proaxia
consulting

Privacy Policy, IT and Data Security

proaxia holding ag and its affiliates

Version	Changes	Responsible	Approval
1	Creation	Willy Wolf / 5.12.2013	Peter Lindtner
2	Update	Willy Wolf/23.2.2016	Peter Lindtner
3	Update	Willy Wolf/ 13.2.2018	Peter Lindtner
4	Update	Willy Wolf/4.5.2018	Peter Lindtner
5	Update	Willy Wolf/10.1.2019	Peter Lindtner
6	Update	Susanne Tiedtke/6.7.2022	Peter Lindtner
7	Update	Susanne Tiedtke/15.8.2023	Peter Lindtner
8	Update (CFO signatory change)	Bernd Spreter/29.02.2024	Peter Lindtner

proaxia holding ag
Alter Postplatz 2 | CH-6370 Stans
Phone +41 (0)41 618 00 12
www.proaxia-group.com

1 Preambel

The objective of this Privacy Policy is to provide guidance on the responsible handling of personal data in order to ensure the risk-conscious use of IT systems and applications. When handling personal data, the regulations of the Federal Data Protection Act (BDSG for Germany) as well as the General Data Protection Regulation (DSGVO for the EU) and the Federal Data Protection Act (DSG for Switzerland) must be complied with; for projects in other countries, the regionally applicable laws must also always be considered.

2 Scope

The Privacy Policy applies to all employees of proaxia holding ag. Employees of other branches, affiliates, freelancers and subcontractors are included in the scope of the Privacy Policy and are bound to data protection when working on projects of any proaxia entity.

3 Personal Data, Collection, Processing, Use and Disclosure - Principle of Data Economy

Personal data are individual details about the personal and factual circumstances of a specific or identifiable employee, customer or supplier. Personal data includes all information such as address, telephone number, date of birth, photos, employer, information on salary, assets, property, vacation planning, work behavior, work results, but also data without a direct personal reference, if it is possible to infer the associated person from them (personnel number or a PC user ID). In particular, this also includes data such as IP addresses and cookies.

Before any intended acquisition of personal data of employees, customers, suppliers or applicants or third parties in contact with proaxia, the person concerned shall be informed in advance, unless an exceptional case exists in accordance with the applicable law. In particular, the identity and contact details of the data controller, the purpose of the processing and, where applicable, the recipients or categories of recipients to whom personal data will be disclosed. If the personal data are disclosed abroad, information must also be provided about the receiving country and any guarantees to ensure an adequate level of data protection.

If the processing leads to automated individual decisions, the person concerned shall be informed and given the opportunity to comment on the outcome of the decision and to request a review of the decision by a natural person, unless an exceptional case exists in accordance with the applicable law.

In principle, personal data shall only be collected, processed, used and disclosed if the persons concerned have given their consent, if this is necessary for the fulfilment of contractual and pre-contractual obligations or if laws prescribe or permit this. They are to be collected from the data subject himself, unless the law provides for an exception. The data must be relevant and accurate for the purposes for which it is collected. They may only be processed for as long and to the extent required by the designated purpose or by law. Incorrect data must be deleted or corrected. Consent is only effective if it is based on the free decision of the data subject.

All relevant data and processing operations shall be documented in an inventory with regard to their permissibility under data protection law.

3.1 Special Categories of Personal Data

Personal data requiring special protection include information about health, privacy or racial or ethnic affiliation, genetic data, biometric data that uniquely identifies a natural person, data about administrative and criminal prosecutions or sanctions, and data about social assistance measures. This data is generally not stored. However, if personal data requiring special protection is processed, the corresponding consent must be obtained explicitly. If an employee becomes aware of special categories of personal data in the course of his or her project activities, he or she must maintain absolute silence about these facts.

3.2 Data protection impact assessment

If an intended processing of personal data may entail a high risk to the personality or fundamental rights of the person concerned, a data protection impact assessment must be prepared in advance.

If it is apparent from a data protection impact assessment that the planned processing would still result in a high risk to the personality or fundamental rights of the person concerned despite the measures envisaged, the opinion of the Federal Data Protection and Information Commissioner (hereinafter referred to as “EDÖB”) must be obtained in advance. The consultation of the EDÖB may be waived if the internal data protection advisor is consulted.

Data controllers are exempt from preparing a data protection impact assessment if they are legally obliged to process the data.

4 Right to information

In principle, proaxia grants all persons concerned a comprehensive and generally free right to information about, among other things, which personal data has been stored, as well as about the purpose and legal basis of the storage. The person concerned shall receive the information necessary to enable him or her to assert his or her rights under the applicable data protection law and to ensure transparent data processing. Information shall be provided without delay, but at the latest within one month of receipt of the request from a data subject. It must be ensured that appropriate security requirements are met when providing information, especially when using remote access systems for the data subject.

The person concerned may, provided that the legal requirements are met, request that his or her personal data be handed over in a commonly used electronic format and that the personal data be transferred to another data controller.

proaxia grants the right to correct incorrect data and undertakes to delete unlawfully stored data. Those affected have the right to call in the data supervisory authorities.

The relevant contact person at proaxia is the data protection officer Ms. Nicole Hoppe.

5 IT and data security rules

The most important technical and organizational measures implemented at proaxia are described below:

5.1 Access controls in all proaxia offices

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process Personal Data; persons are unauthorized if their activity does not correspond to tasks assigned to them. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by proaxia and do not get access to the personal data themselves.

All proaxia offices are secured by electronic access controls or security locks. The issuance and return of tokens or keys is monitored and documented by the respective administration. To protect against unauthorized access, proaxia does not install computers/servers in the offices. The implemented access control measures are checked for suitability by the data protection officer.

Further requested by SAP:

- Use video surveillance and alarm devices with reference to access area
- Have an access control process to restrict access to data centres / rooms where data servers are located
- Personnel without access authorization (e.g. technicians, cleaning personnel) must be accompanied all times

5.2 System Access Control

Data processing systems must be prevented from being used without authorization.

To prevent unauthorized persons form accessing any personal data all computers and remote access are password protected. A password is required after boot sequences, locking the system and when left a system even for a short period. Fingerprint unlocking is used for the Microsoft Windows operating system.

User access is assigned centrally. Each user has a unique ID and with an individual user password assigned for authentication.

The validity of user access is checked with the aid of an authorization concept, which is deactivated if the user leaves the company.

5.3 Access control to Personal Data

Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing.

Clearly defined rules determine - depending on the function of the respective person and based on a "need-to-know-basis" – the access person to the system.

Data carriers are stored in secured areas.

Each employee shall observe the following rules regarding data privacy and security defined in the IT regulation and password directive.

5.4 Data Transmission Control

It must be ensured that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

proaxia will adequately protect its personal data transiting networks against tampering and eavesdropping using a combination of network protection and encryption. No unprotected HTTP connections are allowed. TLS, the protocol underlying secure HTTPS connections, must be configured on the connecting server with a minimum of: minimum TLSv1.2 with forward secrecy, no known insecure cryptographic primitives like SHA-1 or RC4, minimum key size of 2048bits of RSA and 256bit for EC. Any other used protocols used must be secured and encrypted.

Personal data on data carriers shall be adequately encrypted.

5.5 Data Entry Control

It shall be possible retrospectively to examine and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed.

In the systems used internally by proaxia, there is both user identification and logging. Log files document who has accessed applications or documents, when and for how long. After a logout, a new logon via the user identification is mandatory. The internal allocation of roles and rights ensures that processing by employees can only be carried out in accordance with the client's instructions.

proaxia contractually obligates its subcontractors to process proaxia's personal data exclusively to the agreed extent and to delete or block the personal data at the end of the retention period.

5.6 Job Control

Personal Data being processed on commission shall be processed solely in accordance with the relevant contract with a client and the service schedule and instructions of the Controller.

Personal data that are processed on behalf of the customer (e.g. in the case of support contracts) must be processed in accordance with the customer's instructions. For this purpose, proaxia shall request the relevant guidelines from the client and inform the relevant employees.

In particular, the following rules are in force:

- Work performed only according to written instructions or contracts
- Clear areas of responsibility
- Authority to issue instructions
- Spot checks and controls
- Process the Personal Data received from different clients to ensure that in each step of the processing the Controller of Personal Data can be identified, so data is always physically or logically separated

5.7 Availability Control

Personal Data shall be protected against disclosure, accidental or unauthorized destruction or loss.

Proaxia creates back-up copies and stores them in a specially protected environment. Regular restore tests are performed from those backups.

proaxia only uses personal data within its organization and only abroad (support center of proaxia in Wroclaw), as far as this is necessary for the execution of the employment contract and the work processes and for no other purpose. Personal data is not disclosed to third parties, either for payment or free of charge.

Personal Data is not removed from proaxia's business computers or premises for any reason (unless such removal for business purposes has specifically been authorized before).

For the performance of services only authorized business equipment is used.

Whenever a user leaves its desk unattended during the day and prior to leaving the office at the end of the day, he/she must ensure that documents containing personal data are placed in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space. (clean desk).

For secure disposal of documents or data carriers containing personal data a process is implemented and the employees are instructed.

Proaxia has firewalls on network level to prevent unauthorized access to systems and services on network level.

Each computer system runs an up to date antivirus solution.

5.8 Organizational Requirements

The internal organization of proaxia shall meet the specific requirements of data protection. In particular, proaxia shall take TOMs to avoid the accidental mixing of Personal Data.

proaxia appointed a data protection officer. Questions regarding data protection may be asked at any time and should be addressed to:

Nicole Hoppe
Industriestrasse 176
CH-8957 Spreitenbach
Tel.: +41 (0) 56 418 20 80
Fax: +41 (0) 56 418 20 81
Mail: Datenschutz@proaxia-consulting.com

All employees commit in writing to maintain confidentiality in connection with personal data.
Personal Data received from different clients is processed in a way to ensure that in each step of the processing the respective client can be identified, so data is always physically or logically separated.

5.9 Disconnection control

proaxia points out to the customer that a three-tier SAP system landscape should exist. Except for the customer's ticket system, proaxia only works in development and test systems. Access to the customer's productive system will only be made on explicit instruction of the customer.

The internal systems of proaxia are separated into areas of responsibility. Thus, there are different SharePoint pages or addresses.

There is no direct contact or handling of personal data.

5.10 Data protection management

proaxia shall establish a procedure for the regular evaluation and review of the security of data processing, including incident response management which will be outlined in separate policies.

6 "Privacy by Design" and "Privacy by Default"

All software, hardware as well as the services must be configured in such a way that personal data is protected and the privacy of the users is preserved. For this, developers shall build the protection and respect of users' privacy into the structure of products or services that will collect personal data ("Privacy by Design"). In addition, it must be ensured that the highest security level is already in place when the product or service is placed on the market, in that all necessary measures for data protection and restriction of data use are activated by default, i.e. without user intervention ("Privacy by Default").

7 Obligation of data secrecy

According to the law, personal data must be processed in such a way that the rights of data subjects to confidentiality and integrity of their data are guaranteed. Therefore, all employees are only permitted to process personal data to the extent and in the manner necessary to perform the tasks assigned to them. Accordingly, all employees are prohibited from processing personal data in an unauthorized or unlawful manner or from intentionally or unintentionally violating the security of the processing in a manner that results in its destruction, loss, alteration, or unauthorized disclosure or access. Violations of data protection regulations may be punishable by a fine, monetary penalty or imprisonment, if applicable. If the data subject suffers material or immaterial damage as a result of the unauthorized processing of his or her personal data, a claim for damages may arise. Furthermore, a breach of confidentiality and data protection regulations constitutes a breach of employment contract obligations, which may be punished accordingly by proaxia.

The obligation of confidentiality shall continue indefinitely after termination of the employment relationship with proaxia.

All employees are instructed and regularly trained on these obligations.

8 Contact person

proaxia shall appoint a data protection officer. Questions regarding data protection may be asked at any time and should be addressed to:

Nicole Hoppe
Industriestrasse 176
CH-8957 Spreitenbach
Tel.: +41 (0) 56 418 20 80

Fax: +41 (0) 56 418 20 81
Mail: Datenschutz@proaxia-consulting.com

9 Responsible for data processing

Responsible for the data processing is:

proaxia holding ag
Alter Postplatz 2
6370 Stans
Switzerland
Phone +41 (0)41 618 00 12
www.proaxia-group.com

proaxia holding ag

Peter Lindtner
CEO

Bernd Spreter
CFO

Acknowledged and accepted:

……

Auszug aus BDSG:

§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

....

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

....

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschafts-zugehörigkeit, Gesundheit oder Sexualleben.

§ 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

....

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben.

....

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

....

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 Rechte des Betroffenen

Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

...

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Auszug aus der DSGVO

Art. 4 Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

„Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

„Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

„Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person

zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

„Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

1„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. 2Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

„Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

„genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige

Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

„Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

„Hauptniederlassung“ im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

„Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

„Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

„Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

„verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern ;

„Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

„betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist, diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

„grenzüberschreitende Verarbeitung“ entweder

eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

„maßgeblicher und begründeter Einspruch“ einen Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

„Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[1] ;

„internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 29 Bearbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des

Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

1Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. 2Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

1Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. 2Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

Art. 82 Haftung und Recht auf Schadenersatz

Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

1Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. 2Ein Auftragsverarbeiter haftet für den durch eine

Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Art. 83 Allgemeine Bedinungen für die Verhängung von Geldbussen

Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

1Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. 2Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10’000’00 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20’000’000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

1Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. 2In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. 3Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Auszug aus dem DSG

Art. 5 Begriffe

In diesem Gesetz bedeuten:

a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

b. *betroffene Person:* natürliche Person, über die Personendaten bearbeitet werden;

c. *besonders schützenswerte Personendaten:*

   1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,

   2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,

   3. genetische Daten,

   4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,

   5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,

   6. Daten über Massnahmen der sozialen Hilfe;

d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten;

f. *Profiling:* jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

g. *Profiling mit hohem Risiko:* Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

h. *Verletzung der Datensicherheit:* eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;

i. *Bundesorgan:* Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist;

j. *Verantwortlicher:* private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;

k. *Auftragsbearbeiter:* private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

Art. 6 Grundsätze

[1] Personendaten müssen rechtmässig bearbeitet werden.

[2] Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.

[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.

[6] Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

[7] Die Einwilligung muss ausdrücklich erfolgen für:

a. die Bearbeitung von besonders schützenswerten Personendaten;

b. ein Profiling mit hohem Risiko durch eine private Person; oder

c. ein Profiling durch ein Bundesorgan.

Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

[1] Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

[2] Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

[3] Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

Art. 8 Datensicherheit

[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

[2] Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

[3] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Art. 9 Bearbeitung durch Auftragsbearbeiter

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

[4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Art. 10 Datenschutzberaterin oder -berater

[1] Private Verantwortliche können eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

[2] Die Datenschutzberaterin oder der Datenschutzberater ist Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind. Sie oder er hat namentlich folgende Aufgaben:

a. Schulung und Beratung des privaten Verantwortlichen in Fragen des Datenschutzes;
b. Mitwirkung bei der Anwendung der Datenschutzvorschriften.

[3] Private Verantwortliche können von der Ausnahme nach Artikel 23 Absatz 4 Gebrauch machen, wenn die folgenden Voraussetzungen erfüllt sind:

a. Die Datenschutzberaterin oder der Datenschutzberater übt ihre oder seine Funktion gegenüber dem Verantwortlichen fachlich unabhängig und weisungsungebunden aus.
b. Sie oder er übt keine Tätigkeiten aus, die mit ihren oder seinen Aufgaben als Datenschutzberaterin oder -berater unvereinbar sind.
c. Sie oder er verfügt über die erforderlichen Fachkenntnisse.
d. Der Verantwortliche veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters und teilt diese dem EDÖB mit.

[4] Der Bundesrat regelt die Ernennung von Datenschutzberaterinnen und Datenschutzberatern durch die Bundesorgane.

Art. 12 Verzeichnis der Bearbeitungstätigkeiten

[1] Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.

[2] Das Verzeichnis des Verantwortlichen enthält mindestens:

a. die Identität des Verantwortlichen;
b. den Bearbeitungszweck;
c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
d. die Kategorien der Empfängerinnen und Empfänger;
e. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
f. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8;

g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

[3] Das Verzeichnis des Auftragsbearbeiters enthält Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, sowie die Angaben nach Absatz 2 Buchstaben f und g.

[4] Die Bundesorgane melden ihre Verzeichnisse dem EDÖB.

[5] Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.

Art. 22 Datenschutz-Folgenabschätzung

[1] Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

[2] Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

[3] Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

[4] Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind.

[5] Der private Verantwortliche kann von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 zertifiziert ist, oder wenn er einen Verhaltenskodex nach Artikel 11 einhält, der die folgenden Voraussetzungen erfüllt:

a. Der Verhaltenskodex beruht auf einer Datenschutz-Folgenabschätzung.
b. Er sieht Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Person vor.
c. Er wurde dem EDÖB vorgelegt.

Art. 23 Konsultation des EDÖB

[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, so holt er vorgängig die Stellungnahme des EDÖB ein.

[2] Der EDÖB teilt dem Verantwortlichen innerhalb von zwei Monaten seine Einwände gegen die geplante Bearbeitung mit. Diese Frist kann um einen Monat verlängert werden, wenn es sich um eine komplexe Datenbearbeitung handelt.

[3] Hat der EDÖB Einwände gegen die geplante Bearbeitung, so schlägt er dem Verantwortlichen geeignete Massnahmen vor.

[4] Der private Verantwortliche kann von der Konsultation des EDÖB absehen, wenn er die Datenschutzberaterin oder den Datenschutzberater nach Artikel 10 konsultiert hat.

Art. 24 Meldung von Verletzungen der Datensicherheit

[1] Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

[2] In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

[3] Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

[4] Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

[5] Er kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn:

a. ein Grund nach Artikel 26 Absatz 1 Buchstabe b oder Absatz 2 Buchstabe b vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet;
b. die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert; oder
c. die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.

[6] Eine Meldung, die aufgrund dieses Artikels erfolgt, darf in einem Strafverfahren gegen die meldepflichtige Person nur mit deren Einverständnis verwendet werden.

Art. 25 Auskunftsrecht

[1] Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

[2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt:

a. die Identität und die Kontaktdaten des Verantwortlichen;
b. die bearbeiteten Personendaten als solche;
c. der Bearbeitungszweck;
d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer;

e. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;
f. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;
g. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Artikel 19 Absatz 4.

[3] Personendaten über die Gesundheit können der betroffenen Person mit ihrer Einwilligung durch eine von ihr bezeichnete Gesundheitsfachperson mitgeteilt werden.

[4] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig.

[5] Niemand kann im Voraus auf das Auskunftsrecht verzichten.

[6] Der Verantwortliche muss kostenlos Auskunft erteilen. Der Bundesrat kann Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.

[7] Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt.

Art. 26 Einschränkungen des Auskunftsrechts

[1] Der Verantwortliche kann die Auskunft verweigern, einschränken oder aufschieben, wenn:

a. ein Gesetz im formellen Sinn dies vorsieht, namentlich um ein Berufsgeheimnis zu schützen;
b. dies aufgrund überwiegender Interessen Dritter erforderlich ist; oder
c. das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist.

[2] Darüber hinaus ist es in den folgenden Fällen möglich, die Auskunft zu verweigern, einzuschränken oder aufzuschieben:

a. Der Verantwortliche ist eine private Person und die folgenden Voraussetzungen sind erfüllt:
    1. Überwiegende Interessen des Verantwortlichen erfordern die Massnahme.
    2. Der Verantwortliche gibt die Personendaten nicht Dritten bekannt.
b. Der Verantwortliche ist ein Bundesorgan, und eine der folgenden Voraussetzungen ist erfüllt:
    1. Die Massnahme ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder der äusseren Sicherheit der Schweiz, erforderlich.
    2. Die Mitteilung der Information kann eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden.

[3] Unternehmen, die zum selben Konzern gehören, gelten nicht als Dritte im Sinne von Absatz 2 Buchstabe a Ziffer 2.

[4] Der Verantwortliche muss angeben, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt.

Art. 29 Einschränkungen des Rechts auf Datenherausgabe oder -übertragung

[1] Der Verantwortliche kann die Herausgabe oder Übertragung der Personendaten aus den in Artikel 26 Absätze 1 und 2 aufgeführten Gründen verweigern, einschränken oder aufschieben.

[2] Der Verantwortliche muss angeben, weshalb er die Herausgabe oder Übertragung verweigert, einschränkt oder aufschiebt.

Art. 60 Verletzung v on Informations-, Auskunfts- und Mitwirkungspflichten

[1] Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;
b. die es vorsätzlich unterlassen:
    1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder
    2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

[2] Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoss gegen Artikel 49 Absatz 3 dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

Art. 62 Verletzung der beruflichen Schweigepflicht

[1] Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.

[2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser Kenntnis erlangt hat.

[3] Das Offenbaren geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.