the Personal Data is lawfully provided to or made accessible to Salure, that there is a valid legal basis for the Processing and that the instructions to Salure comply with applicable laws and regulations.

Within the limits of the Customer's instructions, Salure determines the practical and technical manner in which it performs the agreed services. This includes choices regarding tooling, configuration, security, planning, quality control and continuity measures, provided those choices do not lead to a different purpose of Processing.

5. Security

Salure implements appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

When determining the level of security, Salure takes into account the state of the art, implementation costs, the nature, scope, context and purposes of the Processing and the risks to the rights and freedoms of Data Subjects.

Salure structures its measures in accordance with the principles of ISO 27001. The main categories of measures are included in Annex C. Salure may amend or replace measures, provided that the overall level of protection is not materially reduced.

6. Confidentiality and access

Salure ensures that persons who have access to Personal Data under its responsibility are bound by confidentiality or are subject to an appropriate statutory duty of confidentiality.

Access to Personal Data is limited to persons who reasonably need such access for the performance of the Main Agreement, management, security, support, quality control or compliance with legal obligations.

Salure limits access to customer environments to the practical minimum necessary and uses appropriate authorisation and control measures.

This duty of confidentiality does not apply insofar as the Customer has given express permission to provide the information to third parties, if providing the information to third parties is logically necessary given the nature of the assignment provided and the performance of the Data Processing Terms, or if there is a legal obligation to provide the information.

7. Sub-processors

The Customer grants Salure general written permission to engage Sub-processors for the performance of the Main Agreement. The Sub-processors known at publication are listed in Annex B.

Salure imposes written obligations on Sub-processors that, insofar as appropriate to the nature of their services, provide as much as possible the same level of protection as these Data Processing Terms.

Salure informs the Customer of any intended addition or replacement of Sub-processors via the publication page, email, customer portal or another appropriate electronic notification. The Customer may object on reasonable privacy or security grounds within fourteen (14) days after notification.

If the Parties cannot resolve an objection within a reasonable period, Salure may choose not to use the relevant Sub-processor for the Customer, to offer a reasonable alternative or, if the Sub-processor is necessary for the service, to terminate the relevant part of the Main Agreement subject to a reasonable transition period.

Salure remains responsible towards the Customer for compliance with the obligations of engaged Sub-processors, insofar as those Sub-processors process Personal Data on behalf of the Customer.

8. Transfers outside the EEA

Salure processes Personal Data in principle within the European Economic Area. If Processing takes place outside the EEA or access from outside the EEA is possible, Salure ensures a valid transfer basis and appropriate safeguards in accordance with the GDPR.

Appropriate safeguards may include an adequacy decision, standard contractual clauses adopted by the European Commission, additional technical and organisational measures or another transfer mechanism permitted by the GDPR.

9. Assistance to the Customer

Taking into account the nature of the Processing and the information available, Salure provides reasonable assistance to the Customer in complying with its obligations under the GDPR.

That assistance relates in any event to requests from Data Subjects, security of Processing, Data Breaches, data protection impact assessments (DPIAs), prior consultation with a supervisory authority and demonstrating compliance.

If a Data Subject contacts Salure directly with a request concerning Personal Data for which the Customer is the Controller, Salure refers the Data Subject to the Customer, unless the Parties agree in writing that Salure will handle the request on behalf of the Customer.

Insofar as the requested assistance goes beyond the standard services, Salure may charge its reasonable costs at the applicable rates, unless the assistance is necessary due to an attributable failure by Salure.

10. Data Breaches and security incidents

Salure has internal procedures for assessing, recording and following up security incidents.

Salure informs the Customer without undue delay and no later than thirty-six (36) hours after Salure becomes aware of a Data Breach that directly relates to Personal Data of the Customer, unless the data breach is unlikely to result in risks to the rights and freedoms of natural persons.

The notification contains, insofar as known at that time, the nature of the Data Breach, the likely categories and numbers of Data Subjects and Personal Data, the likely consequences, measures already taken or proposed and a contact point for follow-up.

The Customer remains responsible for assessing whether notification to the Dutch Data Protection Authority or Data Subjects is required, unless applicable law directly imposes a separate notification obligation on Salure.

11. Retention periods, return and deletion

Salure does not retain Personal Data longer than necessary for the performance of the Main Agreement, compliance with legal obligations, evidentiary purposes, security, continuity or completion of the services.

After the end of the Main Agreement, Salure deletes or returns, at the Customer's choice, the Personal Data it processes as Processor, unless Union law or Member State law requires Salure to retain it or further storage is temporarily necessary in backups, logs or continuity facilities.

If the Customer does not communicate a choice, Salure may delete or anonymise the Personal Data after a reasonable transition period. Salure retains data still required for operational or legal purposes for a maximum of one (1) year after the end of the Main Agreement, unless a longer statutory retention period applies.

The Customer acknowledges that it is fully responsible for the retention obligation for the data in its own systems. After transfer and deletion by Salure, any obligation of Salure relating to the retention obligation lapses.

Salure may deviate from the above insofar as a statutory retention period applies to Personal Data, on the basis of a legal ground or insofar as this is necessary to prove to the Customer that Salure has fulfilled its obligations.

Backups are not actively used for regular Processing and are overwritten or deleted in accordance with the normal backup cycle. These Data Processing Terms continue to apply in the event of restoration from backup.

12. Audit, information and DPIA

Salure makes available upon request all information reasonably necessary to demonstrate that it complies with its obligations as Processor, insofar as that information is available and disclosure does not harm the security, confidentiality or rights of other customers.

Salure may provide information in the form of certificates, audit reports, summaries, policy documents, completed questionnaires or other appropriate documentation.

If the available documentation is reasonably insufficient, the Customer may have an audit carried out by an independent third party bound by confidentiality. The audit must be limited to the Processing for the Customer and may not unreasonably disrupt Salure's business operations, security and confidentiality or those of other customers.

The Customer announces an audit in writing at least two (2) months in advance, stating the purpose, scope, method, auditor and desired planning. Unless there is a specific Data Breach or compelling reason, an audit will not take place more than once every twelve (12) months.

The costs of an audit and Salure's reasonable effort are borne by the Customer, unless the audit reveals a material shortcoming by Salure.

The findings following the audit carried out will, insofar as reasonable and fair, be implemented by Salure within a reasonable period, provided that the findings have been agreed in proper consultation with Salure and, where applicable, Salure's external auditor. Salure bears only the costs of implementing findings that necessarily must be implemented.

When the Customer submits a request for information to Salure for the purpose of a DPIA, Salure provides reasonable cooperation and, taking into account the nature of the Processing, provides the information the Customer reasonably needs to carry out the DPIA. The provision of existing standard documentation and a reasonable explanation thereof are included in the services. Salure may charge reasonable costs for additional customer-specific work. This does not apply insofar as the assistance is necessary as a result of an attributable failure by Salure.

13. Liability and indemnity

The liability arrangement in the applicable General Terms and Conditions of Salure or the Main Agreement applies to these Data Processing Terms.

Insofar as mandatory law, the GDPR or a supervisory authority provides otherwise, this does not affect the statutory liability of the Parties. As between the Parties, Salure is not liable for damage, fines or claims insofar as these arise from unlawful instructions, insufficient legal basis, incorrect data, acts or omissions of the Customer or Processing outside the agreed scope.

The Customer indemnifies Salure against claims from third parties, including Data Subjects and supervisory authorities, insofar as those claims arise from a failure by the Customer to comply with these Data Processing Terms, the Main Agreement or applicable privacy legislation.

14. Order of precedence

In the event of a conflict between these Data Processing Terms and the Main Agreement, the following order of precedence applies to matters that specifically concern the Processing of Personal Data: first, written and expressly agreed deviating privacy provisions in the Main Agreement, then these Data Processing Terms, then the General Terms and Conditions of Salure.

The Customer's general terms and conditions or other standard terms do not apply to the Processing, unless Salure has expressly accepted those terms in writing.

15. Amendments

Salure may amend these Data Processing Terms if this is necessary or desirable due to changes in laws and regulations, case law, guidance from supervisory authorities, changes in services, security measures, Sub-processors, technical setup or business processes.

Amendments do not materially reduce the overall level of protection for Personal Data. Material amendments are announced in advance via the publication page, email, customer portal or another appropriate electronic notification.

The Customer may object to a material amendment on reasonable privacy or security grounds within fourteen (14) days after announcement. The Parties will then consult with each other. If no reasonable solution is reached and the amendment is necessary for the services, either Party may terminate the relevant part of the Main Agreement subject to a reasonable transition period.

Non-material amendments, such as clarifications, contact details, formatting, hyperlinks or updates to the Sub-processor Register without material consequences for the Processing, may be implemented immediately.

16. Term and termination

These Data Processing Terms apply from the moment they have become part of the Main Agreement and remain in force for as long as Salure processes Personal Data on behalf of the Customer.

Termination of the Main Agreement results in termination of these Data Processing Terms, insofar as Salure no longer processes Personal Data on behalf of the Customer afterwards. Provisions that by their nature must continue, including confidentiality, security, audit, return, deletion, liability and dispute resolution, remain in force for as long as necessary.

17. Governing law and disputes

These Data Processing Terms and their performance are governed by Dutch law.

Disputes relating to these Data Processing Terms will be submitted to the competent court of the place of establishment of Salure, unless mandatory law designates another court.

If a provision of these Data Processing Terms proves invalid or is set aside by a court, this does not affect the other provisions of these Data Processing Terms. The Parties will then consult with each other to agree a new provision that is as close as possible in substance to the original provision.

Annex A. Description of the processing

Component	Description
Subject matter	Performance of the Main Agreement and the Salure services agreed therein.
Duration	During the term of the Main Agreement and thereafter insofar as necessary for transfer, deletion, statutory retention periods, evidentiary purposes, security, backups and continuity.
Nature of the processing	Collecting, receiving, recording, organising, structuring, storing, consulting, altering, using, checking, analysing, transmitting insofar as necessary, backing up, shielding, deleting and anonymising.
Purposes	• Providing the following service(s), the scope of which is indicated in the quotation(s), by Salure: • Payroll administration; • Implementing changes in AFAS Profit; • Managing and optimising administrative processes in AFAS Profit; • Developing and maintaining interfaces between systems; • Performing the activities agreed in the Main Agreement(s) and related activities; • Developing and further developing software in connection with the proper performance of the Main Agreement(s) and Salure's services; • Safeguarding the continuity and proper functioning of the services in accordance with the agreements in the Main Agreement(s), including maintenance, making backups and implementing improvements; • Handling specific customer requests; • The performance or application of laws and regulations.
Categories of Data Subjects	Employees, former employees, applicants, temporary workers, directors, contact persons, users, supplier contacts and other persons whose Personal Data the Customer provides to or makes accessible to Salure in the context of the Main Agreement.
Categories of Personal Data	See the further list below. The actual categories depend on the purchased services and the data that the Customer provides or makes accessible.
Special or sensitive data	Insofar as necessary for the services, data may be processed such as BSN, identity document, data relating to sickness/leave, trade union membership, wage garnishment, certificate of conduct (VOG) or comparable data. The Customer remains responsible for the lawfulness and necessity of providing such data.
Categories of recipients	Authorised employees of Salure, engaged Sub-processors and third parties insofar as the Customer instructs this or legislation requires it.

Employee data may include, among other things:

- name and address details
- employment contracts
- payslips
- salary data and data on reimbursements, allowances, benefits and deductions
- job data
- identity document
- BSN
- email address and telephone number(s)

- bank account number
- place and date of birth
- gender
- pension data
- data on trade union membership insofar as relevant
- information about a company car
- VOG
- data on completed and planned training
- data on employment conditions
- data for calculating, recording and paying taxes
- data on leave, maternity and sickness
- data on wage garnishment
- other data that the Customer provides or makes available and that is necessary for the performance of the Main Agreement
- other data necessary for specific customer requests
- data necessary for the performance of laws and regulations

Customer and contact data may include, among other things:

- surname, first names, initials, title and gender
- telephone number, email address and similar communication data
- bank or giro account number insofar as necessary
- data of the Customer's contact persons
- data for processing orders, assignments or service requests
- data necessary for the performance of the agreement or assignment
- other data whose processing is required by law or regulation or is reasonably necessary for the services

Annex B. Sub-processor Register

The overview below shows the Sub-processors known for version 2026.1. A Sub-processor is used only insofar as relevant to the service(s) purchased by the Customer. Salure may publish a current register electronically. Insofar as Processing by a Sub-processor takes place outside the EEA or access from outside the EEA is possible, Salure states the relevant country or region and the applicable transfer basis in or with the current register.

Sub-processor	Payroll administration	Implementing changes in AFAS Profit	Management and optimisation of administrative processes in AFAS Profit	Developing and maintaining interfaces between systems
Microsoft 365 (Outlook, SharePoint, Teams, etc.)	X	X	X	X
B2IT				X
Leaseweb	X			X
Atlassian				X
Zoho helpdesk				X
Monday.com				X
Amazon Web Services				X
Qlik				X
OpenAI / Claude				X
HubSpot	X	X	X	X
Perspectief				X
Computest				X
DNV	X	X	X	X
Adapt Business Analytics B.V.				X
Nxtmed Support B.V.		X	X	
Worldofwork		X	X	
AKM sarl		X	X	
Vplan		X	X	
Interim employees operating as own employees via Delta Payroll B.V., HK Payroll Services B.V., MK Payroll Services, StijlHR, Expatteam, MaviQ Solutions, Payroll enzo and Link2Linker	X			

Annex C. Technical and organisational measures

Salure applies appropriate technical and organisational measures. The measures are periodically assessed and may be adjusted to technological, organisational or legal developments, provided that the level of protection is not materially reduced.

Measure category	Description
Access security	Purpose-based authorisations, periodic review of granted permissions and, where appropriate, strong authentication.
Physical security	Physical access security measures for office environments where Personal Data may be processed.
Encryption	Encryption of digital files containing Personal Data that are stored on data carriers or in appropriate Salure systems, insofar as appropriate to the nature of the storage and the risk.
Organisational security	Policies, procedures, allocation of roles, awareness and instructions for employees who process Personal Data.
Monitoring and logging	Sample-based checks of compliance with policies, logging and investigation of relevant events insofar as available and appropriate.
Backups and continuity	Making backups and implementing continuity measures to support the availability and recoverability of services.
Incident management	Internal procedure for detecting, assessing, escalating, recording and following up security incidents and Data Breaches.
Supplier management	Assessment and contractual safeguarding of relevant Sub-processors and suppliers involved in the Processing.
Development and management	Appropriate measures for the development, maintenance and modification of systems and interfaces, including segregation of responsibilities where appropriate.