pureservice

PURESERVICE SERVICE AGREEMENT

Table of contents

1 General Provisions

1.1 Definitions

“Service Agreement” or “Main Agreement” refers to this agreement.

“Pureservice” refers to Pureservice AS, org. no. NO 929 782 216.

“Customer” refers to the organization that has signed this agreement.

“Pureservice Support” refers to the team at Pureservice responsible for resolving the Customer’s issues and/or inquiries related to the Service.

“Incident” means any event resulting in a breach of agreed service levels.

“Service” refers to the Pureservice service and/or software as specified in the agreement.

“Service Level” describes the standards by which Pureservice measures the quality and reliability of the Service as outlined herein.

“Assignment” refers to any work Pureservice undertakes for the Customer.

“Scope of Work” describes a specific task, including the desired outcome, execution plan, and estimated scope.

“Credit” refers to a percentage of the monthly fee for the Service reimbursed to the Customer when the Service Level falls below contractual thresholds.

“Subscription” is an agreement whereby the Customer commits to pay for the Service over a defined period.

“Customer Data” includes all data uploaded to or stored in the Service during its use.

1.2 Validity of the Agreement

This Agreement governs the Customer's use of the Service and any related services. By accessing the Service, the Customer agrees to the terms herein. If the Customer does not accept these terms, the Service may not be used.

This Agreement remains in force for the duration of the Customer’s active Subscription. Additional conditions may be found in Pureservice’s Standard Terms and Conditions.

1.3 Amendments

This Agreement supersedes all previous service and license agreements. Any amendment or deviation from this Agreement shall be valid only if documented in writing with explicit reference to this Agreement. Pureservice reserves the right to amend its terms, effective from the next renewal date.

1.4 Payment Terms

The Customer agrees to pay for the Service in accordance with current pricing and Pureservice’s Standard Terms and Conditions. Pureservice may restrict or terminate access to the Service in case of non-payment.

1.5 Data Retrieval

During the term of the Agreement, the Customer may retrieve their own data from the system. Should Pureservice assist with this, the Customer will be charged according to applicable rates.

Upon expiry of the Agreement, access will be deactivated and all Customer Data deleted. Deleted data may not be recoverable.

1.6 Breach and Sanctions

In case of material breach by the Customer, Pureservice reserves the right to take immediate action, including pointing out deficiencies, removing content, or revoking access to the Service. Material breach includes but is not limited to any violation of the Customer's license restrictions. Upon termination, Pureservice may demand the return of all delivered material (e.g., software, documentation), and the deletion and uninstallation of all software.

Pureservice reserves the right to pursue any breach through civil and/or criminal legal proceedings.

1.7 Notification Register

Pureservice maintains a register of the Customer's designated contacts. These contacts will be notified of changes to the Agreement, breaches, and other relevant matters by email or other suitable means. The default contact is the person who signed the agreement. The Customer is responsible for updating this information via the Service or by notifying Pureservice Support.

Pureservice is not liable for any failure in the delivery of notices or messages to the Customer if the Customer has not provided updated contact information.

1.8 Confidentiality

All information exchanged between the parties in connection with the delivery and use of the Service is considered confidential. Both Pureservice and the Customer agree not to disclose any such information to third parties. This obligation remains in effect even after the termination of the Subscription.

This obligation does not apply to information that:

– Was publicly known at the time of disclosure,

– Was already known to the receiving party prior to disclosure.

The provision does not prevent the use of the Customer's name and/or logo as specified in section 1.11.

1.9 Governing Law

This Agreement and any disputes arising out of or in connection with it shall be governed by and interpreted in accordance with the laws of Norway.

1.10 Dispute Resolution

Any disagreement regarding the validity, content, or execution of the Agreement shall first be attempted resolved through negotiations. Failing this, either party may bring the matter before the ordinary courts. If agreed, disputes may be resolved by arbitration in accordance with the Norwegian Arbitration Act of 14 May 2004 No. 25. Confidentiality regarding arbitration proceedings and rulings must be agreed in writing at the time arbitration is chosen. Legal proceedings shall be held in the jurisdiction of Pureservice's registered office.

1.11 Marketing and References

The Customer grants Pureservice the right to use the Customer's name and logo in Pureservice's marketing solely for the purpose of identifying the Customer as a user of the service. Such use may occur in reference lists, customer cases, presentations, tenders/offers, websites, and social media. Press releases and quotes from the Customer's employees require prior written approval from the Customer. The Customer may at any time opt out in writing from further use; such reservation applies going forward.

This right applies during the agreement period and for up to 12 months after termination.

2 Use of the Service

2.1 Right of Use

The Customer is granted a non-exclusive and limited right to use the Service.

The right of use grants the Customer access to and use of the user licenses, modules, applications, integrations, APIs, and any other add-ons subscribed to by the Customer.

User licenses are based on concurrent use, where concurrent use is defined as activity within the solution during a single hour. If the Customer operates multiple instances of the Service, concurrent use is calculated per instance and then aggregated. Pureservice reserves the right to notify the Customer of any under-licensing.

Actively using a single license in two or more sessions constitutes a breach of this Agreement.

The Customer may not transfer, lease, lend, sublicense, or otherwise permit any third party to use the Service, license codes, or associated documentation without prior written consent from Pureservice.

The right of use terminates when the Subscription is no longer active.

2.2 Installation, copying, decompiling, etc.

If the Service is installed locally (on the Customer's or their hosting provider's servers), the license permits installation and use on a single server (physical or virtual). Necessary components (email integration, Active Directory, data listeners, service portal, etc.) are installed as needed.

Beyond what is required for legal use of the Service and documentation, the Customer may not reproduce software, documentation, or related material—either digitally or in print. Security copies are allowed to the extent necessary under applicable law.

The Customer is not permitted to decompile the software to obtain techniques used by Pureservice, nor to modify, edit, or create derivative works, including removing design templates or branding belonging to Pureservice.

2.3 Modifications to the Service

The Customer may not make changes to the Service unless explicitly agreed in writing with Pureservice. This includes modifications to custom workflows.

2.4 Third-Party Software

The Customer is responsible for acquiring and maintaining any third-party software licenses required (e.g., server OS, databases).

2.5 Customer Data

Customer Data remains the property and responsibility of the Customer. Data stored in the Service may be processed via storage, transfer, backup, and analysis to enhance protection and improve the Service.

Pureservice will take all necessary steps to ensure the consistency, integrity, and availability of Customer Data. Unless the Agreement is breached, data cannot be deleted from the Service without written consent from the Customer.

2.6 Privacy

As part of this Agreement, the Customer consents that Pureservice may access, generate, and store information related to the use of the Service, including data collected during use, to comply with laws and regulations.

Pureservice may extract statistics and usage patterns from anonymized data, which may be stored on Pureservice's servers, cloud infrastructure, or relevant web services. Pureservice is responsible for ensuring data security.

Pureservice must comply with lawful data retention and disclosure orders from legal authorities. Data may be disclosed in connection with formal investigations or legal proceedings.

See Chapter 8 – Data Processing Agreement and Pureservice's Privacy Policy: https://pureservice.com/trust/

2.7 Limitation of Liability

The total liability Pureservice may incur under this Agreement is limited to the amount paid by the Customer during the last 12 months prior to the event giving rise to the claim.

Pureservice is not liable for indirect losses, including but not limited to, loss of profit, lost savings, or third-party claims, as well as any other losses deemed indirect under Norwegian law.

This limitation does not apply in cases of gross negligence or willful misconduct by Pureservice.

Any other compensation shall be deducted from the total amount recoverable for the same issue.

2.8 Intellectual Property Rights

Pureservice retains full ownership, copyright, patents, design rights, and all other current and future rights to all forms of software, integrations, applications, databases, documentation, and similar. Pureservice owns all rights to any suggestions from the Customer regarding modifications or new features to Pureservice products and services. Such rights are granted to Pureservice without compensation, unless otherwise agreed in writing.

2.9 Assignment

Pureservice reserves the right to transfer its rights and obligations under this Agreement to a third party.

The data controller must be notified no later than 90 days in advance so the Agreement may be terminated per the applicable terms.

3 Service Description

3.1 Introduction

Pureservice provides a Service Management solution accessible via web browser or mobile application. The service adheres to best practices in process support, business functionality, security, and quality delivery.

3.2 Service Design

The Service is available in two deployment models:

– As a cloud service (SaaS – Software-as-a-Service), hosted in local data centers, on dedicated or shared servers with full data isolation

– Installed on the Customer’s own servers

The Service can authenticate against the Customer's directory services (e.g., Active Directory, CRM systems) for simplified access and user management.

Pureservice uses a subcontractor for hosting the cloud service, for which Pureservice remains fully responsible. The service is delivered in accordance with the SLA agreement ensuring optimal performance and availability.

3.3 Updates

Pureservice will automatically verify the customer's service version and perform system maintenance and updates. Major updates will be communicated in advance; minor updates may be implemented without notice. Pureservice cannot guarantee that updates to the service support the current systems on which the solution was originally implemented and integrated.

3.4 Pureservice Continuous Delivery

Pureservice Continuous Delivery ensures the Service runs on the latest version. URL access to https://*.pureservice.com is required from the application server.

3.5 Pureservice OnPremise Infrastructure

When installed on the Customer’s own servers, infrastructure includes:

– Application server

– Database server (data and configuration storage)

– Email server (for case registration and follow-up)

3.6 Third-Party Hosted Installation

Dedicated instances of the application server and database server may be implemented in a third-party operations center and operated and maintained in accordance with agreements between the Customer and the third party.

All costs related to third-party operational services shall be borne solely by the Customer. Any additional costs related to setup, configuration, administration, and similar activities shall also be the sole responsibility of the Customer.

3.7 Customer Responsibilities – Cloud Service

– Configure configurable data like users, groups, permissions, categories, workflows, zones
– Ensure user internet and network access
– Ensure local services (e.g., AD sync, email) are operational and available for the Service
– Install and maintain client software as needed

3.8 Customer Responsibilities – On-Premise Installation

Same as above, plus:

– Provide internet access (DMZ or equivalent) for mobile/self-service
– Install updates from Pureservice
– Perform data backups

3.9 Pureservice Responsibilities – Cloud Service

– Perform backups
– Manage software updates

3.10 Security

Pureservice follows OWASP top 10 security practices. The SaaS service is hosted in Microsoft Azure (SOC 2 Type 2, ISO 27001:2022 certified). Visit the Microsoft Trust Center for more details.

3.11 Encrypted Customer Data

Data is encrypted in transit and at rest, including sensitive credentials used for email integration.

3.12 Self-Service Configuration

The Service provides a web interface for self-management of key configuration elements.

3.13 Access for Users and Applications

Accessible via web browsers, mobile app, or APIs. Supported browsers are listed on www.pureservice.com. Latest browser versions are recommended.

3.14 Disaster Recovery – Cloud Service

The service operates in high-availability data centers and follows procedures to minimize downtime.

3.15 Switching Between Cloud and On-Premise

Customers may migrate between cloud and on-premise models. Service fees apply. Contact Pureservice for details.

4 Service Level Agreement (SLA) – Pureservice Cloud Service

4.1 Acceptable Use

The Customer must comply with configuration requirements, use supported platforms, and adhere to the Service Description to qualify for SLA coverage.

To ensure stable performance for all customers, a limit of 100 API calls per minute per customer applies. Exceeding this limit may result in temporary blocking of further API requests.

4.2 SLA Exclusions

This SLA does not apply to performance or availability issues caused by:

– Services installed on Customer's or third-party servers

– Factors beyond Pureservice's control

– Customer's or third-party actions or inactions

– Non-compliance with Pureservice's configuration guidance

– Planned maintenance

– Beta testing or trial periods

– Test environments

4.3 Service Credit

Service credits are the sole financial remedy for SLA violations. Monthly credits are capped at the monthly service fee and do not apply to one-time delivery fees.

Credits require prompt notification to Pureservice Support upon downtime. Claims must be submitted in writing within four weeks.

4.4 Uptime Measurement

"Downtime" means total unavailability preventing all user logins and use, excluding planned maintenance.

"Planned downtime" is agreed maintenance or major upgrades.

"Total time" is the total time in a calendar month.

$$Monthly\ uptime\% = \frac{Total\ time\ -\ Downtime}{Total\ time}$$

4.5 Guaranteed Uptime and Credits

Monthly uptime-%	Service Credit
< 99.5%	25%
< 99%	50%
< 95%	100%

5 Customer Success

The Agreement includes support for implementation and onboarding, as well as ongoing follow-up during production use.

5.1 Implementation and Onboarding Support

The goal is to prepare the Service for use and equip the Customer for effective adoption. Pureservice will inform the Customer about the distribution of responsibility and participation at the start of establishment and onboarding. Activities typically include:

- Preparation
- Technical setup
- Training
- Kick-off
- Configuration
- Health check
- Go-live
- Evaluation

5.2 Ongoing follow-up

Once live, Customer Success offers guidance and advisory through:

- Dedicated Customer Success Manager (CSM)
- Follow-up plan
- Scheduling with CSM
- Usage discussions, tips, best practices, and experience sharing
- Service-related articles and guides

Note: Configuration assistance, custom integrations, or workflow setup are not included.

6 Pureservice Support

The Agreement allows Customer to contact Pureservice Support for questions or incidents regarding the implemented solution, including product, database, infrastructure, and integrations.

Support is provided for the current and previous minor version.

Errors caused by the Customer may incur charges.

Support Hours: Weekdays 08:00–16:00 (excluding holidays)

Pureservice Support Tlf +47 22 12 00 26

support@pureservice.com

https://support.pureservice.com/

Included Support Services

Phone and email support for product-related inquiries	■
Web portal for case tracking servicedesk.pureservice.com	■
Support in Norwegian	■
Response time from case registration	2 hours
Designated contacts	3
Contacts must complete free user training: https://www.pureservice.com/kurs/	■

7 Consulting Assignments

7.1 Obligations

The Customer must provide all necessary information for Pureservice to fulfill the assignment as per the Scope of Work. The Customer shall ensure access to systems and applications required for execution.

Pureservice shall likewise gather all necessary information for delivering the assignment. Any delays or potential delays must be reported to the Customer without undue delay.

Pureservice must conduct a functional test according to the Assignment description before finalization.

7.2 Changes

The Customer may issue written change orders to adjust the scope or timeline of the assignment. This is permitted provided the change is within what was reasonably foreseeable at the time of agreement.

Pureservice must promptly inform the Customer of any impact on pricing, timelines, or other relevant conditions.

Additional time caused by unforeseen issues in the Customer's environment, or delays caused by the Customer, will be billed at standard consulting rates.

Cancellations/rescheduling:

– 7 days prior: 50% charge

– 3 days prior: 100% charge

Assignments involving integrations apply only to current versions. Work related to new versions is billable under standard rates.

Any corrections due to deficiencies in Pureservice's delivery shall be performed free of charge, provided the Customer reports the issue within a reasonable time, and no later than 3 months after occurrence.

7.3 Acceptance

The Customer shall confirm acceptance within two weeks of Pureservice's completion notice. If no response is received, the assignment shall be deemed accepted.

8 Data Processing Agreement

Standard Contractual Clauses
For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Between

Customer, as specified in the Main Agreement, see below, hereinafter referred to as 'the Data Controller

and

Pureservice

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

8.1 Preamble

8.1.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

8.1.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

8.1.3 In the context of the provision of the agreement between the data controller and the data processor regarding delivery (the main agreement) to which these terms and conditions are attached, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

8.1.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

8.1.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.

8.1.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

8.1.7 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8.1.8 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

8.1.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

8.1.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

8.1.11 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

8.2 The rights and obligations of the data controller

8.2.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

8.2.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

8.2.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

8.3 The data processor acts according to instructions

8.3.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

8.3.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

8.4 Confidentiality

8.4.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

8.4.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

8.5 Security of processing

8.5.1 Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.5.2 According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

8.5.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

8.6 Use of sub-processors

8.6.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

8.6.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

8.6.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least four weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

8.6.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

8.6.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

8.6.6 The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

8.6.7 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8.7 Transfer of data to third countries or international organisations

8.7.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

8.7.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.7.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

a. transfer personal data to a data controller or a data processor in a third country or in an international organization

b. transfer the processing of personal data to a sub-processor in a third country

c. have the personal data processed in by the data processor in a third country

8.7.4 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.7.5 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8.8 Assistance to the data controller

8.8.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject

b. the right to be informed when personal data have not been obtained from the data subject

c. the right of access by the data subject

d. the right to rectification

e. the right to erasure ('the right to be forgotten')

f. the right to restriction of processing

g. notification obligation regarding rectification or erasure of personal data or restriction of processing

h. the right to data portability

i. the right to object

j. the right not to be subject to a decision based solely on automated processing, including profiling

8.8.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, i Norge (Datatilsynet), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, i Norge (Datatilsynet), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

8.8.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

8.9 Notification of personal data breach

8.9.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

8.9.2 The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

8.9.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.9.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

8.10 Erasure and return of data

8.10.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or to return all the personal data to the data controller and delete existing copies, by choice of the data controller, unless Union or Member State law requires storage of the personal data.

8.11 Audit and inspection

8.11.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

8.11.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

8.11.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

8.12 The parties' agreement on other terms

8.12.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

8.13 Commencement and termination

8.13.1 The Clauses shall become effective on the date of both parties' signature.

8.13.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

8.13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

8.13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

8.13.5 These terms are entered into as part of the Main Agreement between the Data Controller and the Data Processor.

8.14 Data controller and data processor contacts/contact points

8.14.1 The parties may contact each other using the following contacts/contact points:

8.14.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

8.14.3 The same contact persons as may be designated in the Main Agreement between the Data Controller and the Data Processor shall apply

8.15 Appendix A: Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the processing is to fulfill the agreement entered into between the data controller (customer) and the data processor (supplier), see the Main Agreement for more details.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Storage and necessary processing as part of the services under the Main Agreement. The Main Agreement provides that the Data Controller shall use the Data Processor's software for digital registration, storage and follow-up of inquiries from the Data Controller's employees ("tickets").

The Data Processor shall make a dedicated instance of the service provided under the Main Agreement available to the Data Controller and shall perform necessary maintenance of the system.

The system shall be used to store the Data Controller's information related to registration and follow-up of tickets related to its own employees, customers and their employees/contact persons, as well as other relevant contacts.

A.3. The processing includes the following types of personal data about data subjects:

Name, email address and telephone number of users as well as other information and data that the controller enters into the system that is delivered under the Main Agreement as a result of the use of the system.

A.4. Processing includes the following categories of data subject:

Employees of the data controller, customers of the data controller, contact persons of customers and suppliers of the data controller, as well as others to whom the customer gives access to the system, as well as other persons covered by information that the customer enters into the system.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Upon termination of the Main Agreement and this Data Processing Agreement, the Data Processor shall return all personal data received on behalf of the Data Controller and covered by this Agreement. Such return may be made in the form of a printout and/or copy of customer data in databases covered. The costs of this shall be borne by the Data Processor.

Unless the Data Controller so requests, the Data Processor shall delete all data containing information covered by the Data Processing Agreement. This also applies to any backup copies. The Data Processor shall document in writing that deletion has been carried out within a reasonable time after termination of the Agreement. The above applies provided that there is no statutory obligation to retain the data. Deletion will then take place as soon as this obligation no longer exists.

8.16 Appendix B: Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

Name	Country of processing	Description of processing
Microsoft Norge AS (Azure), see: https://www.microsoft.com/en-us/trustcenter/	Norway	Host to offer the software in the cloud (by Pureservice SaaS)
Mailgun, owned by Sinch AB in Sweden	EØS	Receive and deliver e-mail. Only for customers who do not have their own e-mail server.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. For changes to sub-processors, see section 8.6 of the terms.

8.17 Appendix C: Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

See section A.2 above.

The data processor shall also comply with the obligations imposed on the data processor as such under the data protection regulations, including the General Data Protection Regulation and other relevant legislation.

The data processor's personnel will not have access to customer data during normal operations, nor do they need to. When troubleshooting the service or in connection with troubleshooting for the data controller, the dev-ops team has access to customer data stored in the service. All members of the dev-ops team have received extensive training in security and privacy.

The data processor may extract statistics and metadata about the tickets, for example the number of tickets and activated modules, usage patterns, etc. Such statistics shall be anonymized prior to transfer to the data processor's servers and shall not contain personal data. Such statistics and usage patterns may be stored either on the data processor's servers, servers that the data processor has at its disposal in a cloud service or in relevant online services. It is the data processor's responsibility to ensure satisfactory security around this data.

As with all cloud service providers, the data processor will have to comply with orders from public authorities, prosecutors, etc. for storing data in data centers. The data processor will be obliged to comply with orders for making information or customer data available in connection with formal investigations or lawsuits.

The Data Processor may use service data to optimize the solution and develop new services. Service data may, for example, be whether a limited function in the solution (Change and/or SLA) is activated or not and does not include personal data or sensitive information.

C.2. Security of processing

The level of security shall take into account:

The data processor shall ensure that appropriate technical and organizational measures are implemented to secure personal data processed pursuant to the agreement, taking into account what is technically feasible, the costs of securing it, and the processing of personal data to be carried out and the risk of such processing related to the privacy of those to whom the personal data relate. Including, depending on what is necessary and appropriate for the security:

Organizational measures

- An internal management system for information security has been established that has been approved by management and is known and implemented in the organization, with training, regular checks to reveal whether the routines are being followed, and regular auditing (GDPR art. 32).
- Pureservice is hosted in a data center that is SOC 2 Type 2 Compliant and ISO 27001:2022 certified according to ISO 27002 best practices.
- Pureservice employees are required to follow a set of safety instructions and only employees with official needs have access to the production platform.

- The development team works according to the SCRUM method and uses the GIT version control system. Changes are tested in separate environments before being approved for release to the production environment. This is made possible by using separate update channels (dev, main, preview and release) in our release routines and an update is not published until the integrity of the package has been verified and tested. These steps also include manual approval routines. There are automated tests at the forefront of all channels. Before an update is approved, it goes through a quality check in a separate QA process.
- The Pureservice DevOps team regularly updates the infrastructure as needed. Changes that particularly affect customers are announced in the news function in the application. Maintenance and updates at lower infrastructure levels, e.g. OS updates, bug fixes for infrastructure components, are performed automatically and regularly by Microsoft.
- Changes are planned and executed by the DevOps team. The team tests changes in a suitable environment before any changes are transferred to production. All planned changes undergo a risk assessment in advance.
- Pureservice runs a CSIRT (Computer Security Incident Response Team) to follow up on all security incidents. The team investigates the type of incident and takes necessary measures to correct them. This also includes notifying the customer's main contact if customer data may have been affected, or filing a case with the national Data Protection Authority if possible violations of the General Data Protection Regulation have been discovered.
- Pureservice has several sources that can lead to the registration of deviations. Examples of this are monitoring/alarms, manual analysis of event logs or customer-reported deviations via our service desk. All deviations are registered and further processed by DevOps or CSIRT team.
- Emergency response is covered by a 24/7 standby plan and CSIRT.
- Alerts regarding vulnerabilities that are of interest to all customers are published in the application. If a vulnerability has been reported by a customer, it is first notified through version history when the vulnerability has been resolved.
- Pureservice conducts annual penetration and security testing with an external vendor. The tests are based on the OWASP top 10.
- The data controller or their representative may conduct penetration tests on their own Pureservice cloud instance up to once per year. This must be approved in advance by contacting Pureservice support.

Technical measures

- All data is stored in a minimum of two physically separate database instances to ensure availability. Multitenant architecture with separate databases per customer instance.
- All databases are encrypted at rest. Data is encrypted during transport between user device and Pureservice in the cloud
- Continuous monitoring of performance and availability is carried out.
- Pureservice is operated and developed by personnel with knowledge and experience in security work.
- Pureservice develops, tests and verifies Pureservice based on the guidelines in the OWASP top 10. External security audits are performed with penetration testing at the network and application level.
- User authentication and access control per instance.

- Continuous updating of the code ensures that all customers are up to date with functionality and security features at all times.
- Backup of all data continuously within the last 30 days.
- The service is delivered on the Microsoft Azure platform, which is robustly designed to maintain availability at all times. The service is continuously monitored with necessary notification routines to maintain an acceptable service level as described in the service agreement. Security on the cloud platform (Azure) is handled by Microsoft, see more about the measures here: https://www.microsoft.com/en-us/trustcenter/.
- Pureservice supports Single Sign-On for integration with the customers existing Identity Provider through OpenID Connect, SAML. OAuth 2.0, WS-Federation and more. For example, if the customer uses Entra ID as an identity provider "IdP", MFA, whitelisting, access rule sets and advanced access control will be managed from Entra ID.
- Pureservice supports multi-factor authentication through integration with the company's existing Identity Provider.
- Pureservice is regularly updated with code that adds new functionality or addresses known bugs. Upgrading Pureservice in the cloud is announced in the news function in Pureservice and occurs automatically at the notified time.
- The development team undergoes training in secure development in connection with penetration and security testing every year and is otherwise continuously updated on threats defined in, for example, the OWASP top 10 list.
- Pureservice uses functionality in Microsoft Azure Security Center for continuous security monitoring of Pureservice in the cloud.

Further information on the organization of security work and measures is described in our CAIQ – see https://pureservice.com/trust

In addition to the above, the data processor regularly conducts security audits for systems and the like that are covered by this agreement. The audit may include a review of routines, random checks, more extensive on-site inspections and other appropriate control measures.

The data controller may require a review and audit of the service, systems and documentation to ensure that it is legal, and the data processor shall enable and contribute to such audits. Each party shall cover its own costs of audits. If the data controller uses an external auditor, the data controller shall cover the costs of this.

The data processor nevertheless has the right and obligation to make decisions about which technical and organizational security measures shall be implemented to establish the necessary (and agreed) level of security.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Assistance to the controller by the data processor shall comply with the duty of assistance imposed by the General Data Protection Regulation.

If the data processor becomes aware of unlawful access to the data controller's data stored by the data processor or the data processor's subcontractors, the data processor shall without undue delay 1) inform about the type of data breach and affected data subjects, 2) investigate the security breach and provide the controller with detailed information about the security breach, 3) implement and inform about responsible and reasonable measures to remedy the impact of the security breach and limit the damage.

Notification of suspected security breaches can be sent to: personvern@pureservice.com, which will then handle the case for the data processor. Such notification does not change the data controller's obligation to report deviations/data protection breaches to the Data Protection Authority and, if applicable, to the data subjects.

Assistance from the data processor to the data controller beyond what follows from this agreement and which are obligations incumbent on the data processor under the data protection regulations, will have to be carried out according to the data processor's current hourly rates as assistance.

This applies to tasks such as deleting personal data outside of what is done automatically or the controller can do through the solution, providing access to personal data beyond what can be done through the solution, assisting the controller with risk assessments and documentation, etc.

C.4. Storage period/erasure procedures

See section A.5 above

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorisation:

The processing shall only take place within the EEA.

The location for sub-processors' processing of personal data follows from the table under section B1.

C.6. Instruction on the transfer of personal data to third countries

The data processor may only transfer personal data to a third country if the data controller has given written consent to such transfer, and there is a lawful basis for the transfer.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller’s audits, including inspections, of the processing of personal data being performed by the data processor

None beyond what is regulated in the General Data Protection Regulation (GDPR) Article 28.

8.18 Appendix D: The parties' terms of agreement on other subjects

The following changes shall be made to the Terms:

Section 8.6.6 shall be deleted.

In section 8.8.2a, "where feasible, not later than 72 hours" shall be deleted.

In section 8.9.2, "if possible within 24 hours" shall be replaced with "without undue delay".

Requirements related to data processing are covered by the same liability regulations and liability limitations as follows from the Main Agreement.

Pureservice notes that if the Customer provides its own customers or partners with access to the solution, this is done under the Customer's full responsibility as data controller. Separate regulations must be established if such third parties exercise independent data processing responsibility.

Change log

Date	Version	Change	Effective from
	2.9	New section 1.11 Added right to use the customer’s name and logo in marketing Changed: 1.8 Clarified with regard to section 1.11	
1.8.2025	2.8	First english version	1.8.2025

For previous changes, please contact Pureservice.