ottobock.

Policy.
Data privacy management system.

Version 1.0 / March 2024

Foreword.

Dear Colleagues,

The protection of your personal data and the personal data of everyone we deal with, in particular our patients, is a fundamental concern for Ottobock. In Germany and the European Union, we are subject to the provisions of the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG) and in the United Kingdom to the UK Data Protection Act 2018 (collectively GDPR), which are comprehensive data protection laws aimed at the protection of personal data and the protection of data of natural persons in the EU, the European Economic Area and the United Kingdom. Outside the EU, data protection law is also being modernised and becoming increasingly important.
Ottobock continues to develop into a data-driven company. Strategically, we will increasingly use personal data to improve Ottobock products and services and to improve patient treatment. To do this, we need to ensure that our data protection organization complies with the new requirements.

With this policy, we therefore want to adapt organisational responsibility accordingly to ensure that we are able to rise to future challenges.

ottobock.

Contents.

Scope

This policy applies for all employees and for all members of governing bodies (supervisory bodies, Executive Directors, employees with and without management responsibilities) of Ottobock SE & Co. KGaA (hereafter: Ottobock).

Objective of this document

The Data Privacy Management System Policy (DPMS Policy) explains the importance of data protection and the need for a data privacy management system (DPMS) in general, and also provides an overview of the DPMS at Ottobock. It also describes in detail the design of the individual elements that form the organisational and procedural framework for the DPMS.

The policy is intended to provide an overview of the tasks and responsibilities associated with the DPMS. Together, it is intended to contribute to the introduction, description and adherence to appropriate regulations, processes and procedures to minimise data protection risks. It is intended to form the basis for a group-wide DPMS.

Designation of the “Cyber Security” and “Data Privacy" department

The “Cyber Security” department is the organisational unit responsible for developing and implementing the DPMS at Ottobock. References to the department in the context of the tasks and/or responsibilities described in this policy generally refer to the organisational area of the department that is involved with data privacy management matters. Thus the department is referred to as the "Data Privacy department" in the following. This improves readability and avoids misinterpretations in the context of tasks and/or responsibilities.

Notice of equal treatment

To improve readability, the simultaneous use of male, female and diverse forms of speech is avoided. All designations apply equally to all genders.

A. DATA PROTECTION AND DATA PRIVACY MANAGEMENT SYSTEM

1. Data protection compliance – what does that mean for Ottobock?

Ottobock defines “data protection compliance”[1] as adhering to the legal provisions and requirements for data protection by which Ottobock is bound and implementing them by means of internal Ottobock rules and policies. In this context, entrepreneurial activities must also comply with the organization's internal rules, which are shaped by general social values and moral and ethical considerations. Ensuring data protection compliance is the task of each individual, from the Supervisory Board and Management Board to the Executive Directors, managers and every Ottobock employee.

2. Basic elements of the Ottobock data privacy management system

The objective of Ottobock's DPMS is to achieve compliant behaviour through a systematic framework and to minimise data protection risks. The scope of the DPMS is determined by the sum of all data protection-relevant measures. Measures are derived on the basis of risk. They are based centrally in the Data Privacy department as well as locally in the various Ottobock departments.

In addition, the DPMS provides a uniform organisational and procedural framework for all data protection-relevant topics with significant data protection risks: It thus creates a structure to be able to effectively and efficiently implement measures to comply with the legal regulations and requirements in the respective data protection focus topics in terms of processes and methods. It also defines standards in order to establish minimum requirements for data protection-related processes and procedures, etc. This includes, for example, the creation of standards for identifying compliance risks at a department level, or for preparing compliance training modules.

The structure of the Ottobock DPMS is fundamentally based on the auditing standard “IDW PS 980” and, in particular, the content of the auditing standard “IDW PS 986.1” published by the IDW (Institute of Public Auditors in Germany). In line with this standard, the CMS at Ottobock is broken down into the following seven elements. These elements form the foundation for the company-specific structure and implementation of the DPMS:

- Data protection culture
- Data protection objectives
- Data protection organisation
- Data protection risks
- Data protection programme
- Data protection communication
- Data protection monitoring and improvement

[1] These factors make a distinction between compliance risks that are managed in other compliance management systems (such as the tax compliance management system and the (legal) compliance management system).

B. DATA PROTECTION CULTURE

The basis of a functioning DPMS is the active data protection culture in the company. This culture is primarily created by the basic attitudes and behaviour of the Executive Board and the supervisory bodies ("tone from the top"). The data protection culture influences the importance that the company's employees attach to observing data protection rules and thus the willingness to behave in compliance with data protection regulations. The company values and the code of conduct derived from these are of special importance for Ottobock in this context.

1. Code of Conduct

The code of conduct reflects the commitment of the shareholders, and in particular the Näder family, Supervisory Board, Management Board and Executive Directors as well as the Works Council, to the fundamental values of the Ottobock company culture. Within the Ottobock Group, the code of conduct serves as a binding basis for the behaviour of all employees (with and without management responsibilities) and the Executive Board in day-to-day business.

The Code of Conduct was developed by the Executive Board and approved by the Management Board with the consent of the Supervisory Board. By request of the CEO, the Executive Boards of all[2] subsidiaries of Ottobock SE & Co. KGaA have also approved and implemented the code of conduct in the companies under their responsibility. The Ottobock SE & Co. KGaA code of conduct is available in German and in English, and can be accessed through the intranet and on the company website.

Section 8 of the code of conduct is committed to complying with data protection:

> **Sensitive information must be handled discreetly**
> The protection of confidential, secret and personal data is part of the principles in all our relations with colleagues (including former ones) as well as their families, with job applicants, customers, suppliers and other people.
>
> Personal data may only be collected, processed or used where this is required for clearly defined and lawful purposes. Our company ensures that the use of data is transparent to those concerned and that their rights to information and correction are protected.
>
> Every employee is obligated to comply with the provision on data protection as well as the statutory and corporate rules on information security. Furthermore, they are obligated to protect data entrusted to our company against misuse. Our company undertakes to guarantee an appropriate standard in securing information processing. All components of information processing shall be secured in such a way that the confidentiality, integrity, availability and verifiability of the protected information is given, thus preventing any unauthorised internal or external use thereof.

[2] This refers to all subsidiaries of Ottobock SE & Co. KGaA in which it holds more than 50% (majority shareholding).

Business and trade secrets are strictly confidential. This principle also needs to be observed for protecting the information of our business partners. Processes and transactions in the company that are sensitive for our company or our business partners must be kept confidential. The direct or indirect use of business information that is not available to the general public for personal gain, the benefit of third parties or the detriment of our company is prohibited.

Intellectual property is essential for the success and economic development of Ottobock. This means protecting our intellectual property, including all patents, trademarks and copyrights, trade secrets, technical and scientific knowledge and the know-how of our company developed over the years. Ottobock also respects the intellectual property of others.

The obligation to comply with all the points above continues to apply beyond the duration of the active employment relationship.

2. Tone from the top

The exemplary behaviour of the Executive Board in adhering to and observing the company values and applicable internal and external regulations on data protection is crucial in order to establish a strong compliance culture at Ottobock. Setting an example of compliance with data protection regulations forms the basis for motivating all employees to help shape the data protection culture and follow the rules.

At Ottobock, the tone from the top on the subject of data protection takes specific form through contributions of the Executive Board to adherence to the company values and applicable legal provisions and requirements for data protection. These include, for example, the support and provision of resources for the implementation of necessary data protection measures by the departments, the membership of a member of company management in the Data Privacy Management Committee (DPMC), communication measures for specific, current data protection topics, and also ensuring data protection requirements are implemented by the controllers in the other Ottobock companies.

All measures taken by the Executive Board and the resulting contribution they make towards strengthening the data protection culture are referred to collectively as the "tone from the top".

3. Consulting and mandatory involvement of the Data Privacy department

One of the Data Privacy department's core tasks is advising the Executive Board and the departments on aspects relevant to data privacy.[3]
In order to perform this consulting task adequately, the Data Privacy department must be involved in data protection-related matters. The goal is to ensure that preventive action can be taken where necessary and that planned decisions, communication measures and documents adhere with all applicable legal provisions and requirements.

[3] The statutory advisory task of the Company Data Protection Officer is not restricted by this task assignment.

Data protection-related matters on which the Data Protection department should be consulted include in particular

- the processing of complaints by the responsible departments for data protection-related topics,
- communication by the Corporate Communications department with representatives of the press on data protection focus topics and
- communication with public authorities on matters relevant to data protection by the Data Privacy department (as part of Cyber Security department).

The Data Privacy department may also be consulted by the departments in an advisory capacity in the course of developing principles and processes, and in the preparation and further development of internal organisational guidelines and work instructions relating to key data protection topics.

The definition of data protection focus topics is in the point 2. Depicted.

In future, in order to address compliance risks fully and in a timely manner, the Data Protection department must also be consulted and involved in the following matters, where these have data protection-related relevance:

- development of new markets,
- strategic company decisions,
- operational changes and
- planned integrations and outsourcing, which are in connection with the data protection focus topics (see point 2.).

4. Incentive system & improvement process

An incentive system plays an important role in promoting the development of a positive compliance culture. Various measures can serve to sustainably promote compliant behaviour. Global HR is in charge of designing the respective framework, choosing methods and implementing the corresponding measures.

The purpose of the improvement process is to establish guidelines and uniform processes for dealing with unintentional misconduct and deliberate or intentional violations of the rules.

Learning from mistakes, and particularly from unintentional misconduct, is an indispensable ingredient for Ottobock's success. Hence the "error culture" is an integral element of the compliance culture. Otto Bock's principle applies for unintentional compliance violations:

> *"Encourage others to correct errors, be proactive and make decisions."*
> [Otto Bock, 1944]

On the other hand, a zero-tolerance principle applies for intentional misconduct and deliberate compliance violations. Resolute action and sanctions are essential in these cases to reinforce and maintain our compliance culture at Ottobock.

The Global HR department has defined requirements for dealing with misconduct and deliberate data protection violations. These guidelines provide a uniform

framework for handling and determining disciplinary actions[4]. This serves as an objective and transparent assessment for third parties. While the circumstances always need to be examined on a case-by-case basis, a uniform framework is indispensable for the fair and just handling of comparable compliance incidents.

C. DATA PROTECTION OBJECTIVES

In the course of establishing compliance objectives, Ottobock differentiates between the following two aspects:

1. Definition of specific DPMS objectives

Firstly, the objectives pursued by the DPMS are defined and described. These objectives complement and promote Ottobock's business objectives. The primary objectives of the DPMS at Ottobock are:

1. To actively and efficiently manage data protection risks by creating methodological approaches for operational responsibilities.
2. To establish a framework to promote data protection-compliant behaviour
3. To promote and foster the data protection culture and to contribute to good corporate governance
4. To design an organisational framework for data protection-related topics
5. To contribute to the success of the company by enabling the sustainable use of data in order to improve our patient care products and services

The objectives of the DPMS are reviewed at regular intervals by the Data Privacy department and the Company Data Protection Officer, in consultation with the Executive Board, depending on the ongoing further development of the DPMS, and adjusted to the maturity level of Ottobock's DPMS.

2. Definition of data protection focus topics

On the other hand, Ottobock defines data protection focus topics. These are topics that may be associated with significant compliance risks, so the adequate and effective management of compliance risks will play a very important role. The data protection focus topics are considered in the context of the compliance programme and included in the data protection risk analysis. The DPMS defines the methodological and organisational framework for these data protection focus topics, which is applicable to each data protection focus topic. This enables the company to exploit interfaces and increase synergies.

The key data protection topics listed in the table below are considered essential for Ottobock. The department responsible for each data protection focus topic is also listed in the table. To ensure the compliance risks for these topics are taken into consideration properly, a **Data Protection Coordinator** has been appointed in the respective department for each topic (see point 8.).

Data protection focus topic	Responsible department
Data protection in the employment relationship	Global HR Management (Head of Global HR Management)
Data protection in information technology	Global IT (Head of Global IT)
Data privacy for Patient Care	Patient (Head of Patient Care)
Data protection in research and development	Global Research and Develeopment (Management of Research and Develeopment)
Data protection in Clinical Research	Clinical Research (Head of Clinical Research)
Data protection in market research	Global O&P Solutions (Head of Global O&P Solutions)
Data Protection, Marketing Technologies	Marketing Technologies (Head of Marketing Technologies)
Digital Health Solution data protection	Digital Health Solution (Head of Health Solution as part of Marketing Technologies)

The data protection focus topics are reviewed at regular intervals and updated as necessary. In part, this is because data protection-related topics also constitute the basis for the evaluation of compliance risks. Therefore, it is essential that the topics relevant for data protection are up-to-date, because Ottobock can use them as an appropriate basis for determining the compliance risk situation.

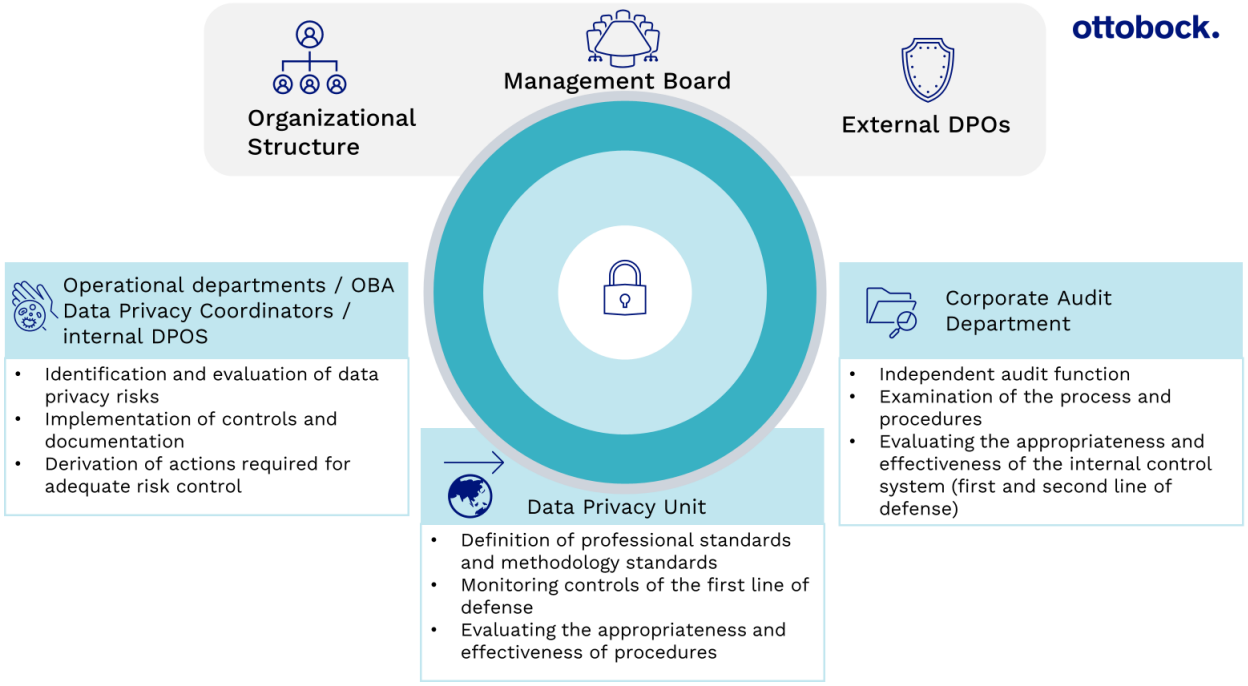
D. DATA PROTECTION ORGANISATION

Data protection concerns the entire company. An adequate governance structure in the company is an essential prerequisite for establishing and maintaining an effective compliance organisation. Ottobock bases its approach here on the three lines (of defence) model.

Overall responsibility for data protection management rests jointly with all the Executive Directors. Organisationally, the Data Privacy department is assigned to the CXO and Global IT, and it reports directly to the CXO. The CXO and Data Privacy department are assisted by the Data Protection Coordinators who are appointed for the data protection focus topics listed above.

In addition, Ottobock SE & Co. KGaA has appointed an external Company Data Protection Officer. The Company Data Protection Officer reports directly to the CXO. The Data Privacy department cooperates with the company's data protection officer. Corporate Audit performs an independent control function in this collaboration model.

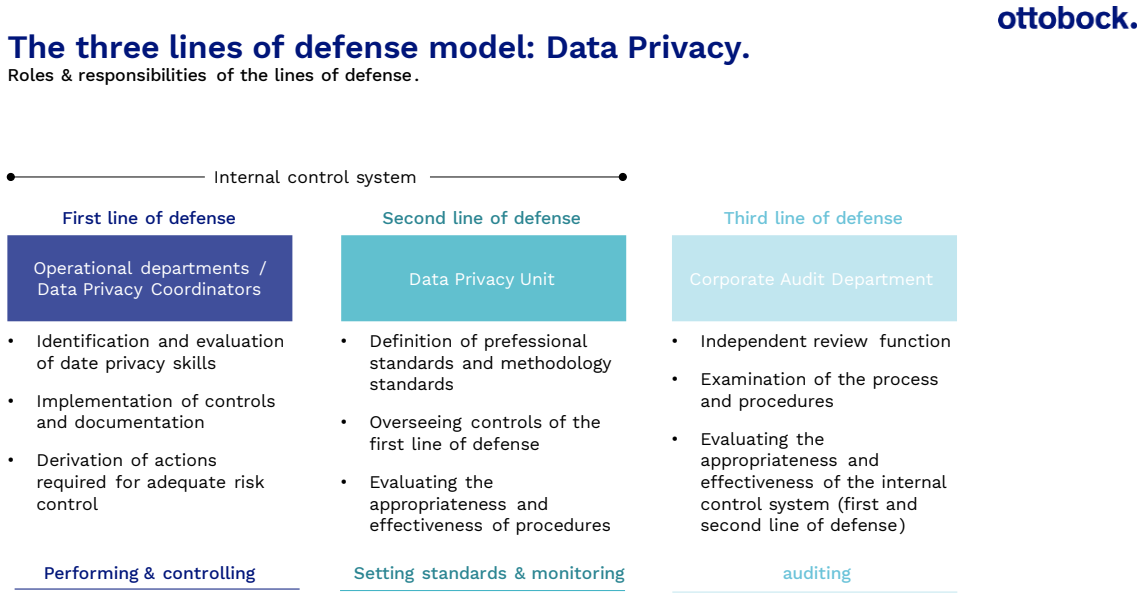
A simplified illustration of Ottobock's data protection organisation:



1. Model of the three lines (of defence) as the central organisational principle

The three lines (of defence) model establishes a structural framework for effectively controlling (data protection) risks in a company. It also serves as an important cornerstone for strengthening data protection awareness and data protection culture. In the following, the model is discussed from a data protection management perspective.

The introduction of the three lines (of defence) organisational principle at Ottobock is intended to help identify data protection risks at an early stage and manage them adequately and effectively across departments, for example, in order to prevent or minimise data protection incidents and any associated damage. In this context, the first and second lines (of defence) pursue a systematic, methodological approach in order to evaluate implemented procedures and measures to avert data protection risks and to identify the potential need for action.



Notice: Additional/other departments can also serve as the second line (of defence) (e.g., Risk Management or Legal Compliance). These have been omitted from the illustration since the model only represents the compliance perspective

In this model, each of Ottobock's existing organisational units is assigned to one of the three lines (of defence). Here each line performs different tasks: The manager and the employees of each operational department are responsible for identifying the relevant compliance risks in their department, and for controlling them adequately and effectively (*first line (of defence)*). The Data Privacy department is the *second line (of defence)*and sets minimum standards for adequate and effective compliance risk management. Furthermore, the Data Privacy department ensures that control structures are adequate and effective. The first and second lines (of defence) therefore form the internal control system (ICS). Corporate Audit forms the subsequent *third line (of defence)* as an independent auditing body. It reviews the overall structure of the ICS and therefore the first and second lines (of defence).

For the Company Data Protection Officer, the same applies accordingly as for the Data Privacy department.

2. Role & responsibility of the first line (of defence)

Each department in the first line (of defence) bears responsibility for its own data protection risks *(risk owner)* and performs the following tasks:

- Identifying data protection risks in the department based on the specifications for data protection standards established by the Data Privacy department.
- Managing data protection risks within the department by:
    - Specifying department-specific data protection standards (where required)

- Implementing processes, measures, work instructions etc., for example, maintaining relevant procedure directories, to ensure that relevant internal/external rules are followed. Identifying data protection risks, if applicable, in the course of conducting a data protection risk analysis and, if applicable, conducting data protection impact assessments.
    - Identification of data protection-relevant processes (see data protection-relevant topics under point 2.)
    - Establishing process-based control mechanisms and regularly performing (risk-based) reviews to determine whether the implemented measures are put into practice and thus achieve the intended objective. In principle, the departments can organise their own form of control documentation; however, it must include the following information as a minimum:
        - Name of the control
        - Description of the control
        - Underlying process/measure
        - Scope
        - Cycle
        - Result
        - Derived need for action
        - Date of the control and name of the person performing the control
    - Determining the course of action to be taken when potential areas for improvement are identified in the course of the monitoring processes.
    - Documenting the identified data protection risks, planned and implemented controls, as well as risk reduction measures
    - Reporting data on protection risks and risk-reduction measures to the Data Privacy department
    - Reporting as and when necessary to the Data Privacy department if significant new or changed data protection risks are identified and data protection violations are suspected or identified

3. Role & responsibility of the second line (of defence)

3.1 Data Privacy department

In the three lines (of defence) model, the Data Privacy department primarily performs the following tasks in the second line (of defence):

- Specification of data protection standards and, where applicable, initiating their implementation by the relevant departments to provide the first line (of defence) with expert support in the completion of their tasks
- Supervising and, if necessary, initiating the data protection risk analysis and, together with the Data Protection Coordinators,
- Support and advice for the departments during the implementation and subsequent validation of the results
- Advising the company's data protection officer on the planning and implementation of risk-oriented monitoring activities in order to assess whether the first line (of defence) has implemented appropriate procedures, measures and controls to adequately and effectively counteract the relevant data protection risks
- Advice to the departments on data protection-related matters

- Providing information to Corporate Audit so that Internal Auditing can fulfil its task as the third line (of defence)
- Liaising once per year with Corporate Audit to discuss the activities planned under the monitoring plan and the audit schedule, in particular to avoid time overlaps within the same topics
- Regular reporting to the Executive Board
- Reporting as and when necessary to the Executive Board if significant new data-protection risks arise, significant changes to data-protection risks are identified, or data-protection violations are suspected or confirmed
- Cooperation with supervisory authorities in coordination with the Company Data Protection Officer

.

3.2 External Company Data Protection Officer

The external Company Data Protection Officer performs the legal tasks of a data protection officer in accordance with Art. 39 GDPR:

- Informing and consulting Ottobock and its employees who carry out processing regarding their obligations under the GDPR and other data protection provisions of the European Union and/or the Member States
- Monitoring compliance with the GDPR, other data protection regulations of the European Union and/or the Member States and Ottobock's strategies for the protection of personal data, including assignment of responsibilities, awareness-raising and regular training of employees involved in processing operations and related reviews
- Upon request, advice in connection with the data protection impact assessment and monitoring of its implementation in accordance with Art. 35 GDPR
- Acting as a contact point for the supervisory authority on matters related to processing, including prior consultation pursuant to Art. 36 GDPR and, where appropriate, advising on any other matter.

In the performance of activities, the Company Data Protection Officer acts without instructions in accordance with Articles 38 and 39 GDPR.

4. Role & responsibility of the third line (of defence) – Corporate Audit

The task of the third line (of defence) is to review adherence to legal provisions and requirements, and to the specific internal rules that were implemented by the first and second lines of defence for this purpose. The third line (of defence) primarily uses internal audits for this purpose. These help to evaluate the adequacy and effectiveness of data protection and risk management in general, as well as the internal control system in particular.

As a rule, Corporate Audit conducts reviews as internal audits, subsequent to the completion of processes and also independently of processes.

An overview of the points of intersection (interfaces) between the Data Privacy department and Corporate Audit is found in Appendix: Interface agreement with the third , page L.5 ff.

5. Departmental responsibility of the Chief Experience Officer

The CXO is responsible for the Data Privacy department. This means that the CEO assumes management responsibility for the data protection organisation. Important fundamental decisions related to data protection management are made by this person, where applicable with the approval of other members of the Executive Board. The CXO is also responsible for the approval and company-wide publication of basic standards (such as this policy). A regular flow of information is ensured in the course of regular meetings and also ensured by the fact that the CXO is a member the Data Privacy Management Committee (DPMC). Furthermore, the CXO receives regular reports from the Data Privacy department (see point F.3) and the company's data protection officer.

6. Data Privacy department

6.1 Organisation

The Data Privacy department is part of the Cyber Security department, which carries out data protection tasks. It consists of the Head of Data Privacy and department employees who are responsible for data protection tasks.

6.2 Key tasks

The core tasks of the Data Privacy department in connection with the DPMS include the following in particular:

- Advising the departments on the establishment of data protection-related processes, guidelines and instructions
- Developing data-protection objectives for submission to and decision by the Executive Board
- Advising the Executive Board and departments on matters related to data protection (see point 3.)
- Development of measures to continuously strengthen the data-protection culture and raise awareness of data protection
- Promoting the exchange of information on legal changes and reforms in all data protection focus topics with the Data Protection Coordinators, and carrying out legal monitoring for data protection-related topics under its own responsibility
- Advising the Company Data Protection Officer on the performance of risk-oriented monitoring activities in his/her role as the second line (of defence) (see point 3)
- Assisting the Company Data Protection Officer in receiving and evaluating anonymous or confidential information and, if necessary, initiating further investigation or remedial action.
- Supporting the Company Data Protection Officer when a data protection violation is initially suspected; a recommendation is made to the Executive Board regarding internal investigations to be conducted by the third line (of defence) or by third parties (e.g., audit firms)
- Supporting the Company Data Protection Officer in regularly reviewing the need to adapt the training concept (methodological framework) for data protection training courses in cooperation with the HR department

- Making sure that training courses on data protection focus topics are held and conducting its own training programmes for the data protection-related topics under its own responsibility
- Initiating specific communication measures on data protection-related matters
- Regularly informing the CXO by sharing information in the DPC or in the course of regular meetings
- Reporting regularly to the Executive Board on data protection-related risks, activities and circumstances

To properly perform these core tasks, the employees of the Data Protection Management department also participate regularly in further education programmes (annually as a rule).

6.3 Rights and administrative powers

In order to perform the tasks associated with the DPMS, various rights and competencies have been assigned to the Data Privacy department by the Executive Board. The rights and competencies listed below apply within Ottobock SE & Co. KGaA.

Escalation right

The Data Privacy department has the right to submit data protection-related matters to the Executive Board and, where applicable, to the Supervisory Board for decision-making. They can do so via their regular reports, at any scheduled meeting, or on an ad hoc basis, depending on the relevance and urgency.

Right to information

The Data Privacy department has a comprehensive right to information on all data protection-related matters (for example in the form of a report), which is to be provided by the departments on request. If a department fails to provide essential information on request, the Data Privacy department has an escalation right (see above). The Data Privacy department is permitted to use the data and information solely for the purpose of fulfilling its data protection tasks and treats them strictly confidentially.

Supervision right (assistance to the data protection officer)

In accordance with the organisational principle of three lines (of defence), the Data Privacy department is obliged to support the Company Data Protection Officer in performing risk-based monitoring activities in their role as the second line (of defence) (see point 3). The above right of information is granted to the Data Privacy department for the performance of this task. In the course of this work, the Data Privacy department provides technical support to the Company Data Protection Officer. As needed, the departments can derive measures based on the results in order to further reduce the data protection risks. In addition, the results of the monitoring activities are regularly reported to the Executive Board by the Data Protection Management department and the Company Data Protection Officer.

Voting right

The Data Privacy department can recommend the renouncement of specific business or sales activities, business relationships or similar if they fail to comply with

applicable legal provisions and requirements or the internal Ottobock rules designed to implement these legal provisions. If a department fails to follow the recommendation, the Data Privacy department has the right to escalate (see above).

6.4 Organisational agreements between the 1st and 2nd lines of defence

The 1st and 2nd lines of defence enter into organisational agreements on the basis of the data protection organisation described under this point. To this end, the Data Privacy department defines data protection focus topics (point 8.) in order to ensure inter-organisational division and responsibility.

7. Company Data Protection Officer

The Company Data Protection Officer is responsible for the tasks and obligations assigned by law (see also Section 3.2).

These tasks include the following rights:

- **Escalation right**
- **Right to information**
- **Monitoring right**
- **Voting right**

In the performance of his or her tasks, the Company Data Protection Officer takes due account of the risk associated with the processing operations, taking into account the nature, scope, circumstances and purposes of the processing (Art. 39 para. 2 GDPR).

The Data Protection Management department supports the company's data protection officer in the performance of their duties.

The Company Data Protection Officer is bound by Union or Member State law to maintain secrecy or confidentiality in the performance of his or her tasks (Art. 38 para. 5 GDPR).

8. Data Protection Coordinators

As a rule, the head of the department is appointed as Data Protection Coordinator.

This appointment takes the form of a mutual agreement that is then included in the personnel file. The Data Protection Coordinator thus becomes part of Ottobock's data protection organisation. The role of Data Protection Coordinator may be further delegated hierarchically by department managers.

In the Data Privacy department, the Data Protection Coordinators serve as operational controllers for data protection-related matters. The main tasks of the Data Protection Coordinator are to initiate and coordinate the implementation of data protection requirements and to work towards the appropriate and effective design and continuous risk-oriented development of the DPMS in the respectively assigned data protection-related topic. The Data Protection department acts on behalf of the Executive Board and issues legal, methodological and organisational guidelines in this context. These guidelines are taken into account by the Data Protection Coordinators during department-specific implementation.

In particular, the tasks of the Data Protection Coordinator in connection with their assigned data protection-related topic include the following:

- Advising department employees on data protection-related questions associated with the data protection-related topic (serving as the first point of contact)
- Ensuring (new) legal requirements are accommodated and deficits are corrected
- Preparing standards, instructions, processes etc. to adhere to the requirements
- Helping to prepare, conduct and validate the data protection risk analysis
- Providing support with deriving measures, and overseeing review activities
- Providing support and/or making preparations when risk-oriented monitoring activities are performed by the Data Privacy department
- Implementing training and communication measures
- Supporting the Data Privacy department when dealing with suspected cases or analysing data protection breaches
- Reporting on a regular and, when needed, ad hoc basis, particularly on data protection risks and activities
- Participation in and reporting in the meetings of the Data Privacy Management Committee by invitation.

The Data Privacy department recommends the preparation of a data protection plan which encompasses the tasks of the respective Data Protection Coordinator for the data protection-related topic under their responsibility. This is generally prepared for one calendar year and can be updated on an ongoing basis. The Data Privacy department provides a template for this purpose.

The Data Protection Coordinator can delegate some of the tasks to employees in their department. The Data Privacy department advises and supports the Data Protection Coordinators and the employees assisting them in fulfilling their tasks. Furthermore, the Data Protection Coordinator role and performance of the associated tasks requires the following particular competencies:

- Unrestricted access rights and the right to information
- Advisory authority (including the right to provide mandatory training)
- A right to escalate to the Executive Board
- A right to implement control measures

The Executive Board shall assign the aforementioned competencies to the Data Protection Coordinators in documented form and provide them with the required resources. Where necessary, administrative powers shall be extended to or established for individual employees who assist the Data Protection Coordinators in specific tasks.

To properly perform their core tasks, both the Data Protection Coordinators and employees who assist them in their tasks regularly participate in further education programmes (annually as a rule). The respective Data Protection Coordinator is responsible for choosing suitable training programmes.

A regular meeting is scheduled between the Data Protection Coordinators and the Data Privacy department to discuss current issues and topics related to data protection. In particular, these meetings are used to discuss the following topics:

- The current status regarding data protection risks and implemented measures
- Current activities/focal points and insights
- Legal changes

Regular exchange of information with the specialist departments is a key success factor for strengthening the data protection culture (essential element of a DPMS) at Ottobock. Decentralised Data Protection Coordinators are appointed in order to ensure information is shared, awareness for compliance is raised, and the data protection culture permeates the entire company in an organised manner.

This will also serve to establish a broader basis for managing data protection risks. The departments in which Data Protection Coordinators are appointed are established in a first step on a risk-oriented basis for data protection-related topics (defined as sub-areas encompassing significant data-protection risks).

Additional, specific interfaces are found in the appendix.

9. Data Privacy Management Committee

The Data Protection Management Committee [hereafter: DPMC] acts as the central body of the data protection organization and meets quarterly. Under the chairmanship of the CXO, the CFO is also an integral part of the DPMC. The DPMC is an advisory body. Decisions are made and recorded by the Executive Board.

The DPMC consists of the following permanent members:

- CXO
- Head of Data Privacy
- Data Privacy Manager and other relevant employees of the Data Privacy department

An employee of the Data Privacy department is responsible for keeping minutes of the results of the meeting.

The Company Data Protection Officer may attend the meetings of the DPMC as a guest at any time, and any member may request this person's attendance.

The DPMC may invite guests such as regional presidents and department managers to its meetings.

In particular, core tasks of the DPMC include the following:

- Supervisory function:
  The Executive Board supervises the Data Privacy department through the Executive Director who is represented in the DPMC
- Planning and coordination function:
  Sharing information on current and planned activities, including monitoring activities
- Information function:
  Presentation of selected data protection topics, in particular with a high data protection risk and identification of need for action
- Decision preparation function:
  If decisions relating to data protection are necessary by the Executive Board, these are prepared by the DPMC or made directly by the Executive Board present at the DMPC

E. DATA PROTECTION RISKS

Like every company, Ottobock is exposed to various data protection risks. Compliance risks are risks that may arise from violations of the legal provisions and requirements by which Ottobock is bound, or from violations of the specific internal Ottobock rules and policies which support these legal provisions. A non-exhaustive list of possible risks is provided in the annex.

If data protection risks materialise, this can result in extensive damage for Ottobock, including penalties and other financial damage. In addition, personal liability claims against the governing bodies and a significant loss of reputation can also be indicators for data protection risks.

The departments play a central role in the management of data protection risks. Various legal provisions and requirements apply, depending on the field of activity. Each department is therefore exposed to a specific data protection risk situation and is responsible for identifying, controlling and minimising the corresponding data protection risks.

F. INTERNAL COMMUNICATION

1. Fundamental communication concept

The Data Privacy department communicates according to the following communication concept:

- Communication with the departments primarily takes the form of advice on data protection-related requirements and specific matters, in particular DPMS-related topics (including standards), (potential) suspected data protection violations and the data protection-related topics of anti-fraud and anti-corruption, both in regard to abnormalities within the scope of monitoring activities and to the corresponding need for action.
- In addition, the Data Privacy department conveys minimum standards and, in some cases, specific requirements associated with the DPMS or with other data protection-related matters. These take the form of directives

and other written requirements/guidelines (primarily the code of conduct, anti-corruption guideline, DPMS policy) or are conveyed via the intranet (for example contacts, description of the DPMS and links to relevant documents).
- The Data Privacy department regularly meets with the designated Data Protection Coordinators (twice a year as a rule) and contacts in the remaining departments, with whom key interfaces exist (see point 6.4). Thus ensures information is shared in both directions.
- In general, information is shared with the remaining departments in the second line (of defence) and with the entity responsible for the ICS on a quarterly basis (see point 3).

- Aside from the regular reporting channels (see point 3), communication with the Executive Board takes place within the framework of the Data Privacy Management Committee (see point 9.) and the regular meetings.

The Data Privacy department issues ad hoc reports to the relevant departments and/or the Executive Board as needed (for example, when data protection incidents occur). Sustainable data protection communication is also ensured by statements of the Executive Board, which are usually released in response to specific events (see point 0.). Furthermore, the company values and data protection principles in the Global Policy for Data Privacy and in the Code of Conduct are underlined by the personal foreword by Professor Hans Georg Näder as Chairman of the Board.

2. Training

In order for data protection risks to be identified in a timely manner and handled appropriately, it is vital that all employees are taught the required skills. Corresponding training has to be provided in this context. The following channels are used to impart the required knowledge:

- Basic training on data protection for new employees
- General data protection training measures controlled by the Data Privacy department
- Supplementary risk-specific data protection training in the individual data protection focus topics controlled by the Data Protection Coordinators (see point 2.).

The training measures are carried out by or in coordination with the Company Data Protection Officer in accordance with the provisions of Art. 39 (1) lit. b. GDPR.
In order to meet these requirements, the Company Data Protection Officer must develop a data protection training concept in cooperation with the Data Privacy department and in coordination with the HR department. It specifies a uniform framework in which the relevant training for each data protection focus topic (see point 2.) must be carried out. Responsibility for implementing the training concept and providing the training rests with the respective department managers.

The Data Privacy department advises the departments as needed in the implementation of the training concept, and conducts its own training programmes for specific topics (such as anti-corruption).

3. Internal reporting

The Data Privacy department informs the Executive Board in text form about the data protection activities of the past year and provides an outlook for the coming year. The annual report must be submitted to the Executive Board, who will forward it for informational purposes to the Management Board, the Chairman of the Supervisory Board, and the Audit Committee of the Supervisory Board.

In addition, the Data Privacy department regularly (quarterly, as a rule) reports on current data protection topics in the Management Board and in the course of the DPMC meetings (see point 9.).

Depending on the circumstances, ad hoc reports can be made to the CEO and/or the entire Executive Board outside of regular reporting.

The Data Privacy department also reports the results of the data protection risk analysis to the Corporate Risk Management department to support a consolidated examination of Ottobock's overall risk situation. The presentation of data protection risks is also discussed in order to avoid reporting inconsistencies.

In order to fulfil its reporting obligations, the Data Privacy department receives decentralised reports from the departments responsible for the data protection focus topics.

4. Communication with data protection authorities

Unless otherwise agreed in the context of interface agreements, communication with data protection authorities regarding matters relevant to data protection is handled by the Data Privacy department (as part of Cyber Security), assisted by the Company Data Protection Officer, depending on the circumstances.
Insofar as there is an actual threat of regulatory offence proceedings and criminal proceedings, contact with public authorities may also be handled by the Legal department. Legal has a right of first decision in this regard. In these cases, a report must be submitted to the Data Privacy Management department, should such be required for its activities.

G. EXTERNAL COMMUNICATION

1. Communication with persons affected

Communication with the data subjects for the implementation of data subjects' rights is handled by the external Data Protection Officer, supported by the Data Privacy department.

2. Further external communication

Communicating information to external parties

Third parties are provided with data protection-related information by the Data Privacy department on the Ottobock homepage. Aside from the code of conduct, reference is also given, for example, to the Ottobock whistleblower office.

Communication with suppliers

The general terms and conditions of purchase of Ottobock SE & Co. KGaA include an obligation for suppliers regarding certain matters relevant for data protection.

Communication with the German Public Prosecution Service, police, State Office of Criminal Investigation or Federal Office of Criminal Investigation (or foreign law enforcement agencies where applicable)

Communication with the aforementioned entities on matters relevant to data protection is always handled by the Legal department. The Data Privacy department, Data Protection Coordinators or other affected departments are included as needed, depending on the circumstances.

Communication with external investigators

Unless otherwise agreed within the scope of interface agreements, communication with external auditors regarding data protection-related matters is handled by the Data Privacy department (as part of Cyber Security), Group Tax, Environment, Health and Safety, Compliance Treasury (for the topic of money laundering prevention) or Regulatory Affairs, according to the circumstances. The Data Privacy department must be included in communication from the outset.

In the event that there is a substantial threat of regulatory offence procedures and criminal proceedings, contact with public authorities is handled by the Legal department (authority rests with Legal). In these cases, a report must be submitted to the Data Privacy department, should such be required for its activities.

Communication with the press

If data protection incidents or other circumstances relevant to data protection require communication with representatives of the press, the Data Privacy Management department must be consulted by the Corporate Communications department from the outset to review and coordinate the contents.

Communication with associations and workgroups

Communication in the course of association work or workgroups is generally handled by the departments. Regarding data protection-related matters, the Data Protection Management department and, depending on the circumstances, Data Protection Coordinators must be included from the outset.

H. DATA PROTECTION MONITORING AND ADAPTATION

The DPMS is subject to ongoing development and optimisation so that we can continuously adapt to current circumstances (such as entering new markets, new legal regulations) and learn from identified weaknesses to avoid them going forward. Regular monitoring and reviews of the DPMS serve to identify potential weaknesses.

The aim of data protection monitoring is to assess the adequacy and effectiveness of the DPMS as a whole. Assessments are carried out by a body that is not otherwise involved in the process, such as internal auditing or external auditors. Risk-oriented monitoring activities can also provide insights into the adequacy and effectiveness of the DPMS. One goal is to determine whether the measures implemented within the framework of the DPMS are suitable for the purpose, i.e., minimising data protection risks; another goal is to determine whether the measures are also effectively put into practice. Another aspect which needs to be monitored is whether the existing measures are sufficient, or whether specific risk-reduction measures are needed.

The DPMS must be reviewed at regular intervals. If the DPMS review shows that the measures implemented within the framework of the DPMS are not put into practice effectively or are only partially practiced, or that measures are lacking, a corresponding need for action must be derived.

In addition to identifying areas that require improvements in the course of data protection monitoring, any data protection violations that are noted also serve as grounds for reviewing the DPMS. This can help, for example, to determine whether systematic mistakes can be counteracted through specific measures within the DPMS. If a data protection breach is exposed, the Data Privacy Management department initiates a follow-up process. In this process, the affected departments analyse the causes of the violation, establish corrective actions and submit a report on implementation to the Data Privacy department.

I. PUBLICATION AND VERSION HISTORY

The data privacy management system policy with its appendices is available in electronic form on the intranet of Ottobock SE & Co. KGaA and in the business process management software used throughout the company.

Version	Date	Author	Notes
1.0	24-02-28	Matthias Horn	1. Version

This policy is reviewed regularly (at least annually) to ensure that it is up to date, and is amended if needed. If significant legal changes that affect the content of this policy come into effect between review cycles, the policy will be revised shortly after the changes enter into force.

Published by
Ottobock SE & Co. KGaA
Max-Näder-Str. 15
D-37115 Duderstadt, Germany

Contact

Matthias Horn
Data privacy lawyer
E-mail: privacy@ottobock.de

J. APPENDICES

This policy has various appendices. The appendices can be amended directly by the Head of Data Privacy. Insofar as the organisational agreements listed here are affected, they can be amended jointly by the Head of Data Privacy and the head of the affected department, respectively in coordination with the Executive Director responsible for the departments.

- Interface agreements with departments in the first line (of defence)
- Interface agreement for the third line (of defence)
- Overview of data protection risks
- Glossary

K. APPENDIX: ORGANISATIONAL AGREEMENTS WITH DEPARTMENTS IN THE FIRST LINE (OF DEFENCE)

Aside from the Data Privacy department, the departments in the first line (of defence) are responsible (see point 10) for various data protection-related topics (see point 8). The heads of these divisions shall appoint Data Protection Coordinators.

Data protection focus topic	**Responsible department**
Data protection in the employment relationship	Global HR Management (Head of Global HR Management)
Data protection in information technology	Global IT (Head of Global IT)
Data privacy for Patient Care	Patient Care (Head of Patient Care)
Data protection in research and development	Global Research and Development (Head of Research and Development)
Data protection in Clinical Research	Clinical Research (Head of Clinical Research)
Data protection in market research	Global O&P Solutions (Head of Global O&P Solutions)
Data Protection, Marketing Technologies	Marketing Technologies (Head of Marketing Technologies)
Digital Health Solution	Digital Health Solution (Head of Digital Health Solution as part of Marketing Solution)

I. Organisational agreement with Global HR-Management

The heads of the Data Privacy and Global HR Management department have drawn up an organisational agreement in accordance with the data protection organisation (point D.).

II. Organisational agreement with Global IT

The heads of the Data Privacy and Global IT departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

III. Organisational agreement with Patient Care

The heads of the Data Privacy and Patient Care departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

IV. Organisational Agreement with Global Research and Development

The heads of the Data Privacy and Global Research and Development departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

V. Organisational agreement with Clinical Research

The heads of the Data Privacy and Global Research and Development departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

VI. Organisational Agreement with O&P Solutions

The heads of the Data Privacy and Global Research and Development departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

VII. Organisational Agreement for Marketing Technologies

The heads of the Data Privacy and Global Marketing Technologies departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

VIII. Organisational agreement for Digital Health Solution

The heads of the Data Privacy and Digital Health Applications departments have concluded an organisational agreement in accordance with the data protection organisation (point D.).

L. APPENDIX: INTERFACE AGREEMENT WITH THE THIRD LINE (OF DEFENCE)

Berlin, March 2024

Interface agreement for Corporate Audit

The heads of the Data Privacy and Corporate Audit department have jointly defined and agreed on the following interfaces:

- Review of the adequacy and effectiveness of the implemented DPMS as part of audits by Corporate Audit. Corporate Audit can issue best practice notices in the course of the audit, and the Data Protection Management department can consult Corporate Audit regarding audit findings and questions that arise.
- Audit assignment encompassing the activities of the Data Privacy department as the second line (of defence). Corporate Audit can issue best practice notices in the course of the audit, and the Data Privacy department can consult Corporate Audit regarding audit findings and questions that arise.
- Regular data protection-related audits, e.g. in operational departments
- Regular intercommunication:
  - in the course of preparing the annual audit schedule and data protection monitoring plan; this will help, for example, to avoid time overlaps or to exploit synergies in on-site audits abroad,
  - on matters relevant for data protection within the scope of the CC; here the particular focus is on current risk-related circumstances and developments, and
  - to establish a consistent reporting to the Executive Board on matters relevant for data protection regarding compliance-related topics
- Provision of information by Corporate Audit on data protection matters such as identifying (new) data protection risks in the course of auditing activities, e.g.
  - findings made in the course of reviewing data protection-relevant matters
  - insights/information from internal investigations related to data protection
- provision of information by the Data Privacy department in cases where data protection activities reveal topics relevant for auditing or audit topics relevant for data protection, for example:
  - new legal requirements (and associated data protection risks) that should be included in the audit plan after implementation
  - suspected cases or indications of data protection incidents that need to be analysed and reviewed in more detail in the course of an internal investigation (source: whistleblower office among others), insofar as the investigation is conducted by Corporate Audit
- Handling of data protection incidents or suspected data protection cases:
  - The authority to handle data protection incidents or suspected data protection violations rests with the Data Privacy department.
  - In the event of a data protection incident, or in the event of an initial suspicion being confirmed, the Data Privacy department can make a recommendation to the Executive Board to commission an internal investigation by the Corporate Audit department or by a third party (such as an audit firm)

- Data Privacy is responsible jointly with the Company Data Protection Officer and/or Legal in the course of external investigations by public authorities (legal advice)
- Communication with public authorities on matters relevant to data protection, depending on the circumstances, is handled by Data Privacy, Legal, Regulatory Affairs, Group Tax, Treasury (for the topic of money laundering prevention)
- Data privacy and/or Legal assists in communication with the press or similar on situations relevant to data protection.

***

M. APPENDIX TO THE TRAINING CONCEPT: SAMPLE TRAINING PLAN

Type:	Content:	Depart-ments:	Reason for training	Target group:	Training me-thod:	Most recent training	Cycle	Date
Basic training	Data Protection	All depart-ments	Initial trai-ning	All employees	Online	Initial	Annually	Q1

N. APPENDIX: DATA PROTECTION RISKS

Violations of formal data protection law

- Missing or insufficient legal basis for the processing of personal data, e.g. consent, contract, legal obligation or legitimate interest
- Failure to consider the special requirements when processing data concerning health (Art. 9 GDPR)
- Lack of transparency regarding mandatory information/data protection declaration, Art. 12ff GDPR
- Missing entries in the processing register, Art. 30 GDPR
- Missing agreement on contract agreement or missing agreement for data transfers to service providers and partners
- Lack of guarantees in respect of transfers from third countries
- Missing notification of a data breach under Art. 33/34 GDPR
- Lack of appointment of Company Data Protection Officers
- Lack of data protection impact assessment

Breaches of substantive data protection law; image risks

- Loss, unintentional deletion or compromise of patient data
- In addition, special risks generally exist in the following cases:
    - Systems that process large amounts of data from individuals (CRM systems)
    - In the EU: Storage of personal data in so-called third countries, i.e. in countries outside of the EU or EEA. The same applies if personal data stored in the EU can be accessed from these countries.

Principles of risks in data protection

- **Large / small / without GDPR fine:** Art. 83 para. 4 and 5 GDPR defines two classes of fine for violations of different standards.

  ➔ **Up to 4 % of the global annual turnover can be imposed!**

- Some violations are not subject to fines. This is not only relevant because of the amount of a possible fine, but also because it also reflects the legislative assessment of which infringements are particularly serious and which may be slightly less relevant to risk.

- **Image risks:** Irrespective of any risk of fines, it is important to consider which actions may result in particular image risks (including in social media).

- **Standards with/without balancing:** In the event of violations of standards with a balancing option (such as the existence of a legitimate interest within the meaning of Art. 6 para. 1 sentence 1 (f) GDPR or the appropriateness of protective measures), there is often room for argumentation, so that an alleged violation is not completely clear from a legal point of view. In the case of standards without any possibility of balancing (such as the existence of consent or the documentation of the legitimate interest), however, the violation is undeniable and therefore the risk is even higher.

- **Claims for damages by data subjects:** According to Art. 82 GDPR, any person who has suffered material or immaterial damage as a result of a breach of this Regulation may be entitled to compensation against the controller or the processor

- Claims for damages **from contracting parties:** On the basis of contractual obligations relating to data protection, contracting parties may claim damages if a breach of contractual obligations exists.