Technical and Organizational Measures (Dräger Group)

These technical and organizational measures of the Dräger Group for the protection of personal data in accordance with Articles 28 and 32 of the GDPR and information on the protection of trade secrets are subject to constant development, taking into account the state of the art, the implementation costs and the type, scope, circumstances and purposes, as well as the probability of occurrence and severity of the risks, and can be retrieved in the current Version under www.draeger.com/dpa.

1. Cyber hygiene

Cyber hygiene involves the application of basic procedures and approaches that generally lead to an improvement in the cybersecurity level of an institution.

1.1. Patch Management
Centralized patch and update management is carried out on the end devices managed by Dräger. For network elements and sever infrastructure, there are dedicated specifications and regular checks for patch and update management. If security vulnerabilities are discovered, software is updated depending on the criticality or the affected system is isolated.

1.2. Regulations for strong passwords
The Dräger Password Directive specifies how secure passwords are to be designed according to the current state of the art and how IT systems must implement this.

1.3. Manage devices and device configurations
Management and configuration of the various end devices used is operated centrally at Dräger.

1.4. Identity and access management
An identity management system operated for the Dräger Group controls access management on end devices and for system accounts.

1.5. Network segmentation
At Dräger, networks are separated according to functions and thus enable context-specific protective measures.

1.6. Backup and backup concepts for data
For systems with information worthy of protection, Dräger has backup and security concepts in place that ensure that the relevant information is not lost and that systems can be set up anew in a reasonable time.

1.7. Protection against malware
Dräger's computers, servers and network run powerful programs for detecting and eliminating malware. These programs and their detection patterns are continuously kept up to date.

2. Confidentiality of systems and services

2.1. Entry control

Entry control comprises those measures that are suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data is processed or used.
At Dräger, the following measures are used to control access to operating sites and branches:

- Authorization-controlled access badges (card readers at the main and side gates of the company premises) and/or manual locking systems with key control and/or code blocking;
- Visitor management (reception, protocol, escort, visual identification);
- Alarm systems and building surveillance;
- Security of the factory premises in Lübeck by carefully selected security personnel;
- Careful selection of cleaning services.

2.2. System access control

System access control comprises all measures that are suitable for preventing unauthorized use of or access to data processing systems.

At Dräger, unauthorized use of IT systems is prevented by the following measures:

- Login with user ID and password;
- Screen lock with password activation;
- Remote maintenance only takes place via a portal system with its own access codes and a dedicated authorization concept or via an individual session release by the user;
- Each authorized person has their own password that is known only to them. Password complexity and change cycles are based on the state of the art, in accordance with BSI specifications;
- Multi-factor authentication;
- Central guidelines for deletion/destruction;
- Centrally controlled data protection and information security regulations and associated training concept with mandatory training;
- Enforcement of policies through end device management (MDM, MEM);
- Functional assignment of data terminals to users;
- a dedicated roles/rights concept for each device.

2.3. Data access control

Data access control refers to those measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing and after storage.

For the relevant IT systems with which personal data is processed, authorization concepts are in place that technically allow access to the personal data stored therein only to those users who also have the required role / the associated authorization.

Storage media of the Controller that are taken out of operation are subjected to a controlled and documented destruction process.

Paper copies made by the Processor for the purpose of providing the service shall - if on Dräger premises - be disposed of using document shredders or in locked data protection containers, which shall be disposed of in a process approved under data protection law by a specialized service provider with whom an order processing contract exists. If paper copies are disposed of at the customer's premises, the customer's specifications and processes are followed.

Every employee is obliged to maintain data confidentiality at the start of their employment and receives an introduction to handling personal data and the Controller's business and trade secrets.

This obligation to maintain data secrecy continues even after the employment relationship has ended.

All information and documents at Dräger are classified based on their confidentiality. Technical and organizational protective measures are defined on the basis of these classifications (public/internal/confidential/strictly confidential).

2.4. Pseudonymization and encryption

Where possible, data is processed in such a way that it can no longer be attributed to a data subject without the use of additional information (pseudonymization). This additional information is stored separately and is subject to appropriate technical and organizational measures (e.g. encryption).
As a rule, Dräger also uses the most comprehensive encryption possible in conjunction with authorization systems in its electronic processes. This controls who has access to the data to be protected. There are context-specific approaches to encryption and key management that follow the "need to know" principle. The choice of the right technology and scope of encryption depends on both the security and functionality of the product.
The following concrete measures have been established:

- Hard disks in work-computers are encrypted with BitLocker
- USB sticks are provided with hardware encryption (AES 256 bit)

There are internal requirements to process personal data that is processed for customers in accordance with the principles of "Privacy by Design" (data minimization, data separation, storage limitation, technical protective measures, pseudonymization and anonymization).

3. Integrity of systems and services

3.1. Input control: Input control refers to those measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed from data processing systems.
The following measures are always implemented at Dräger:

- Logging of the entry, modification and deletion of data records;
- Traceability through unique usernames;
- Assignment of rights to enter, change and delete data;
- Monitoring of irregularities, including in login attempts, are monitored via an automated SIEM (Security Incident Event Management), which is operated and evaluated by a dedicated SOC (Service Operation Center).

3.2. Transfer control: Data transmission control comprises those measures that ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which bodies personal data is intended to be transmitted by data transmission equipment.
The following security measures are used on Dräger's computers and network:

- Virus protection on all end devices provided by Dräger;
- Network segmentation;
- firewalls at the network boundaries and network segments;
- Use of spam filters with continuous updates;
- VPN (Virtual Private Networks) to the Dräger Global Network;
- Content filters / proxies and DMZ (Demilitarized Zones);
- IPS / IDS (Intrusion Detection / Prevention Systems) on the Internet outbreaks;
- Encryption of e-mails (via S/MIME);

- Processes for electronic signatures established;
- Patch and update management for end devices.

3.3. Separation control: Separation control includes all measures that ensure that data collected for different purposes can be processed separately. The following measures ensure the separate storage, modification, deletion and transmission of data with different contractual purposes:

- Multi-Controller capable applications and logical Controller separation;
- Functional separation in production, test and development environments;
- Control via authorization concept;
- Definition of database access rights.

4. Availability and resilience of systems and services

4.1. Availability control

Availability control and emergency planning describes those measures that ensure that personal data is protected against accidental destruction or loss.
At Dräger, the Controller's data is only processed within the Controller's infrastructure as part of service activities. A failure of the systems at Dräger would therefore, in the worst case, only result in the pending maintenance having to be postponed.
Irrespective of this, the following measures are implemented as standard for the provision of infrastructure at Dräger:

- Fire and smoke detection systems;
- water-free fire extinguishing systems in server rooms;
- Air conditioning and monitoring of server rooms;
- UPS (uninterruptible power supply) using diesel generators;
- NAS storage systems that include RAID systems / hard disk mirroring;
- Active monitoring of central systems and alerting with recovery processes;
- Backup procedures with application-specific cycles.

4.2. Resilience

Resilience is understood as a combination of robustness and resilience. Robustness involves hardening the components used in accordance with the risk level and resilience involves the measures taken to be able to react to unexpected disruptions.
The IT systems used at Dräger are hardened in accordance with their use and regularly checked for weaknesses, and penetration tests are carried out by external providers. Any security vulnerabilities identified are assessed and rectified immediately. Software developed in-house is also regularly checked for OWASP10 criteria by a risk management system.

In order to be able to react to unforeseen incidents, a security incident response management process has been established in IT at Dräger, which also provides for the convening of a CERT (Computer Emergency Response Team) in particularly critical cases.

Dräger IT operates a continuous, tool-based vulnerability management system that ensures the identification and elimination of security gaps. This includes regular scans and a well-defined patching process that ensures risk is minimized.

Dräger uses up-to-date cyber threat intelligence to detect threats at an early stage and react proactively. Information from trusted sources is incorporated into the security strategy and strengthens defenses.

Using specially provided forensic systems, possible security incidents can be analysed seamlessly and evidence can be secured in a way that will stand up in court. Automated logging and central data storage enable fast and precise investigations.

4.3. Recoverability

In the context of remote service and continuous monitoring, it is ensured that the availability of data and access to it can be restored immediately in the event of a physical or technical incident. In the case of remote maintenance, an incident during access has no impact on availability.

5. Remote maintenance of medical devices

Remote maintenance of medical devices and/or in the medical context, includes the measures in the area of our range of services for medical technology customers, which ensure that spatially separated access to IT systems for maintenance and repair purposes can be protected from access by unauthorized persons. This is only done in cases where this has been contractually agreed with the Client and the technical solutions provided by the Processor are used. For the remote maintenance solutions provided by the processor, the technical and organizational requirements listed under the section Access Type, Connection Establishment and Security Measures have been met.

If, in special exceptional cases – which are agreed separately between the Client and the Processor – a technical solution provided by the Client is used for remote maintenance instead, the Client alone, in its role as controller within the meaning of Art. 4 No. 7 GDPR, shall in particular ensure compliance with an appropriate level of security in accordance with Art. 24, 25 and 32 GDPR.

5.1. Access Type

In principle, the client network is reached via a secure connection to dedicated systems of the client, which is either E2E encrypted after the connection has been established or is encrypted point to point via an intermediary server provided by carefully selected and tested service providers for specific, selectable forms of encryption. Depending on the state of the art, encryption is chosen to be sufficiently secure even for particularly critical data.
At the request of the client, it is possible to restrict access, e.g. to the time of day and the group of participants. Where 24/7 support contracts exist, 24/7 access to the dial-in nodes is mandatory.
Remote maintenance is carried out almost exclusively on server systems; the client's end user works at remote workstations that are only accessed in absolutely exceptional cases in coordination with the personnel on site.

5.2. Link Connection

In order to establish contact between the remote maintenance computer and the gateway in the customer network, a secure intermediary server of a portal system is called via HTTPS, which establishes contact between the end devices in question so that an encrypted tunnel can be established. Schematically, the connection is established as follows:

Remote maintenance computer -> mediation server -> system to be maintained by the client. The Dräger remote maintenance computer connects to the mediation server. Only after successful authentication can the named Dräger service employee only access the client's assigned devices and call up a connection to them.

5.3. Security Measures

It is also ensured that:

- the remote management software terminates when the connection is lost;
- the client can cancel remote maintenance at any time;
- a logging of access takes place.

6. Order control

Order control refers to those measures that ensure that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

6.1. If another company provides services for Dräger as a Processor ("sub-Processor") and personal data is collected, processed and used in this context, Dräger ensures that the sub-Processor is carefully selected, and that the selection is based in particular on the protection of personal data. In addition to the legal requirements, service providers are commissioned based on the standards applicable at Dräger.

6.2. Furthermore, the data protection department must be informed, and the Processor must be checked regarding the technical and organizational measures it has taken for data protection and data security. Dräger shall oblige its Processors to comply with the legal requirements for the protection of personal data and, in particular, to provide evidence upon request that the employees who work for Dräger in the course of providing services have been obliged to maintain data secrecy. Dräger makes use of its right to issue written instructions to the Processor regarding the type, purpose and scope of the processing of personal data and to ensure compliance with the specifications by means of checks. The use of further sub-Processors is also only possible after prior notification to Dräger.

6.3. The processors used were obliged to comply with the data protection requirements by means of a contract for order processing (DPA). In addition, when the data is transferred to a third country, the EU Standard Contractual Clauses will be imposed on the sub-Processor, unless exempted by an adequacy decision.

The relevant processors are:

- Service providers for the operation and management of client computers and the software used on them;
- Service providers for the operation and management of the network and network access;
- Service providers for the disposal of paper-based documents and electronic storage media.

7. Procedures for regular monitoring, assessment and evaluation

7.1. Data protection and security measures

The data protection management system implemented at Dräger consists of guidelines, training and a tool-supported register of processing activities. The directory is updated annually. Processes (documented in the IMS) have been established and trained for reporting new or changed data processing procedures to the data protection officer. If necessary, a data protection impact assessment is carried out to ensure secure processing. Random checks are conducted by means of data protection audits.

In order to maintain data protection-friendly default settings, no more personal data is collected than is necessary for the respective purpose. Implementation is also ensured through guidelines and information sheets. In addition, technical measures have been implemented to make it easy for data subjects to exercise their right to withdraw consent.
The measures implemented for the IT systems used are recorded in security concepts and regularly reviewed with regard to the effectiveness of the technical measures.
Employees are regularly made aware of and trained in the secure handling of personal data and are obliged to maintain confidentiality. In addition, there is central documentation of the procedures and regulations on data protection at Dräger.

7.2. Incident response management

Incident response management refers to the measures used to support the response to security breaches.
A process for the preparation, identification and rectification of security breaches and system malfunctions is anchored in risk management and IT management. Furthermore, there is a process for reporting security incidents (also with regard to the obligation to report to the supervisory authority). The involvement of the data protection officer is also regulated here. All security incidents are documented and filed centrally. A detailed end-of-day report at records the measures taken daily to prevent the risk of a security incident.