T1A /S - Privacy Policy

Last updated 02.02.2026

Protecting your data is something we take seriously. In our daily operations of our company, we treat personal data and have therefore adopted this privacy policy that tells you how we treat your data.

Tier1 Asset A/S, Hejrevang 18, DK-3450 Allerød, Comp.Reg.No. DK-26031486 are data administrators for the information we collect about you and we ensure that your personal information is processed in accordance with the law.

If you would like to contact us regarding our processing of personal information, you can do it at marketing@tier1asset.com or mlp@tier1asset.com.

Processing of personal data

Personal information is any kind of information that may be attributed to you to some extent. When using our website, we collect and process a variety of such information. This happens for example by common access content if you sign up for our newsletter, participate in competitions or surveys, register yourself as a user or subscriber, otherwise use of services or make purchases through the website.

We typically collect and process the following types of information: A unique ID and technical information about your computer, tablet or mobile phone, your IP number, geographic location, and which pages you click (interests).

Normally, in our daily work, we will collect the personal data you provide in connection with Customer- or Supplier Application.

To the extent that you give explicit consent, we may process other personal data. This will typically be associated with the creation of login, purchase, sign-up for an online service or newsletter.

Security

We have taken appropriate technical and organizational measures against the fact that your information is accidentally or illegally deleted, published, lost, impaired or comes to the knowledge of a person, misused or otherwise treated in violation of the law.

Purpose

The information is used to identify you as a user and show you the ads that are most likely to be relevant to you, to register your purchases and payments, and to provide the services you have requested, such as. to send a newsletter.

In addition, we use the information to optimize our services and content.

Marketing and promotional communications

You agree to be contacted for the purpose of arranging a collection of your used IT equipment, as well as to receive marketing and promotional communications from T1A A/S, including insights, services, and offers related to IT asset recovery and IT lifecycle management.

You can withdraw your consent at any time by contacting marketing@tier1asset.com

Data minimization

We collect, process and store only the personal data needed to meet our intended purpose. Additionally, it may be decided by law what type of data is required to collect and store for our business operations. The

type and extent of the personal data we process may also be required to fulfill a contract or other legal obligation.

Data is kept up to date

As our service is dependent on your data being accurate and up to date, please inform us about relevant changes to your data. You can use the contact details above to notify us of your changes, so make sure to update your personal data.

If we become aware that data is incorrect, we update the information and notify you.

Period of storage

The information is kept for the time allowed by law and we delete them when they are no longer necessary. The period depends on the nature of the information and the background for storage.

Therefore, it is not possible to specify a general timeframe for when information is deleted.

Consent

Your consent for receiving, for example, Newsletter is optional, and you can withdraw it at any time by contacting us. Use the contact information above for more information.

Disclosure of information

Disclosure of personal information such as name and e-mail, etc. will only happen if you consent to it.

Your rights

You are entitled at any time to know what data we treat about you, where they originate and what we apply them to.

You can also find out how long we keep your personal data and who receives data about you, to the extent that we pass data in Denmark and abroad.

If you request, we can inform you about the data we process for you. Access may, however, be limited for the protection of other people's privacy, business secrets and intellectual property rights.

You can make use of your rights by contacting us. You can find our contact information at the top. If you believe that the personal data we treat about you is inaccurate, you are entitled to correct them. You must contact us and indicate what the inaccuracies are and how they can be corrected.

In some cases, we will have an obligation to delete your personal data. This applies, for example, if you withdraw any given consent. If you believe your data is no longer necessary for the purpose we obtained them, you may want to have them deleted. You can also contact us if you believe your personal data is being processed in violation of the law or other legal obligations.

You also have the opportunity to file a complaint with the Data Inspectorate – but we will also cooperate and make you feel safe about our processing of your personal data.

When you address a request to correct or delete your personal data, we will investigate whether the conditions are met and, in that case, make changes or deletions as soon as possible.

You are entitled to object to our processing of your personal data. You may also object to our disclosure of your data for marketing purposes. You can use the contact information at the top to send an objection. If your opposition is justified, we will stop processing your personal data.

You have the opportunity to avail yourself of data portability, in which case you wish your information moved to another data controller or data processor.

We will delete your personal data when they are no longer required for the purpose for which they are collected.

Terms & Conditions for Data Processing for T1A A/S – Online Acceptance

Table of Contents

1. Preamble

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.
2. The Clauses are designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR).
3. The lawful basis for the processing is the performance of a contract under Article 6(1)(b) GDPR. The data processor's operations are limited to physical handling and deletion of data storage

devices without viewing or extracting any data. This technical nature significantly mitigates risks to data subjects.

4. In providing IT equipment processing and data erasure services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
5. The Clauses take priority over any conflicting provisions in other agreements between the parties.
6. Four appendices form an integral part of the Clauses.
7. Appendix A describes the purpose and nature of the processing, types of personal data, categories of data subjects, and processing duration.
8. Appendix B sets out conditions for the processor's use of sub-processors and lists those authorised by the controller.
9. Appendix C provides the controller's instructions, required minimum security measures, and audit procedures for both processor and sub-processors.
10. Appendix D contains additional provisions not otherwise covered in the Clauses.
11. The Clauses and appendices must be retained in writing, including electronic form, by both parties.
12. The Clauses do not exempt the processor from obligations under GDPR or other applicable legislation.

2. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data complies with GDPR Article 24, applicable EU or Member State data protection laws, and these Clauses.
2. The data controller determines the purposes and means of processing.
3. The data controller is responsible for ensuring that all processing instructed to the data processor has a valid legal basis.

3. The data processor acts according to instructions

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. Such instructions are specified in Appendices A and C. Any updated instructions during the contract must be documented in writing, including electronically.
2. The data processor shall immediately inform the data controller if, in the processor's opinion, an instruction appears to violate GDPR or applicable data protection legislation.

3. The data processor does not access, view, extract, or otherwise interact with personal data contained on devices. Processing activities are strictly limited to secure, automated data erasure without human inspection of data content. Processing is limited to metadata such as device serial numbers required for traceability and certification of erasure.

4. Confidentiality

1. The data processor shall grant access to personal data only to persons under its authority who are subject to confidentiality obligations, either by contract or statutory requirement, and strictly on a need-to-know basis. Access shall be reviewed periodically. If access is no longer necessary, it shall be withdrawn immediately.
2. At the request of the data controller, the data processor shall demonstrate that all individuals under its authority who have access to personal data are subject to appropriate confidentiality obligations.

5. Security of processing

1. In accordance with Article 32 GDPR, and taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of processing—as well as risks of varying likelihood and severity to individuals—the data controller and data processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall assess risks to the rights and freedoms of natural persons and implement appropriate mitigation measures. Depending on relevance, these may include:

   - a. Pseudonymisation and encryption of personal data.
   - b. Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
   - c. The ability to restore access to personal data in a timely manner in the event of a physical or technical incident.
   - d. Regular testing, assessment, and evaluation of the effectiveness of technical and organisational measures.

2. The data processor shall independently evaluate risks to the rights and freedoms of individuals inherent in the processing and implement suitable mitigation measures. The data controller shall provide all information needed for such assessments.
3. The data processor shall assist the data controller in complying with the controller's obligations under Article 32 GDPR, including providing information about the processor's implemented measures and any additional measures required by the controller.

If the controller determines that further mitigation measures are needed, these will be specified in Appendix C.

6. Use of sub-processors

1. The data processor shall meet the requirements of GDPR Article 28(2) and 28(4) when engaging any sub-processor.
2. The data processor shall not engage a sub-processor without the prior general written authorisation of the data controller.
3. The data controller provides general authorisation for the use of sub-processors. The data processor shall notify the data controller of any intended additions or replacements of sub-processors, allowing fourteen (14) days for objection. Additional notice terms may be specified in Appendix B.
   The current list of authorised sub-processors is set out in Appendix B.
4. When a sub-processor performs processing activities on behalf of the data controller, the data processor shall ensure that the same data protection obligations as described in these Clauses are imposed on the sub-processor by contract or other legal act under EU or Member State law.
   The data processor shall ensure that the sub-processor provides sufficient guarantees for implementing appropriate technical and organisational measures.
5. Upon request, the data processor shall provide the data controller with a copy of the sub-processor agreement and any subsequent amendments, excluding business-related terms not affecting the legal data protection content.
6. The data processor shall agree a third-party beneficiary clause with sub-processors, ensuring that if the processor ceases to exist or becomes insolvent, the controller may instruct the sub-processor to erase or return the personal data.
7. If a sub-processor fails to fulfil its data protection obligations, the data processor remains fully liable to the data controller for the sub-processor's actions. This does not affect the rights of data subjects under GDPR Articles 79 and 82.

7. Transfer of data to third countries or international organisations

1. The data processor shall not transfer personal data to a third country or international organisation unless explicitly instructed by the data controller and only in accordance with Chapter V of the GDPR.
2. If the data processor is required by Union or Member State law to perform a transfer not instructed by the data controller, the processor shall inform the controller of this legal

requirement prior to processing, unless such information is prohibited for reasons of important public interest.

3. Without documented instructions from the controller, the processor may not:
    - a. transfer personal data to a controller or processor located in a third country or international organisation,
    - b. transfer personal data to a sub-processor located in a third country,
    - c. process personal data in a third country.
4. Any controller instructions regarding third-country transfers, including the applicable transfer tool under GDPR Chapter V, must be documented in Appendix C.6.
5. These Clauses are not to be confused with standard contractual clauses under GDPR Article 46(2)(c)–(d), and cannot serve as a transfer tool.

8. Assistance to the data controller

1. Taking into account the nature of processing, the data processor shall support the data controller in fulfilling obligations related to data subject rights under GDPR Chapter III. This includes assisting, to the extent possible, with:
    - the right to be informed (when data is collected from the data subject),
    - the right to be informed (when personal data has not been obtained from the data subject),
    - the right of access,
    - the right to rectification,
    - the right to erasure ("right to be forgotten"),
    - the right to restrict processing,
    - notification obligations regarding rectification or erasure of personal data or restriction of processing,
    - the right to data portability,
    - the right to object,
    - rights relating to automated decision-making, including profiling.
2. The data processor shall also assist the data controller in ensuring compliance with:
    - a. the obligation to notify personal data breaches to supervisory authorities without undue delay and, where feasible, within 72 hours,

- b. the obligation to communicate personal data breaches to affected data subjects when such breaches pose a high risk,
- c. data protection impact assessments (DPIAs),
- d. prior consultation of supervisory authorities where required.

3. The specific measures, scope, and extent of assistance provided by the data processor are described in Appendix C.

9. Notification of personal data breach

1. In the event of a personal data breach, the data processor shall notify the data controller without undue delay after becoming aware of the breach.
2. Notification must occur early enough to allow the controller to meet its GDPR obligation to notify the supervisory authority in accordance with Article 33.
3. The processor shall assist the controller in gathering the information required under Article 33(3), including:
   - a. the nature of the personal data breach, categories and approximate number of affected data subjects, and the categories and approximate number of personal data records concerned,
   - b. likely consequences of the breach,
   - c. measures taken or proposed by the controller to address and mitigate the breach.
4. All specific elements of the breach-notification assistance provided by the processor are further detailed in Appendix C.

10. Erasure and return of data

1. When the provision of personal data processing services ends, the data processor shall delete all personal data processed on behalf of the data controller and confirm to the data controller that deletion has been completed, unless EU or Member State law requires the data to be retained.
2. The data processor undertakes to process personal data only for the purposes and under the conditions specified in these Clauses.

11. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with Article 28 GDPR and with these Clauses. The data processor

shall allow for and contribute to audits, including inspections, carried out by the data controller or auditors mandated by the data controller.

2. Procedures for audits and inspections, including those of sub-processors, are described in Appendices C.7 and C.8.
3. The data processor shall provide supervisory authorities—who have legal authority to do so—with access to its facilities upon presentation of appropriate identification.

12. The parties' agreement on other terms

1. The parties may agree on additional clauses relating to the provision of the personal data processing service, including liability, provided such clauses do not contradict these Clauses or infringe the rights and freedoms of data subjects under GDPR.

13. Commencement and termination

1. These Clauses take effect when accepted by the customer through the online collection request process.
2. Either party may request renegotiation of the Clauses if changes in law or circumstances make renegotiation necessary.
3. These Clauses apply for the duration of the data processing services. They cannot be terminated while such services continue unless replaced with other valid data processing terms.
4. If the provision of data processing services ends and the personal data has been deleted or returned in accordance with Clause 11 and Appendix C.4, these Clauses may be terminated by written notice.

This Data Processing Agreement becomes effective upon the customer's online acceptance as part of the collection request process and is legally binding without physical signatures.

14. Data controller and data processor contacts/contact points

1. The parties may contact each other using their designated data protection contacts.

Data controller contact:
The data controller shall provide its contact details during the onboarding or collection request process.

Data processor contact:
Data Protection Officer
T1A A/S

Email: ph@t1agroup.com
Phone: +45 48 13 25 21

2. Both parties must notify each other of any changes to their contact details.

Appendix A – Information about the processing

A.1. Purpose of the processing

The purpose of the data processor's processing of personal data on behalf of the data controller is to erase or destroy personal data included in or attached to IT equipment provided by the data controller. This includes equipment intended for reuse, repair or refurbishment, harvesting, recycling, or resale.

A.2. Nature of the processing

The data processor ensures that data erasure complies with the most up-to-date standards, or higher, unless another method is specifically requested and instructed by the data controller. If a data-carrying medium cannot be erased through logical means, it will be physically destroyed using mechanical shredding in accordance with DIN Standard 66399.

Data sanitisation involves a three-step process:

1. **Physical examination and removal of physical data** (e.g., washing, cleaning).
2. **Logical data sanitisation** (software-based erasure solutions).
3. **Physical destruction through shredding**, if logical erasure cannot be effectively performed or if the data controller instructs the processor to do so.

Data-bearing equipment and media will be stored at a suitable, controlled, and secure facility until the erasure process has been completed successfully.

A.3. Types of personal data processed

The processor may handle any personal data stored on or accessible through the IT equipment provided by the data controller. This includes, but is not limited to:

- Basic personal data (name, date of birth, gender, contact details)
- Authentication data (usernames, passwords, PIN codes, security questions)
- Photos, videos, audio
- Unique identifiers (national ID numbers, bank account numbers, passport numbers, driver's licence numbers, IP addresses, employee numbers, signatures)
- Pseudonymous identifiers

- Biometric data (e.g., facial recognition, fingerprint data)
- Location data (cell ID, geolocation data, Wi-Fi access points)
- Internet activity (browsing history, viewing history)
- Device identifiers (IMEI, SIM number, MAC address)
- HR and recruitment data, including education history
- Special categories of data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric identifiers, health data, sexual life or orientation, or criminal conviction data)
- Any additional personal data defined under GDPR Article 4

A.4. Categories of data subjects

The personal data may relate to:

- Employees
- Temporary workers
- Contractors
- Customers
- End-users
- Partners, stakeholders
- Any individual who has used or interacted with the IT equipment in such a way that their data has been stored on the device

A.5. Duration of processing

Processing under these Clauses may commence once the agreement becomes effective and shall continue until the data processor ceases all processing activities on behalf of the data controller.

Appendix B – Authorised Sub-processors

The data controller authorises the use of sub-processors listed in the document titled **"Authorised Sub-processors List"**, which is maintained separately by the data processor and incorporated into this Agreement by reference. The list identifies each sub-processor, their role, and the jurisdiction in which they operate.

The data processor shall not engage a sub-processor for any processing activity different from what the controller has authorised without obtaining the controller's explicit written approval.

Unless secure transport is selected as part of the service, third-party logistics providers may receive devices for transportation only. These logistics providers do **not** act as sub-processors and do **not** access or process personal data.

B.2. Prior Notice for the Authorisation of Sub-processors

1. The data processor shall provide the data controller with at least fourteen (14) calendar days' written notice before adding or replacing any sub-processor.
2. The data controller may object in writing within fourteen (14) days of receiving notice, provided the objection is based on reasonable data protection concerns.
3. If the data controller objects and the data processor nevertheless elects to proceed with the new sub-processor, the controller may terminate the affected services with ten (10) days' written notice. The data processor shall refund any prepaid fees for services not yet delivered after termination.

The Sub-processor List shall be version-controlled, clearly indicating the effective date of the current version. It shall be made available to the data controller upon request. The data processor shall maintain a record of all changes to the list.

Appendix C – Instruction pertaining to the use of personal data

C.1. Subject of the processing

The data processor's processing of personal data on behalf of the data controller consists of handling IT equipment—whether data-carrying or not—and any related products provided under the agreement between the parties. The processing includes the erasure or destruction of personal data contained in or attached to the equipment in accordance with applicable standards. Prior to erasure or destruction, the equipment may be securely stored by the data processor.

The data processor must not process personal data for any purposes other than those stated in these Clauses.

The data processor is authorised to use the sub-processors listed in Appendix B solely for the permitted purposes. These may include secure erasure software providers and cloud-based communication platforms which support the erasure process without accessing data content. Such sub-processors must adhere to the same data protection obligations and provide equivalent protection in accordance with Article 28 GDPR.

C.2. Security of processing

The required level of security must consider the nature, scope, context, and purposes of processing, as well as risks to the rights and freedoms of data subjects. The following were taken into account:

- The volume of personal data potentially involved.
- The uncertainty of the types of personal data stored on the equipment.
- The purpose of processing, which is secure erasure.
- The limited duration of processing.
- That all data will be removed from the equipment.
- That data cannot be recovered after processing.
- That the overall risk to individuals is minimal given the processing context.

The data processor is responsible for choosing the technical and organisational measures necessary to achieve the required level of data security.

At a minimum, the data processor shall implement the following categories of measures:

Organisational Security

- Secure handling and sanitisation of all data-bearing devices, based on device type and data sensitivity.
- Compliance with all relevant environmental, health, safety, transportation, import/export, and data security regulations.
- A documented information and data security policy, communicated to staff and monitored through audits.
- Mandatory confidentiality and security requirements for third-party providers.
- Regular audits of sub-processors and third parties based on risk.
- Appropriate insurance coverage for risks and liabilities associated with operations.
- Legal and financial safeguards to ensure proper facility closure procedures.

Physical Security

- Secure storage and processing of equipment, components, and materials.
- Access restriction across all sites, including offices and off-site storage, to prevent unauthorised data exposure.
- Secure erasure and destruction procedures for all personal data, including paper-based data.
- Mechanical shredding of equipment that cannot be logically erased.

System and Network Security

- Protection of systems from unauthorised internal and external access.
- Use of antivirus, antimalware, secure configurations, and prompt patching.
- Encryption of laptops, devices, portable media, and data transmitted by the processor.
- Documented risk assessments using accepted industry methodologies such as ISO 27001.
- Documented risk management responses.

Access Management

- Access to personal data restricted to authorised individuals only.
- Defined user roles, privileges, and access controls, including multi-factor authentication where appropriate.
- Logging of access and usage of personal data.
- Measures to ensure data integrity and completeness.

Security Events

- Procedures for identifying, analysing, and managing security incidents.
- Documented disaster recovery and business continuity plans for systems used to process personal data.
- A system for logging incidents, performing root-cause analysis, and tracking corrective actions.
- Contingency and resilience planning to reduce impact during an incident.

Data Erasure

- A documented data sanitisation plan with appropriate controls and methods.
- Logical erasure meeting NIST 800-88 or equivalent standards unless another method is instructed by the controller.
- Mechanical destruction using DIN 66399 standards for devices that cannot be erased.
- Random compliance checks on erased equipment.
- Confirmation of receipt of equipment and method of sanitisation.
- Timely erasure performed internally or by verified downstream vendors.

General Security Principles

- Prohibition of unauthorised individuals handling data-containing equipment.
- Designated Data Protection Officer and Data Protection Representative.

- Mandatory training and confidentiality agreements for anyone authorised to handle equipment.
- Authorisation controls aligned with data sensitivity levels.
- Incident response procedures ensuring legal compliance and necessary notifications.

Transport

When responsible for collecting equipment from the data controller's premises, the processor shall:

- Use transport vendors that comply with all legal and safety requirements.
- Ensure secure packaging aligned with data security and environmental considerations.
- Apply additional security measures such as shipment tracking and concealment of contents.
- Use accurate and compliant shipping documentation.

If the data controller handles transport independently, they remain responsible for ensuring equivalent protective measures.

C.3. Assistance to the data controller

The processor shall assist the controller, as far as possible, in fulfilling its obligations under Clauses 8.1 and 8.2. This includes ensuring appropriate security practices that support the controller's ability to respond to data subject rights.

Given the nature of the services provided, the processor is not required to obtain or process additional information solely to identify a data subject for GDPR purposes.

C.4. Storage period and erasure procedures

Equipment must not be protected by passwords or locks (e.g., BIOS, MDM, remote management, SIM lock, "Find My iPhone") which would prevent the processor from performing erasure. All such locks must be removed before collection or delivery.

- Acknowledgement of receipt will be issued without undue delay and no later than ten business days.
- Logical erasure shall be completed within ninety business days from acknowledged receipt.
- Password-protected devices will be quarantined until unlocked, and the erasure timeline will restart once unlocked.
- Additional service fees may apply for handling password-protected equipment.
- Personal data stored on devices may be retained for up to twelve months solely to complete secure erasure. After this period, all data will be erased or destroyed.

- Erasure is irreversible and data cannot be recovered.

C.5. Processing location

Processing may only occur at:

- The data processor's facilities,
- Approved sub-processor facilities listed in Appendix B, or
- Any alternative location expressly authorised by the data controller.

Primary processing address:

T1A A/S Solvang 6 3450 Allerød Denmark

C.6. Transfer of personal data to third countries

Personal data shall not be transferred to third countries unless explicitly instructed by the controller. Without such instructions, no transfers may occur.

For clarity, Microsoft Ireland Operations Ltd. processes all relevant data exclusively within the EU/EEA.

C.7. Controller audits of the data processor

The data processor may obtain industry certifications and independent audit reports to demonstrate compliance with GDPR and these Clauses. These may include:

- ISO 9001
- ISO 14001
- ISO/IEC 27001
- ISO 37001
- ISO 45001
- ISAE 3000
- R2v3
- Annual financial audit reports

Upon request, these certifications and reports shall be made available to the data controller.

The controller may also conduct physical inspections of the processor's facilities with at least 30 business days' notice. The processor will assist with inspections, and any costs incurred by the controller remain the controller's responsibility.

C.8. Controller and processor supervision of sub-processors

The processor shall periodically verify that all sub-processors comply with GDPR and these Clauses.

The processor or its representative may inspect sub-processor facilities. Documentation from such inspections shall be provided to the data controller.

If the data controller deems this insufficient, they may request to participate in a physical inspection, at their own expense.

Appendix D – The parties' terms of agreement on other subjects

D.1. Data breach notification

When notifying the data controller of a personal data breach, the data processor shall provide:

- A description of the breach, including categories and number of affected data subjects, date and time of the incident, summary of what caused the breach, categories and number of data records affected, and the nature and content of the personal data involved.
- A description of the circumstances of the breach (e.g., loss, theft, copying).
- Identity and contact details of the data processor's Data Protection Officer or other relevant contact point.
- Recommended steps to mitigate possible adverse effects.
- A description of measures taken or planned by the data processor and/or any sub-processor to address and mitigate the breach.
- Any additional information reasonably requested by the data controller to comply with GDPR and national data protection regulations, including obligations relating to notification and disclosure to public authorities.

D.2. Liability

The data processor's total liability to the data controller for breaches of data protection obligations under these Clauses is subject to the same limitations of liability as those included in T1A's standard Master Services Agreement (MSA) or Framework Agreement.

In the absence of a separate Master Services Agreement or Framework Agreement, the data processor's liability shall be limited to direct damages caused by breach of its obligations under these

Clauses, subject to applicable law. Indirect or consequential damages are excluded. These Clauses are enforceable independently of any other agreement.

The data controller shall indemnify and hold the data processor fully harmless from all claims, expenses, losses, damages, or liabilities arising out of or connected to the data controller's violation of applicable data protection law.

D.3. Additional services

If the data controller requires additional services — for example, the implementation of new technical or organisational security measures beyond those included in these Clauses — the data processor shall notify the data controller of any associated costs before they are incurred. The data controller shall reimburse reasonable and documented costs.

If the data controller requests the return of any IT equipment for any reason, the data processor is not responsible for costs related to this request. All associated expenses shall be borne by the data controller.

D.4. Assistance to the data controller

The data processor's assistance to the data controller, as set out in the Clauses, shall be charged separately on a time-and-materials basis.

D.5. Choice of law and venue

Governing Law
These Clauses and any disputes or claims arising out of or relating to them are governed by and interpreted in accordance with the laws of Denmark, excluding its rules on choice of law.

D.6. Dispute resolution

Negotiation
If a dispute arises between the parties, they shall first attempt to resolve it through negotiation. If the dispute cannot be resolved through negotiation within thirty (30) business days, the following options apply:

Option 1: Arbitration

i. Any dispute not resolved through negotiation shall be settled by arbitration under the Rules of Procedure of the Danish Institute of Arbitration as applicable at the time the arbitration begins.
ii. The place of arbitration shall be Copenhagen, and the language shall be Danish.
iii. Arbitration proceedings and the resulting award shall remain confidential indefinitely.

Option 2: Court proceedings

If arbitration is not chosen, disputes shall be submitted to the ordinary courts of Denmark, which shall have exclusive jurisdiction over all matters related to these Clauses.