

Data Protection and Security

Technical and Organizational Measures

To the attention of the Customers of Alpega Group

The information covered by this document is subject to change without notice and does not constitute a commitment on the part of Alpega Group (hereinafter referred to as Alpega) or any other company belonging to Alpega Group. This document may not be reproduced or transmitted in whole or in part in any form including photocopying and recording for any purpose whatsoever without the prior written approval of Alpega Group Legal Department.

Copyright Alpega Group 2026 – All rights reserved.

(Document version 2.2 19 May 2026)

Introduction

This document outlines the binding Technical and Organizational Measures associated with commissioned data processing operations carried out between the controllers and processors of Alpega Group and provides information about the valid data protection and data backup concepts.

Scope

The Technical and Organizational Measures described apply to Alpega Group.

Contents

Introduction.....	2
Scope	2
Data Protection and Security Framework	3
Confidentiality	4
Integrity	8
Availability	10
Resilience.....	11
Organizational Measures.....	12

Data Protection and Security Framework

The following outlines the specific Technical and Organizational Measures requested by Art. 32¹ and implemented pursuant to Art. 24² of the EU General Data Protection Regulation (GDPR) for commissioned data processing.

Alpega Group fulfils the obligation established in the GDPR to safeguard processing of personal data by means of appropriate technical and organizational measures and, where possible, to anonymize or pseudonymize personal data. All measures implemented are associating the risk with the respective data processing operation and are state of the art. In particular, the effectiveness of the measure considers the protection objectives of confidentiality, availability, integrity, and capacity. This is supported by integrating data protection measures, information security and additional measures to safeguard data processing operations.

How this is implemented is documented in supporting policies and guidelines. These supporting policies and guidelines are considered confidential and are only shared with third parties based on a specific request or as part of a third-party audit.

On request, the customer receives an audit right to check the status discreetly as agreed in the Data Processing Agreement.

Definition of security value terms:

- **Confidentiality:**
Protection of data, information and programs against unauthorized access and disclosure.
- **Integrity:**
Factual and technical accuracy and completeness of all information and data during processing.
- **Availability:**
Information, data, applications, IT systems and IT networks are available for processing.
- **Resilience:**
Represented as an aspect of availability and thus the capacity of recovery of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

¹ <https://gdpr-info.eu/art-32-gdpr/>

² <https://gdpr-info.eu/art-24-gdpr/>

Confidentiality

Technical and Organizational Measures are implemented that are appropriate for safeguarding confidentiality. Considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the following measures are taken to safeguard the confidentiality of personal data.

1. Access control

Measures are implemented that deny unauthorized persons access to data processing systems that process and/or use personal data. This is done by:

1.1. Property security

- Office premises are monitored 24 hours a day, seven days a week by building security staff or CCTV, depending on local law and regulations.
- Opening of doors is technically monitored.
- Access is logged.
- The Data Centers – and thus the hardware, servers, or components – are located in a separate secure area that is segregated from Office premises.

Access is only granted to authorized persons after checking and establishing identity.

1.2. Security zones

- The Data Centers are segregated from Office premises with strictly restricted access and surveillance.
- Office premises are secured by access control.
- The localities are divided into several security zones.

1.3. Type of access control

- In the Data Centers, an automatic identity check is carried out by means of personal access cards and recording attendance using smart card readers.
- Offices are secured by a controlled key arrangement or electronic locking systems.
- The reception is staffed during core hours and receives visitors.
- Emergency exits are secured against improper use (via alarms).

1.4. Regulation of access authorization

- Access authorization is organized restrictively and granted based on appropriate authorization procedures.
- Authorized people are determined with respect to security areas (e.g. Data Center).
- Visitors and externals must report to the reception desk and are collected and accompanied.
- Rules for employees leaving the company and changes in internal jobs and/or authorization are defined in the On- & Off- boarding process.
- There are rules/follow-up measures if badges, keys, etc. are lost.
- Maintenance and repair staff are supervised.
- Granted access rights are regularly reviewed. The granting and withdrawal of access authorization can be reconsidered at any time.

2. Access control to data processing systems

Use of data processing systems by unauthorized persons is prevented by:

2.1. Access authorization control

- Access authorization is granted to users based on authorization procedures.
- Personal user ID and personal initial passwords are allocated.
- Access is only granted after prior login with authentication (user ID, password or also two factors authentication).
- The screen session is automatically protected by screen savers requiring a password after a certain period and can also be manually locked.
- Measures for password security (length, complexity, and safekeeping) and rules for the use of passwords are in place.
- Rules are in place if passwords are lost or forgotten.
- A rule that makes need-to-know and a least-privilege principles compulsory for authorization procedures is in place.
- Administrator accounts are exclusively used for strictly limited activities.
- Rules are in place for authorized persons leaving the company or changing jobs.
- Disconnection occurs in the case of repeated failed attempts or timeouts.
- Inactive connections are automatically closed after a set waiting period (timeout).

- There is a separate infrastructure for visitors (Wi-Fi Guest protected by password security and policy – this network is distinct from the internal Alpega network).
- Users can only have access to personal data according to the authorization granted to them (by means of role allocation, functional user etc.).
- Unauthorized attempted access is detected (e.g., logging of system use) and investigated accordingly.
- Clean desk principle in place.

2.2. Additional measures for remote access

- Persons authorized to log in externally are specified.
- Network access security is provided by means of hardware and software measures.
- Unauthorized access from the internet is prevented by use of firewalls.
- Unauthorized attempted access can be detected (intrusion detection).
- Protection of existing sessions against takeover by other users (session hijacking) is provided.

2.3. Logging of access

- Access to data processing systems and workstations is logged (e.g., in a log file).
- Use of data processing systems is verifiable (logging of access).
- Remote access via the (SSL) VPN gateway is logged.
- The granting/changing of access authorization is logged.
- Logs are regularly evaluated.

3. Access control/User control

It must be ensured that authorized persons can only access the data covered by their access authorization when using a data processing system and that personal data are not read, copied, altered, or deleted without authorization when processing, using and after storing personal data. This is done by:

3.1. Authorization concept

- Rules are established for granting and managing access authorization.
- Individual access rights and user groups have been formed.
- User groups are managed in a central directory service.
- Granted authorization is regularly reviewed.

3.2. Access control

- The use of encryption routines and a file encryption option have been provided.
- Mobile devices are encrypted.
- Network access security has been set up.
- Only approved hardware and software are used.
- Network components are protected.
- The network is segmented in security zones.
- There is separation between testing and productive environments.
- Critical services are subject to monitoring.
- The secure disposal of information (in accordance with DIN 66399 – Level 4) is guaranteed.

3.3. Safekeeping when using data storage devices

- The safekeeping of data storage devices is controlled.
- Encrypted data storage devices are available.
- Data storage is repaired or replaced in the event of a warranty claim in compliance with data protection regulations.
- Other data storage devices are not repaired but rather are subject to more secure deletion/destruction (in accordance with DIN 66399 – Level 4).
- Persons authorized for data storage device removal are specified.

4. Separation control

It is ensured that data collected for different purposes can be processed separately. This is done by means of the following measures:

- The software and filing structure used are built to support multiple controllers.
- Logical separation of data is established.
- Internal guidelines for data collection and processing are established.

Integrity

Factual and technical accuracy and completeness of all information and data during the processing of personal data are guaranteed. The identification and correction of unauthorized modifications must be ensured. The following checks ensure the integrity of personal data:

1. Transmission control/Transfer control

Unauthorized reading, copying, alteration or deletion in the case of electronic transfer or transmission are prevented. This is done as follows:

1.1. Regulation concerning electronic transfer

- Data transfer takes place in protected networks.
- External networks are used exclusively (ZTNA, dedicated line).
- Filter mechanisms prevent connections to & from unauthorized IT systems (by Firewall systems).
- There is the option of encrypting data (PGP) and transferring encrypted data (TLS).
- Connections from and to external networks are secured via the Demilitarized Zone (DMZ)

1.2. Regulation concerning storage on removable media

In principle, storage of personal data on removable media is not provided. In exceptional cases, only encrypted mobile data storage devices are used:

- Data storage devices (USB sticks, etc.), where personal data could be stored are held in a central storage room with secured access.
- In principle, private data storage devices are prohibited on Office premises; case-specific exceptions are only approved on request.

1.3. Regulations concerning the transportation of data storage devices

- Data storage devices containing personal data are protected against unauthorized access, damage, and loss during transportation.
- Paper is disposed of by means of document shredders and/or disposal firms.

1.4. Regulations concerning the disposal of data storage devices

- Data storage devices are disposed of in accordance with data protection requirements and destroyed by a disposal firm.

2. Input control/Data storage device control/Storage control

It is ensured that it can be subsequently checked and established whether and by whom personal data is entered, altered or deleted in data processing systems. This is done by means of the following measures:

- Responsibilities for data entry, including stand-in arrangements, are established by assigning authorization.
- Logging of all master data entries, alterations, or deletions of data so that the originator, time, and content of the change can be traced.
- Relevant user activities are recorded (sender, time stamp and change content).
- Log evaluation systems can analyze captured logs.
- Databases and corresponding backups are secured by encryption.

Availability

It is guaranteed that personal data is protected against the risk of accidental destruction or loss. To this end, the following measures have been implemented:

1. Creation and safekeeping of backups

- All Backup activities are performed by our Infrastructure Team or by our Service Providers (ISO 27001 certified) in charge of the hosting of our infrastructure.
- A documented data backup concept is available.
- Controlled and regular backup of files and databases.
- Testing of data recovery is regularly carried out and documented.
- Data backup is protected against unauthorized access.
- Backup sets are securely stored separately from the original data at specially protected locations.

2. Safeguarding of day-to-day operations

Day-to-day operations are secured by means of the following Technical and Organizational Measures:

- Shift operation (24 / 7 coverage).
- Capacity planning and monitoring.
- Appropriate Endpoint (virus and malware) protection on clients and servers is implemented.
- IDS, IPS and WAF are largely implemented.
- Measures against DDoS attacks are taken.

Resilience

Completely redundant Systems (providing contractually agreed availability).

1. Uninterruptible power supply

- An uninterruptible power supply (UPS) with sufficient capacity is installed upstream of the Data Centers.
- Proper functioning is ensured by means of regular testing.
- Tests are documented.

2. Fire protection

- Area-wide fire alarms and/or early fire detection devices are available.
- CO2 handheld fire extinguishers are available in the Data Centers.
- Fire drills are carried out at least once a year.

3. Air-conditioning

- Redundant air-conditioning systems are present in the Data Centers.
- Multiple climate control modules are present for optimal cooling distribution.
- Leakage warnings are relayed to the permanently manned security guard post.
- Temperature monitoring is relayed to the permanently manned security guard post.
- Responsible employees (IT Operations, IT Management) are notified by the security guards if triggered.
- Service contracts are in place.

4. Internet connection

- A redundant internet connection is available.

5. Measures for operational disaster control

- A Disaster Recovery Manual (with responsibilities) has been prepared and is maintained.
- Emergency organization is in place.

Organizational Measures

1. General Measures

As security is a continuous work in progress, the General Measures put in place can evolve:

- Security guidelines as well as security and privacy operating procedures exist, have been announced and are checked.
- There are requirements for procedural and program documentation.
- Operational availability is regularly checked.
- Before being put into operation, IT systems are finalized according to defined procedures and thus raised to a higher security level.
- A Business Continuity Management plan has been defined.
- A failover procedure has been defined.
- Users are trained.
- An information security officer has been appointed. There are rules for file retention (central backup).
- Data are deleted at the end of the defined retention periods.
- Escalation Paths are documented and communicated across the organization.

2. Procedure for regular monitoring, assessment, and evaluation

- The effectiveness of the measures implemented are reviewed, assessed, and evaluated by means of internal processes and procedures, especially at organizational level.
- Annual review of safety measures by external auditors, including cooperation with these auditors, to resolve all findings in a timely manner.
- Audit right by the customer according to contractual agreements.

3. Data protection management

The extensive obligations and requirements of the GDPR call for a comprehensive strategy based on a structured approach and an appropriate management system. All the components necessary for ensuring data protection are subject to systematic coordination of data protection management. This includes the following measures:

- Data protection organization has been established.
- Established processes provide for the involvement of the data protection officer (DPO).
- Privacy guidelines and operating procedures have been announced and compliance is monitored.
- There are formalized approval procedures for new data processing procedures and in the case of significant changes in legacy processes.

4. Incident response management

Relevant reporting channels are defined, and responsibilities established to be able to respond to an incident, if necessary. To this end, the following measures have been implemented:

- Employees are trained accordingly.
- Reporting points and escalation channels have been defined for (security-related) incidents.
- Immediate notification of the customer in the event of incidents relevant to data protection is a matter of course.
- Documentation is maintained.
- Experience gained is channeled into the further design and improvement of processes.

5. Data protection by design and by default

Default settings ensure that personal data are only processed in accordance with the specific processing purpose. This applies to the quantity of personal data collected, the scope of processing, the retention period and accessibility. The following measures have been implemented:

- Thanks to the ongoing awareness and training process within the context of data protection management, employees are careful when handling personal data and consider the privacy principle of data minimization to be part of the development of technical and business processes.

6. Order control

It is ensured that commissioned personal data processing is only carried out in accordance with the instructions of the controller. Commissioned data processing as defined in Art. 28³ of the GDPR is not carried out without the appropriate instructions of the controller. To this end, the following measures have been implemented:

- An internal process ensures that the necessary contracts for commissioned data processing are completed.
- A written contract between the controller and the processor is available in each case.
- The controller issues written instructions to the processor.
- The commissioned data processor has ensured appropriate internal rules based on the instructions of the controller.
- Adequate measures to ensure compliance with data protection by a sub-processor are regularly checked.
- If an inspection has been carried out by the regulatory authority at the processor, the controller may request the inspection report.
- Conclusion of a data processing agreement with customers and sub-processors.
- Notification to the customer in the event of data protection-relevant incidents, the corresponding guideline is reviewed annually.

³ <https://gdpr-info.eu/art-28-gdpr/>