Unternehmensrichtlinien
Company-Regulations

Data Privacy-Compliance
Datenschutz-Compliance

Data Protection Regulation
Datenschutzrichtlinie

Spheros Germany GmbH

Drafted by

atarax

Luitpold-Maier-Str. 7
D-91074 Herzogenaurach

Consultant
Schlesinger
Version 0.1
27.06.2024

1 Preamble

The protection of personal data is a high-ranking value for Spheros Germany GmbH (from here on "Spheros", "us" or "our company"). Therefore, we are processing all personal data in compliance with applicable data protection law. As we are an organization with global relations, the relevant provisions regarding data protection are contained in several data protection laws. As a standard, we seek to implement data protection at least on a level as per the EU General Data Protection Regulation (GDPR). In addition, we must be aware, that further local provisions, such as the BDSG (German Data Protection Act) apply. However, all these rules are pointing at the same target: Keeping everyone´s personal rights and privacy protected.

2 Data Privacy and Personal Rights

2.1 Guiding Principles and Target

This regulation aims to implement a compliant standard for the protection of personal data at Spheros. The company´s goal to keeping the data of everyone protected whenever we are processing such data shall be safeguarded by implementing an adequate and legally compliant level of data protection as per the GDPR and any further data protection laws applying. However, where reference to the GDPR is made, this is to define a minimum standard and shall not be understood as to void potential local particularities.

Compliant data processing and an effective data privacy organization, therefore, are essential prerequisites to achieve our joint goals. In addition, we are subject to accountability as data privacy law comes with an inverse burden of proof. This means, that we are required to provide evidence for being compliant with data privacy requirements anytime. This, again, urges us to check this regulation, as well as the data privacy processes for effectivity on a regular basis. Consequently, we are implementing data protection as a management system.

In the presence of fines of -depending on the class of infringement- up to two or even four percent of our previous year´s turnover or of up to 20 million Euros (the respective higher amount applies), data privacy compliance is essential for our company. Fines must be avoided, as must be avoided damage for and any impairment of our goodwill. Besides that, complying with data privacy laws applying is also our responsibility towards all the persons entrusting their personal data to us.

Feeling and being responsible for data protection within his or her area of work **is every employee´s original task**. Awareness for data protection is an elementary precondition of any acting and is expected from everyone anytime. Should one be in doubt about any aspect of fata privacy, the data protection coordinator as well as the Data Protection Officer (DPO) are available anytime.

2.2 Scope of Applicability

This Regulation applies to all employees of Spheros Germany GmbH, at Gilching and Neu-brandenburg, but without any limitation regarding the location the labor is actually executed at.

2.3 Responsibility and Implementation

2.3.1 The Company Management

Being the instance responsible to decide on the purposes and means of personal data processing, respectively being the instance deciding on whether personal data is processed on behalf of Spheros, the company management is the bearer of responsibility when it comes

to data protection. The management ensures that the legally required data protection and the processes respectively required, are implemented and under continuous supervision. Should the company management ever be in doubt about an aspect of data protection, it will consult the Data Protection Officer (DPO)

2.3.2 The local Company Management

On the level of our local operations (sites), the local site management is responsible for the implementation of the requirements as per this regulation and as per locally applying data protection law, in addition. Although the GDPR provides a regime of data protection, which can be said to provide a good standard, it must be emphasized, that just following the GDPR alone does not necessarily have to result in a locally sufficient data protection.

2.3.3 Supervisors

Data protection is an original part of every management job. Every manager is responsible to safeguard data protection in the area which is under his or her supervision. Every manager and supervisor is obliged to safeguard that the personnel under his or her supervision is aligning to the requirements of data protection and under the obligation to execute respective checks. Every employee who identifies a weakness in regard of data security or data protection is obliged to report to his supervisor or to the DPO accordingly.

2.3.4 Data Protection Officer (DPO)

Spheros has implemented atarax Group as their DPO. Therefore, atarax Group executes the legal tasks of a DPO. In addition, atarax provides data privacy consultancy to managers and the staff-base. The Company Management and the DPO jointly define the strategic approach to data privacy compliance and promote this goal as they are supporting the data protection coordinator. The DPO, moreover, is responsible to check, whether the data privacy regulations applying are complied with. The DPO is directly reporting to the Company Management. The DPO is a direct subordinate to the Company Management (see company org-chart) but acts without being bound to instructions.

In case of queries or issues regarding data privacy, you are required respectively entitled to contact the DPO thru datenschutz@atarax.de anytime.

2.3.5 Data Protection Coordinator

The internal coordination of data privacy is the job of the data protection coordinator, who acts in the capacity of an interface between the organization and the DPO. The data protection coordinator is the one instance executing the practical implementation of data protection to the extent, data protection is not directly implemented by the DPO- The data protection coordinator may also be contacted thru datenschutz@atarax.de.

3 Basics and Definitions

3.1 Personal Data / Sensitive Data

The data protection laws are protecting so-called "personal data".

Personal data is any information allowing for the identification of a natural person. The subject of protection, therefore, is the human being.

Data of legal persons as such, e.g., the company „Spheros Germany GmbH", including its address, is no subject to protection under data protection law.

As soon as, e.g., a contact or an e-mail address consisting of name and surname is present, this is personal data. That does also apply for data in a business context. To assume personal data as present, it is already sufficient if a natural person can be identified, which means that information yet by its nature provides for the identification of the data subject. In the age of digitization, also aspects such as an identification by a user-ID or geo-location data must be considered.

Examples for **personal Data** are

- Contact data (name, e-mail-address, postal address, telephone number), marital status, birthdate, occupation, education, skill profile or physical appearance)
- Data which affects a context linked to a person, such as real estate or wealth.

Examples for **data linkable** to a person are für:

- A car´s license plate
- IMEI, IP-address

In addition, the GDPR names so-called sensitive categories of personal data. That data, for reasons of its special protective needs, may be processed under special conditions only. This is the exhaustive catalogue of sensitive data:

- Racial and ethnical origin
- Political opinion
- Religious or philosophical belief
- Union membership
- Health data
- Genetic and biometric data
- Data relating to a data subject´s sex life or sexual orientation.

Additionally, we shall treat bank-account and credit card- related data as sensitive data.

3.2 Accountability Requirements

Spheros is under an **accountability requirement**. This means, that e.g., in case of checks executed by a data protection authority, **we must be able to demonstrate** that we are processing personal data compliantly. **Therefore**, an effective **data protection management** is an elementary **part of our company-defense**. This organization is made up as described below:

Accountability requires, that all processes affecting personal data must be presentable in a revision-proof unaltered manner, as such is deemed to enable compliance with the accountability requirements mentioned. Therefore, the technical and organizational measures implemented are also there to keep information available.

3.3 Lawfulness of Processing/ Transparency

Whenever personal data is processed, the individual rights of the data subjects must be safeguarded. Therefore, personal data must be processed in a lawful manner, basing on due faith and in a way that is transparent to the data subject (which means that the data subjects must be able to understand how their data is processed). Every processing of personal data (including any transfer) requires to be based on one of the following legal bases (so-called "prohibition with the reservation of permission").

- **Processing of data for Contractual Purposes**
  Personal data relating to **customers, prospects** or any further **business partners** may solely be processed to initiate and execute the respectively underlying contract, which includes any accompanying measure of customer care as long as such is covered by the purpose of the contract. Data of **employees and job-applicants** may, to the extent objectively required, be processed for the (decision about the) initiation, execution and termination of the labor contract.

  Processing of personal data for **advertising purposes** is **always** subject to **special requirements**.
- **Processing of Data to comply with a legal Obligation**
  Personal data may be processed to comply with legal requirements (e.g., mandatory notifications to fiscal authorities or social insurance).
- **Processing of Data for the Protection of Vital Interests**
  Processing data for purposes of protecting vital interests of humans is permitted. Should, e.g., an emergency doctor be required, this person may be given all information required.
- **Consent-based Processing**
  Processing of data may also be consent-based. Every declaration of consent must be voluntary, actively and informed and, in addition, must comply with potential formal requirements. Otherwise, consent is invalid. Therefore, every text drafted to obtain consent must be checked by the DPO prior to the first use. Every declaration of consent, moreover, requires to be documented (which can be done physically or electronically). We must consider that no declaration of consent can be obtained bindingly thru an "Opt-Out" (for exception under non-European legislation, the DPO must be consulted).
- **Processing of data based on Legitimate Interest**
  Data may also be processed for purposes of a legitimate interest we may have (such as, e.g., legal claims), provided, that no interests worth protection and weighing heavier are standing against on the side of the data subject. Therefore, a documented balancing of interests is required. The DPO shall be involved in every balancing of interests for the legal dimension of it. Should legitimate interests of the data subjects affected turn out to weigh out our interest, the intended processing may not be executed.
- **Processing sensitive Data**
  Processing sensitive data requires a special legal basis (such as e.g., the originating from labor-law, social law, consent provided by the data subject or the requirement to defend a legitimate legal position).

Processing of data for contractual purposes (example)
Personal data of, e.g., suppliers, customers or further business partners may be processed to initiate and to execute the contract. Such does cover measures of customer care as long as such is directly related to the contract. This means that during the initiation of a contract, the data may be processed for purposes of the respective offer etc.

Should the data be made use of for **marketing purposes** instead, **special conditions apply**. You are obliged to always comply with our internal guidelines and rules on advertising/ marketing and to contact your supervisor or our DPO in every case of doubt.

Also, **data on our staff and job-applicants** may (only) be processed, if so objectively required to initiate, to execute or to terminate the individual labor relationship. Such, e.g., is the case

concerning the processing of personal data for payroll-purposes: Here, your employer must process your bank details to transfer your salary and your denomination to assess whether church tax applies (the latter is a basically German particularly).

3.4 Data Minimization

Every processing of personal data must be designed in a way that provides for the least possible extent of data being subject to processing. Moreover, it must be safeguarded that only the data objectively required is processed. Where data is collected both on a mandatory basis and a voluntary basis, the data shall be marked respectively. Where IT-systems are made use of it shall be checked, whether data may be anonymized or pseudonymized (both of which results in an interruption of the link to the data subject). Where anonymous data is present, data protection law does not need to be applied. All data must be correct and up to date and must be subject to correction, where required.

3.5 Purpose Limitation

For every processing of data, a legitimate purpose must be defined. Changes in such purpose are allowed within a narrow range only and subject to further conditions applying. This requires new processing activities as well as substantial changes to already existing ones to be issued notice on to the data protection coordinator or to the DPO.

3.6 Data Quality

All data which is subject to processing must be correct and up to data, anytime. This requires all adequate measures to be taken as to correct personal data regarding the underlying purpose of processing. However, there is -for instance- no requirement to permanently check, whether the data held in a CRM-system about business contacts, is up to data.

3.7 Storage Limitation and Deletion of Data

The GDPR´s basic principles of data processing are requiring the controller to delete personal data **as soon as the purpose of processing has terminated to apply or to exist**. This requirement, however, may appear to contradict retention obligation which may apply. In brief, the following may be mentioned for purposes of guidance:

- Personal data must be **deleted** as soon as it is no longer required as a part of the underlying processing activity,
- If no **legal retention requirement** applies anymore and
- If no further purposes to retain data (such as, e.g., retention agreed as per a civilian contract, evidence for purposes of retirement-claims or defense against lawsuits) apply.

The implementation of data deletion is the responsibility of the data owner. To get the respective requirements covered within IT-systems, turn to the IT-department for support. Spheros implements a data protection-compliant deletion concept.

3.8 Security and Confidentiality of Data

An adequate level of data security must be safeguarded. Personal data requires to be protected by adequate technical and organizational measures which have been subject to selection under a risk-perspective, anytime. Such shall provide for protection against unauthorized access, processing and transfer, loss, destruction, and impairment (availability, confidentiality and integrity of data).

The safety measures shall be chosen in the light of the technical state of the art and the cost of implementation. The accompanying risk-analysis is executed from the perspective of a data

subject. The kind, extent and purpose of the processing, the likelihood of danger and the effect of a (potential) damage must be considered. Sensitive data, for which job applicants' data shall count for this very purpose, shall be encrypted where possible.

All employees are obliged to duly consider the requirement of confidentiality regarding personal data. Every employee shall sign a commitment to data confidentiality – preferably when on-boarding with Spheros.

Every employee may be granted access to only the data the employee requires to fulfill his tasks ("need-to-know-principle"). Employees may not make use of personal data for their own private or commercial purposes, may not disclose such data to third persons and are required to protect personal data within their sphere of responsibility against unauthorized access, respectively against loss and are obliged to apply available instruments (such as, e.g. passwords, locking-away of documents, data protection compliant data disposal, clean-desk-principle, safe means of data transfer such as PDF).

That being mentioned, it shall expressly be emphasized that more specific rules, e.g., resulting from an information security regulation, may apply.

4 Data Protection Processes

4.1 Rights of the Data Subject

All the persons, whose data we are processing are entitled to so-called rights of a data subject and may exercise these rights with us anytime. Our own employee´s rights to data access are implemented by our HR-department.

Every employee is obliged to familiarize with these rights, with our respective processes and to act accordingly. The processes, however, may be subject to checks by way of dry-runs in the shape of "stress-tests" and may be checked for their effectivity and correctness.

Should you be contacted with a data subject´s right or should you be insecure whether a request you receive might be related to the exercising of a **data subject´s right**,

immediately notify datenschutz@atarax.de

Such requests may be received thru any channel (e-mail, phone call, surface mail, in-person-request) and may not in any case immediately be identified as of a data protection nature. In a significant number of cases, keywords such as „data access", "deletion" or data privacy are made use of.

The Process to implement Data Subjects´ Requests
We have defined a process for the implementation of all the rights a data subject is basically entitled to exercise as per the GDPR. The single process is considering the particularities of the respectively underlying right of the data subject:

4.1.1 Right to Data Access

Data subjects are entitled to be informed on whether data about them is subject to processing. Should this be the case, they are entitled to data access. If so requested, a free copy of this data must be provided. Should our rights or rights of third parties stand against, no copy must be provided or at least do we have to remove the respective data. Whether such interests are prevailing is subject to a legal check in any case.

4.1.2 Right to Data Rectification

Data subjects are entitled to have their data rectified upon request (e.g., if the data subject´s address has changed). Depending on the purpose of processing, the data subject may be

entitled to request completion if data in addition. Should the data have been disclosed to third parties (e.g., service providers), we are obliged to notify all the recipients, if not such is impossible or inappropriate.

4.1.3 Right to Data Deletion („Right to be forgotten")

Data subjects are entitled to have their data immediately deleted, provided that the data is no longer required for the underlying processing purpose, if the consent the processing is based on should have been revoked or if contradiction should have been declared and if -as a further condition- no **retention obligation** stands against data deletion. Whenever data must be deleted, **all the recipients of the data must be informed** about the request. The latter does also mean a requirement to delete links to such data and data-copies which should have been taken.

4.1.4 Right to have the Data Processing restricted

Data subjects are, entitled to request a restriction of the processing of their data. This, e.g., affects cases where the correctness of the data is disputed, where the processing has been executed unlawfully or where legal claims are subject to implementation or defense. The same applies in case the data should be processed to protect the rights of natural or legal third persons. Third parties who should have received the data must be informed accordingly. Whenever a data subject successfully requests to have the processing of its data restricted, we must ensure that the data subject is informed prior it any lift of such restriction.

4.1.5 Right to Data Portability

Data subjects are entitled to having their data transferred in a "structured, usual and machine-readable format". This right to data portability, however, does only affect data the data subject itself has provided, that such data is subject to automated processing and that the legal basis of processing is the data subject´s consent or a contract. The right to data portability does not apply, where rights and freedoms of other persons are affected.

4.1.6 Right to Contradiction

Data subjects are entitled to contradict against a processing for reasons which originate from their special situation, when data is processed basing on a balancing of interests. In such case we are no longer entitled to process the data, if we are not able to name compelling reasons worth protection which are outweighing the data subjects´ interests. The same applies if processing serves the implementation or defense of legal claims. Which of the interests outweighs the other, is always a question which must be answered on a case-by-case basis and in the presence of legal expertise.

Additionally, data subjects are entitled to contradict against a processing of their personal data if such processing is for purposes of direct marketing (also for purposes of profiling in relation to direct marketing). In such case the data may no longer be processed for purposes of direct marketing.

4.1.7 Right to withdraw consent

Every declaration of consent may be revoked anytime, without reasons having to be named, without a specific cause and without any form being required. A data processing which was based on such consent, may then no longer be executed. Any withdrawal of consent requires immediate implementation – also within all IT-systems. In addition, withdrawing consent must be as easy as declaring consent was. This requires us to implement the easiest possible option to withdraw consent, where the data subject´s perspective is the scale. When consent shall be withdrawn, we may especially not ask for any additional data or reason.

4.2 Information Requirements

GDPR requires comprehensive information about the processing of their personal data to be issued to data subjects. This requirement does not only affect the processing of customers´ data but does also exist regarding our own employees as these are data subjects, as well.

Whenever information requirements are implemented, all interfaces to any groups of data subjects (customers, prospects, employees, etc.) must be considered, to safeguard that all transparency requirements are duly implemented both online and offline.

Concerning the content, form and moment of information, the respective requirements are immediately resulting from Art. 13 and 14 of the GDPR. Therefore, privacy information must be drafted individually and, on a case-by-case basis. Especially here, local data protection law may know additional requirements which must also be implemented.

4.3 Automated Decisions and Profiling

Data subjects may not be made subject to a fully automated decision with legal effect on them or which may substantially impair them (so-called profiling, e.g. scoring). Automated decisions, which are legally required or implemented basing on a data subject's´ express consent and which are executed for purposes of contracting might, however, be possible.

It must be safeguarded that a human being interferes with the process upon the data subjects´ request. The data subject, in addition, must be able to present his own opinion and to challenge the decision ("right to remonstration"). Automated decisions may basically not be based on a processing of sensitive personal data (exception: With consent present).

4.4 Data Breach Notification

If data privacy is subject to violation, ("**data breach**"), an obligation to notify a data protection supervisory authority and/ or data subjects may be present. It is decisive, whether the incident is presumably resulting in a risk for the rights and freedoms of the data subject.

If a notification is required, the competent data protection supervisory authority must be **notified asap, which is no later than within 72 hours**. Our processes must be followed.

Never notify a data protection supervisory authority or a data subject yourself.

Immediately notify datenschutz@atarax.de about any (potential) data breach.

4.5 Outsourcing / Data Protection Agreements / NDAs

A data protection agreement is required, whenever service providers are processing personal data on our order. Data protection contracts often are named "DPA", DPC" or data processing contract. Where such contract is required, it **must be entered into prior to data processing**. It is required to provide proof of a careful selection of service providers if requested by an authority. This is, because we are obliged to safeguard data protection at our data processing outsourcing partners as we are acting in the capacity of a data controller. In addition, data processor must be checked at regular intervals.

Conditions given, we must consider particularities that come with a data processing in so-called third countries located outside the EU, respectively the European Economic Area (EEA). For reasons of its complexity, any respective data transfer must be subject to a previous check involving the DPO. Comparable contract requirements may also be present if only non-EU entities/ data subjects are affected by the processing. Also, in such case the DPO shall be contacted for compliance purposes.

Even if no DPA is mandatory, protecting information is required. This usually is implemented by a Non-Disclosure Agreement (NDA). Every employee is required to familiarize with and to act as per the respective work order on DPAs and NDAs Spheros may issue.

4.6 Records of Processing Activities (RoPA)

The records of processing activities are a central document to provide evidence of a compliant data processing. This is due to accountability requirements and documentation is kept in electronic form. The mandatory content is stipulated by the law and is subject to demand-oriented reviews which use to be executed annually. Processing activities, for example, are our customer data base or vacation planning.

4.7 Data Protection Impact Assessment (DPIA)

When a processing of data comes with a certain above-average risk, a DPIA is mandatory. The respective requirement shall be checked whenever a new processing is started and when an existing one is subject to change. A typical challenge is the risk-assessment – given the ever-expanding digitization. Whether a DPIA is required, can also be assessed by checking the local data protection supervisory authority's´ lists of DPIA-requirements and may be decided upon by considering the measures implemented for purposes of limiting the potentials of damage and occurrence when it comes to infringements of the rights and freedoms of data subjects. If a DPIA should uncover a residual risk even though preventive measures have been taken, the data protection supervisory authority must be consulted.

4.8 Data Protection Checks

Compliance with regulations on data protection and data protection laws applying are subject to regular, documented checks. The supervisory authority is entitled to check whether the regulations are complied with. In addition, the DPO executes internal checks to safeguard that both the effectivity and the adequacy of the data protection management system are ensured. The data protection coordinator is usually involved into such checking activities.

4.9 Definition and permanent Improvement of the technical and organizational Measures

The processing of personal data must be subject to adequate technical and organizational measures providing for its security, where both the risk of processing and the state of the art of tech must be considered. This requires data protection and information security to cooperate, risks to be identified and information- and IT-security-measures to be derived.

The risk-process must consider the protective requirements of the data processed concerning availability, confidentiality, and integrity. To be able to execute the data processing by the technical state of the art, a PDCA-cycle which uses to provide for a continuous optimization of measures is required and systems must be designed to be resilient. Resilience, however, means the ability to withstand impacts in case of irregularity, fault, and high operative workload.

During the regular reviews of the RoPA, a risk-analysis is executed per processing activity. Security-measures must be implemented on a processing-specific basis. Crucial processing activities are subject to the implementation of special technical and organizational measures, as well as of organization.

4.10 Ensuring "Privacy by design / by default"

The terms of ‚privacy by design' and ‚privacy by default' mean, that applications and systems are (data protection by design) designed to ensure data protection by consequently considering data protection requirements (e.g., by data minimization/ pseudonymization, transparent functions, deletion routines). Also default settings shall provide for data protection (privacy by default). Implementing these requirements comes with the need to consider data protection at an early stage of every project an requires involving the DPO as early as possible and eventually to even consult further (IT-) experts.

4.11 Sensitizing the Staff base

By sensitization measures which are provided by or at least created under the supervision of the DPO and which shall take place at least annually, the employees are sensitized for data protection requirements. Sensitization measures (which preferably are provided by the DPO) shall also be implemented whenever staff should occupy a different position or if data processing substantially changes.

5 Final Regulations

This regulation consists of its text, annexes and the workflows attached which are an integral part of it. This regulation is drafted in an English and a German language version. In case of any inconsistency or deviation, the German language version shall take precedence.

This regulation is in force from the date of its publication. This regulation leaves other regulations unaffected where it does not explicitly make an alteration or takes precedence.

Compliance with this regulation is every employee´s obligation in the labor relationship. Infringements may be punished by consequences with may involve but are not limited to measures as per labor law.

Subject to their individual applicability, the rules set by this regulation are outlasting the labor relationship. The rules set by this regulation, moreover, are leaving further rules applying at Spheros unaffected if such rules are not expressly changed by this regulation or where this regulation claims a higher priority. By publication of this regulation any former versions shall be deemed outdated.

Rechtsgebiete – Geschlechtsneutrale Formulierung
Auch wenn es Überschneidungen mit anderen Rechtsgebieten, wie z. B. Zivil-, Wettbewerbs-, Arbeits- oder Betriebsverfassungsrecht gibt, bitten wir um Ihr Verständnis, dass wir uns aus rechtlichen Gründen auf datenschutzrechtliche Belange beschränken. Allein aus Gründen der besseren Lesbarkeit werden generisch-maskuline Formulierungen verwendet.

1 Vorbemerkung

Der Schutz personenbezogener Daten ist uns, der Spheros Germany GmbH, (i.F.: „Spheros", „unser Unternehmen", „wir") sehr wichtig. Deshalb verarbeiten wir alle personenbezogenen Daten gemäß anwendbarem Datenschutzrecht. Da wir eine Organisation mit globalen Verbindungen sind, sind die relevanten datenschutzrechtlichen Vorschriften in einer Reihe von Datenschutzgesetzen zu finden. Als globalen Standard verfolgen wir den Ansatz, den Datenschutz mindestens auf dem Niveau der EU-Datenschutz-Grundverordnung (DSGVO) umzusetzen. Ergänzend muss unsere Aufmerksamkeit dem Umstand gelten, dass weitere lokale Vorschriften anwendbar sein können. Alle Vorschriften haben dasselbe Ziel: Die Persönlichkeitsrechte und die Privatsphäre jedes Menschen zu schützen.

2 Datenschutz und Persönlichkeitsrecht

2.1 Leitgedanke und Ziele

Mittels dieser Richtlinie soll ein einheitlicher Standard für den Schutz personenbezogener Daten bei Spheros geschaffen werden. Dem Unternehmensziel, das Persönlichkeitsrecht aller zu schützen deren Daten wir verarbeiten, wird durch die Schaffung eines angemessenen und rechtskonformen Datenschutzniveaus im Sinne der DSGVO und der sonstigen anwendbaren Datenschutzgesetze entsprochen. Wo diese Richtlinie insofern die DSGVO in Bezug nimmt, erfolgt dies zur Gewährleistung eines Minimalstandards und nicht im Sinne des Ausschlusses des Erfordernisses zur Berücksichtigung lokaler Gesetze.

Die ordnungsgemäße Datenverarbeitung und eine wirksame und effektive Datenschutzorganisation wiederum sind zentrale Voraussetzungen für die Erfüllung unserer Ziele. Zudem trifft uns aufgrund der umgekehrten Beweislast im Datenschutzrecht eine Rechenschaftspflicht. Das bedeutet, dass wir jederzeit in der Lage sein müssen unsere Datenschutzkonformität nachzuweisen. Daher müssen wir diese Richtlinie wie auch unsere Datenschutzprozesse regelmäßig auf ihre Wirksamkeit hin prüfen.

In Anbetracht möglicher Bußgelder von -je Verstoß- zwei bis vier Prozent unseres gesamten Vorjahresumsatzes oder von bis zu 20 Mio. Euro (der jeweils höhere Betrag gilt) ist dies elementar für unser Unternehmen. Bußgeld-, Schadenersatz und Imageschäden müssen verhindert werden. Die Einhaltung der datenschutzrechtlichen Vorschriften ist zudem unsere Verantwortung gegenüber allen, die uns ihre Daten anvertrauen.

Die **Selbstverantwortung jedes einzelnen Mitarbeiters** in seinem Arbeitsbereich und das Bewusstsein für einen gelebten Datenschutz sind elementar und werden stets und bei allen Tätigkeiten erwartet. In Zweifelsfällen stehen Datenschutzkoordinatoren und Datenschutzbeauftragter mit Rat und Tat zur Seite.

2.2 Anwendungsbereich

Diese Richtlinie gilt für alle Mitarbeiter an den Standorten Gilching und Neubrandenburg, ungeachtet des Ortes, an dem die Arbeitsleistung tatsächlich erbracht wird.

2.3 Verantwortlichkeit und Umsetzung

2.3.1 Unternehmensleitung

Die Unternehmensleitung ist als diejenige Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet oder eine solche im Auftrag vornehmen lässt, für diese verantwortlich. Sie stellt sicher, dass der gesetzlich erforderliche

Datenschutz sowie die relevanten Datenschutzprozesse umgesetzt und auch durch ausreichende Kontrollmechanismen regelmäßig überwacht werden. Bei Unklarheiten zieht sie den Datenschutzbeauftragten („DSB") beratend hinzu.

2.3.2 Das Management der lokalen Einheiten

Auf Ebene unserer einzelnen lokalen Gesellschaften ist die örtliche Geschäftsführung für die Umsetzung der Anforderungen nach dieser Richtlinie und des örtlich zu berücksichtigenden Datenschutzrechts verantwortlich. Wenngleich die DSGVO für einen Datenschutz steht, der auch global betrachtet als guter Standard gelten kann, muss deutlich hervorgehoben werden, dass eine Orientierung an der DSGVO nicht zugleich auch dazu führen muss, dass zugleich auch ein nach örtlichen Vorschriften ausreichender Datenschutz gegeben ist.

2.3.3 Fachverantwortliche / Führungskräfte

Datenschutz ist ein integraler Bestandteil jeder Führungsaufgabe. Jede Führungskraft trägt die Verantwortung für die Sicherstellung des Datenschutzes in ihrem Aufgabenbereich. Jede Führungskraft ist verpflichtet, die Einhaltung der Vorschriften zum Datenschutz durch die ihr nach- und zugeordneten Mitarbeiter sicherzustellen und regelmäßig zu kontrollieren. Jeder Mitarbeiter, der Schwachstellen im Bereich der Datensicherheit oder des Datenschutzes erkennt, ist verpflichtet, diese seiner Führungskraft oder dem DSB zu melden.

2.3.4 Datenschutzbeauftragter

Spheros hat die atarax Unternehmensgruppe als DSB bestellt. Als DSB übernimmt atarax die gesetzlichen Aufgaben. atarax berät zudem Führungskräfte und Mitarbeiter zum Datenschutz. Der DSB legt mit der Geschäftsleitung das strategische Vorgehen zum Datenschutz fest und unterstützt diese sowie den Datenschutzkoordinator. Dem DSB obliegt ferner die Kontrolle der Einhaltung der Datenschutzvorschriften. Der DSB berichtet unmittelbar der Unternehmensleitung. Der DSB ist der Unternehmensleitung direkt unterstellt und agiert gemäß den gesetzlichen Bestimmungen weisungsfrei (vgl. Organigramm).

Sie können sich bei Fragen und Problemen mit Datenschutzbezug jederzeit an den Datenschutzbeauftragten unter datenschutz@atarax.de wenden.

2.3.5 Datenschutzkoordinator

Die interne Koordination des Datenschutzes liegt beim Datenschutzkoordinator, der als Schnittstelle zum Datenschutzbeauftragten fungiert. Hier erfolgt die praktische Umsetzung der Datenschutzthemen, soweit nicht der Datenschutzbeauftragte unmittelbar tätig wird. Er ist unter datenschutz@atarax.de erreichbar.

3 Grundsätze und Begriffe

3.1 Personenbezogene Daten / Sensible Daten

Vom Datenschutzrecht werden sogenannte „personenbezogene Daten" geschützt.

Personenbezogene Daten sind alle Informationen, mit denen man die Person identifizieren kann. Geschützt ist nur die natürliche Person, also der Mensch.

Daten juristischer Personen als solcher, z. B. die Firma „Spheros Germany GmbH" einschließlich ihrer Anschrift unterliegen nicht der Anwendung des Datenschutzrechts.

Sobald beispielsweise ein **Ansprechpartner** oder eine E-Mail-Adresse bestehend aus Vor- und/oder Nachnamen vorliegt, ist ein **Personenbezug** gegeben. Dies gilt **auch** wenn **Daten im beruflichen Kontext** verwendet werden. Für den Personenbezug reicht es schon aus, wenn die Person identifizierbar ist, also anhand anderer Merkmale als der Daten selbst bestimmt werden kann. Im Zeitalter der Digitalisierung ist damit beispielsweise auch an die Identifizierung der Person mittels einer User-ID oder Standortdaten zu denken.

Beispiele für **personenbezogene Daten** sind:

- Kontaktdaten (Name, E-Mail-Adresse, Anschrift, Telefonnummer), Familienstand, Geburtsdatum, Beruf, Schulbildung, Fähigkeitsprofil, Aussehen
- Daten, die einen Sachverhalt bezeichnen, der mit einer Person verbunden ist, wie z. B. Grundbesitz oder Vermögen

Beispiele für **personenbeziehbare Daten** sind:

- KFZ-Kennzeichen des Autos
- IMEI-Nummer, IP-Adresse

Die DSGVO kennt zudem **besondere Kategorien von personenbezogenen Daten**. Diese unterliegen wegen ihrer besonderen Sensitivität einem strengeren Schutz und dürfen nur unter besonderen Voraussetzungen verarbeitet werden. Sensitive Daten sind:

- Rassische und ethnische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- Gesundheitsdaten
- genetische und biometrische Daten
- Daten zum Sexualleben oder der sexuellen Orientierung

Darüber hinaus behandeln wir Bank- und Kreditkartendaten als besonders schützenswert.

3.2 Rechenschaftspflicht

Spheros trifft eine Rechenschaftspflicht. Dies bedeutet, dass wir z.B. bei Prüfungen durch die Datenschutz-Aufsichtsbehörde in der Nachweispflicht sind. **Wir müssen nachweisen, dass** wir die Grundsätze der Datenverarbeitung beachten. **Daher** ist ein wirksames und nachweisbares **Datenschutzmanagement für die Unternehmens-Verteidigung** elementar. Diese Organisation folgt nachstehendem Ablauf:

Die Rechenschaftspflicht erfordert, alle Vorgänge um die Verarbeitung personenbezogener Daten -bisweilen revisionssicher- nachvollziehbar zu machen, um im Zweifel die Erfüllung der datenschutzrechtlichen Pflichten nachweisen zu können. Insofern erstrecken sich die technischen und organisatorischen Maßnahmen zum Datenschutz insbesondere auch auf die Verfügbarhaltung integrer Informationen.

3.3 Rechtmäßigkeit der Verarbeitung / Transparenz

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte der betroffenen Personen gewahrt werden. Daher müssen alle Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise, also „transparent", verarbeitet werden. Jede Datenverarbeitung (auch -Übermittlung) muss durch eine der folgenden Rechtsgrundlagen gedeckt sein (sog. „Verbot mit Erlaubnisvorbehalt").

- **Datenverarbeitung für eine vertragliche Beziehung**
  Personenbezogene **Daten von Interessenten, Kunden** oder anderen **Geschäftspartnern** dürfen zur Vertragsanbahnung (z.B. Angebote) und -Erfüllung verarbeitet werden, auch zur Betreuung des Vertragspartners im Zusammenhang mit dem Vertragszweck. **Mitarbeiter- (bzw. Bewerber-) Daten** dürfen, soweit objektiv erforderlich, für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses verarbeitet werden.

  Die Verarbeitung für **Werbung** unterliegt immer **besonderen Voraussetzungen**.
- **Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung**
  Personenbezogene Daten dürfen zur Erfüllung von Rechtspflichten verarbeitet werden (z. B. Meldungen an Finanzamt / Sozialversicherungsträger).
- **Datenverarbeitung zum Schutz lebenswichtiger Interessen**
  Die Verarbeitung zum Schutz lebenswichtiger Interessen von Menschen ist gestattet. Wird z.B. ein Notarzt benötigt, dürfen diesem die erforderlichen Angaben gemacht werden.
- **Datenverarbeitung aufgrund von Einwilligungen**
  Die Datenverarbeitung kann auch aufgrund Einwilligung der betroffenen Person erfolgen. Jede Einwilligung muss freiwillig, aktiv und informiert erfolgen und ggfs. Formerfordernissen entsprechen, sonst ist sie unwirksam. Alle Einwilligungstexte sind mit unserem Datenschutzbeauftragten abzustimmen. Jede Einwilligung muss dokumentiert sein (schriftlich oder elektronisch). Einwilligungen per „Opt-out" sind nicht wirksam möglich Zu Ausnahmen im außereuropäischen Kontext ist der DSB zu konsultieren).
- **Datenverarbeitung zur Wahrung berechtigter Interessen**
  Daten dürfen auch für unsere berechtigten Interessen (z.B. Durchsetzung von Forderungen und Ansprüchen) verarbeitet werden, wenn keine schutzwürdigen Interessen der betroffenen Person überwiegen. Deswegen ist eine dokumentierte Interessenabwägung unter Einbeziehung des DSB erforderlich. Überwiegen dabei schutzwürdige Interessen der betroffenen Person, darf die Verarbeitung nicht erfolgen.
- **Datenverarbeitung besonders schutzwürdiger (sensitiver) Daten**
  Die Verarbeitung sensitiver Daten erfordert eine besondere Grundlage (z.B. Arbeits-/ Sozialrecht, Einwilligung des Betroffenen oder das Erfordernis zur Rechtsverteidigung).

Datenverarbeitung für eine vertragliche Beziehung (Erlaubnisbeispiel)

Personenbezogene Daten von z.B. Lieferanten, Kunden oder anderen Geschäftspartnern dürfen zur Erfüllung des jeweiligen Vertrages oder zur Durchführung vorvertraglicher Maßnahmen verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern sie im Zusammenhang mit dem Vertrag steht. In der Vertragsanbahnungsphase ist die Verarbeitung der Daten für z. B. Angebote etc. erlaubt.

Wenn die Daten allerdings **zu Werbezwecken** genutzt werden, sind **besondere Voraussetzungen** zu beachten. Beachten Sie unsere internen Vorgaben für Werbung/Marketing und halten Sie ggf. Rücksprache mit Ihrem Vorgesetzten oder dem DSB.

Auch **Mitarbeiter (Bewerber-)Daten** dürfen (nur) verarbeitet werden, **wenn** diese für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses **erforderlich** sind. So muss der Arbeitgeber z. B. zur Überweisung des Gehalts Ihre Kontodaten wissen oder für Zwecke der Kirchensteuer, ob und welcher Konfession Sie angehören.

3.4 Datenminimierung

Jede Datenverarbeitung muss so angelegt sein, dass so wenige Daten wie möglich und immer nur die Daten verarbeitet werden, die objektiv für den verfolgten Zweck benötigt werden. Bei der Erhebung verpflichtender und freiwillig anzugebender Daten ist jeweils eine Kennzeichnung nötig. Bei IT-Systemen muss zudem geprüft werden, ob die Daten pseudonymisiert oder anonymisiert (keine Zuordenbarkeit mehr zur Person) werden können. Bei anonymen Daten findet das Datenschutzrecht schließlich keine Anwendung. Alle Daten müssen stets sachlich richtig und aktuell sein und wo nötig berichtigt werden.

3.5 Zweckbindung der Datenverarbeitung

Für jede Datenverarbeitung muss ein legitimer Verarbeitungszweck festgelegt werden. Zweckänderungen sind nur unter engen Voraussetzungen und dokumentiert möglich. Daher müssen neue Verarbeitungsvorgänge und wesentliche Änderungen an bestehenden Verarbeitungen frühestmöglich an den Datenschutzkoordinator oder DSB gemeldet werden.

3.6 Datenqualität

Alle verarbeiteten Daten müssen stets sachlich richtig und aktuell sein. Es müssen alle angemessenen Maßnahmen getroffen werden, damit personenbezogene Daten im Hinblick auf den Verarbeitungszweck berichtigt werden. Eine Prüfpflicht, ob Ansprechpartnerdaten im CRM-System noch aktuell sind, besteht aber beispielsweise nicht.

3.7 Speicherbegrenzung und Löschung von Daten

Die Grundsätze der Verarbeitung personenbezogener Daten der DSGVO schreiben die **Löschung** personenbezogener Daten vor, **sobald der definierte Verarbeitungszweck entfallen** ist. Diese Anforderung steht im Spannungsverhältnis zu rechtlichen Aufbewahrungspflichten. Vereinfacht lässt sich festhalten:

- Personenbezogene Daten sind zu **löschen, sobald** diese im Verfahren (datenschutzrechtlicher Prozess) **nicht mehr benötigt** werden,
- **keine** gesetzliche **Aufbewahrungspflicht** besteht und
- auch keine sonstigen Aufbewahrungsgründe (bspw. zivilrechtlich vereinbarte Aufbewahrungszeiten, Erfüllung\Nachvollziehbarkeit von Rentenansprüchen oder Abwehr zivilrechtlicher Klagen etc.) bestehen.

Die Umsetzung und Löschung der Daten ist durch den Data Owner sicherzustellen. Zur systembezogenen Umsetzung wenden Sie sich an die IT-Abteilung. Spheros implementiert ein datenschutzkonformes Löschkonzept.

3.8 Datensicherheit / Vertraulichkeit

Angemessene Datensicherheit ist zu gewährleisten. Die Daten müssen jederzeit durch geeignete, risikoorientiert gewählte technische und organisatorische Maßnahmen gegen unbefugten Zugriff, Verarbeitung und Weitergabe, gegen Verlust, Zerstörung und Schädigung geschützt werden (Verfügbarkeit, Vertraulichkeit und Integrität der Daten).

Die Sicherheitsmaßnahmen sind unter Berücksichtigung des Standes der Technik und Implementierungskosten zu treffen. Die Risikoanalyse erfolgt dabei aus Sicht der betroffenen Person. Art, Umfang, Umstände und Zweck der Verarbeitung, Eintrittswahrscheinlichkeit einer Gefahr und Auswirkung eines (möglichen) Schadens werden berücksichtigt. Sensitive Daten, aber auch Bewerberdaten sollen nach Möglichkeit verschlüsselt werden.

Alle Mitarbeiter müssen die Vertraulichkeit der personenbezogenen Daten beachten. Von jedem Mitarbeiter soll eine Verpflichtungserklärung vorliegen – optimalerweise mit dem On-

Boarding. Wo erforderlich, wird auf das Fernmeldegeheimnis verpflichtet – dies betrifft insbesondere IT-Administratoren.

Jeder Mitarbeiter darf nur Zugang zu personenbezogenen Daten erhalten, soweit dies für die jeweilige Aufgabenerfüllung erforderlich ist („Need-to-know-Prinzip"). Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen und müssen die personenbezogenen Daten in ihrem Verantwortungsbereich gegen unberechtigten Zugriff bzw. Verarbeitung sowie Verlust schützen und verfügbare Lösungen nutzen (z. B. Passwortsperre, Wegschließen von Unterlagen, datenschutzkonforme Vernichtung, aufgeräumter Schreibtisch, sicheres Format beim Versenden, z.B. PDF).

Es ist zu beachten, dass speziellere Regelungen, z.B. aus einer Informationssicherheits-Richtlinie, gelten können.

4 Datenschutz-Prozesse

4.1 Rechte der betroffenen Personen

Alle Personen deren Daten wir verarbeiten haben „Betroffenenrechte", die sie jederzeit bei uns geltend machen können. Auskunfts- und Einsichtsrechte unserer Mitarbeiter werden durch die Personalabteilung erfüllt.

Jeder Mitarbeiter muss sich mit diesen Rechten und den internen Prozessen vertraut machen und danach handeln. Die Prozesse können in Form von „Feuerwehrübungen" (Probedurchlauf) geprüft und hinsichtlich Effektivität und Korrektheit kontrolliert werden.

Wenn Sie zu einem Betroffenenrecht kontaktiert werden oder nicht sicher sind, ob eine Anfrage, die Sie erreicht eine **datenschutzrechtliche Betroffenenanfrage** ist,

melden Sie den Sachverhalt **unverzüglich an datenschutz@atarax.de.**

Solche Anfragen können auf allen Kanälen (E-Mail, Anruf, Post, persönliche Vorsprache) an uns/ an Sie gerichtet werden und sind nicht immer gleich als Datenschutzanfragen erkennbar. Oft sind Stichworte wie „Auskunft", „Löschung" oder „Datenschutz" enthalten.

Der Betroffenenrechteprozess
Wir haben für jedes Betroffenenrecht einen Prozess definiert, mit dem wir die Umsetzung gewährleisten können. Die Prozesse berücksichtigen die Details der einzelnen Rechte:

4.1.1 Recht auf Auskunft

Betroffene haben das Recht, eine Bestätigung darüber zu verlangen, ob personenbezogene Daten über sie verarbeitet werden. Wenn dies der Fall ist, können Sie Auskunft darüber verlangen. Auf Verlangen ist unentgeltlich eine Kopie der Daten zur Verfügung stellen. Wenn Rechte anderer oder unsere Interessen entgegenstehen, darf/ muss keine Kopie herausgegeben werden oder wir müssen diese Inhalte unkenntlich machen. Ob solche Interessen durchgreifen, ist immer vorab datenschutzrechtlich zu prüfen.

4.1.2 Recht auf Berichtigung

Betroffene haben das Recht, Berichtigung sie betreffender unrichtiger Daten zu verlangen (z.B., weil sich die Adresse geändert hat). Je nach Verarbeitungszweck hat der Betroffene auch das Recht, die Vervollständigung unvollständiger Daten zu verlangen. Wenn die Daten auch anderen (z. B. externen Dienstleistern) offengelegt wurden, müssen wir die Empfänger informieren, außer dies ist unmöglich oder unverhältnismäßig.

4.1.3 Recht auf Löschung („Recht auf Vergessenwerden")

Betroffene haben das Recht zu verlangen, dass die über sie gespeicherten Daten unverzüglich gelöscht werden, wenn z.B. die Daten für den Verarbeitungszweck nicht mehr erforderlich sind, eine Einwilligung widerrufen oder ein Widerspruch eingelegt wurde und keine Aufbewahrungspflichten der Löschung entgegenstehen. Hierüber müssen grundsätzlich **auch etwaige Empfänger informiert werden**, dies betrifft auch die Löschung von Links zu diesen personenbezogenen Daten und Kopien solcher Daten.

4.1.4 Recht auf Einschränkung der Verarbeitung

Betroffene haben das Recht, die Einschränkung der Verarbeitung ihrer Daten zu verlangen. Dies betrifft z.B. Fälle, in denen die Richtigkeit der Daten streitig ist, die Verarbeitung der personenbezogenen Daten unrechtmäßig erfolgte oder wenn es um die Geltendmachung, Ausübung oder Verteidigung von rechtlichen Ansprüchen geht.

Bei Einschränkung dürfen diese Daten – von der Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte anderer natürlicher oder juristischer Personen verarbeitet werden. Hierüber müssen Empfänger dieser Daten informiert werden. Wurde eine Einschränkung der Datenverarbeitung erwirkt, müssen wir sicherstellen, dass betroffene Personen vor Aufhebung der Einschränkung darüber unterrichten werden.

4.1.5 Recht auf Datenübertragbarkeit

Betroffene haben das Recht die sie betreffenden Daten kostenlos in einem „strukturierten, gängigen und maschinenlesbaren Format" zu erhalten. Dieses Recht auf Datenübertragbarkeit ist nur bei Daten gegeben, die der Betroffene selbst zur Verfügung gestellt hat, und die automatisiert und -vertrags-/ einwilligungsbasiert verarbeitet werden. Das Recht besteht nicht, wenn Rechte und Freiheiten anderer Personen berührt sind.

4.1.6 Widerspruchsrecht

Betroffene haben das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben gegen die Verarbeitung ihrer Daten, die aufgrund einer Interessenabwägung stattfindet, Widerspruch einzulegen. Dann dürfen wir die Daten nicht mehr verarbeiten, außer wir können zwingende schutzwürdige Gründe für die weitere Verarbeitung nachweisen, welche die Interessen der betroffenen Person überwiegen oder bei Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Welche Interessen letztlich überwiegen hängt vom Einzelfall ab und ist ggfs. juristisch zu klären.

Betroffene können zudem jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten zum Zweck der Direktwerbung Widerspruch einlegen (auch für Profiling in Zusammenhang mit Direktwerbung). Dann dürfen die Daten nicht mehr für Direktwerbung verarbeitet werden.

4.1.7 Recht auf Widerruf von Einwilligungen

Jede Einwilligung kann jederzeit ohne Angabe von Gründen, anlasslos und formfrei widerrufen werden. Eine Datenverarbeitung, die auf diese Einwilligung gestützt war, darf dann nicht mehr stattfinden. Der Widerruf ist unverzüglich umzusetzen; auch in allen IT-Systemen. Zudem muss der Widerruf jeder Einwilligung so einfach sein, wie die Einwilligung es war. Es muss also stets die für die betroffene Person einfachste Möglichkeit des Widerrufs umgesetzt wird, d.h. ohne Fragen nach weiteren Daten oder Gründen.

4.2 Informationspflichten gegenüber betroffenen Personen

Die DSGVO schreibt vor, Betroffene umfassend über die Verarbeitung ihrer Daten durch uns zu informieren. Dies betrifft nicht nur Kunden und Interessenten, sondern gilt auch gegenüber unseren eigenen Mitarbeitern, da auch diese „Betroffene" sind.

Bei der Erfüllung der Informationspflichten müssen sämtliche Kontaktpunkte mit allen Gruppen betroffener Personen (Kunden, Interessenten, Mitarbeiter, etc.) berücksichtigt werden, damit online wie offline alle Transparenzanforderungen eingehalten werden.

Was Inhalt, Form und Zeitpunkt der Information angeht, so ergeben sich die Anforderungen an die Betroffeneninformation direkt aus dem Sachverhalt und den Artikeln 13 und 14 DSGVO. Aus diesem Grund sind Datenschutzinformationen immer individuell zu erstellen. Besonders in diesem Zusammenhang kann örtliches Datenschutzrecht ergänzende Anforderungen stellen, die ebenfalls zu berücksichtigen sind.

4.3 Automatisierte Entscheidung im Einzelfall inkl. Profiling

Betroffene Personen dürfen keiner ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt (sog. Profiling, z.B. Scoring). Für Abschluss oder Erfüllung eines Vertrags nötige, mit ausdrücklicher Einwilligung erfolgende oder aufgrund von Rechtsvorschriften zulässige automatisierte Entscheidungen sind aber denkbar.

Es ist sicherzustellen, dass auf Wunsch des Betroffenen ein Mensch in den Prozess eingreift, der Betroffene den eigenen Standpunkt darlegen und die Entscheidung anfechten kann („Remonstrationsrecht"). Vollautomatisierte Entscheidungen dürfen grundsätzlich nicht auf besonderen Kategorien personenbezogener Daten beruhen (Ausnahme: Einwilligung).

4.4 Meldepflicht bei Datenpannen

Bei Verletzung des Schutzes personenbezogener Daten („**Datenpanne**") kann eine **Meldepflicht** gegenüber einer Aufsichtsbehörde/ Betroffenen bestehen. Es ist entscheidend, ob der Vorfall voraussichtlich zu einem Risiko für die Rechte und Freiheiten Betroffener führt.

Die **Meldung muss unverzüglich, aber binnen 72 Stunden** an die zuständige Aufsichtsbehörde **erfolgen.** Unsere Melde- und Eskalationswege sind einzuhalten.

Nehmen Sie nie selbst eine Meldung an die Aufsichtsbehörde oder Betroffene vor.

Melden Sie jeden Fall/ Verdacht einer Datenpanne sofort an datenschutz@atarax.de

4.5 Outsourcing / Verträge über Auftragsverarbeitung

Bei der Zusammenarbeit mit Dienstleistern, die in unserem Auftrag und auf unsere Weisung hin personenbezogene Daten verarbeiten, ist eine datenschutzrechtliche **Vereinbarung**, ein sogenannter „AVV", „AV-Vertrag", oder „Auftragsverarbeitungsvertrag" nötig, der **vor Beginn der Zusammenarbeit geschlossen** werden muss. Eine sorgfältige Dienstleisterauswahl muss nachgewiesen werden, da wir als Auftraggeber sicherstellen müssen, dass der Datenschutz eingehalten wird. Auftragsverarbeiter müssen in regelmäßigen Abständen geprüft werden.

Gegebenenfalls müssen wir die Besonderheiten berücksichtigen, die sich aus dem Umstand einer Verarbeitung in so genannten Drittstaaten außerhalb der EU bzw. des Europäischen Wirtschaftraums (EWR) ergeben. Aufgrund der Komplexität muss das Thema Datentransfers ins Ausland stets gesondert unter Einbeziehung des Datenschutzbeauftragten geprüft werden. Vergleichbare vertragliche Erfordernisse können auch bestehen, wenn ausschließlich Einheiten/ Betroffene außerhalb der EU von der Verarbeitung berührt sind. Auch in derartigen Fällen ist der DSB aus Compliance-Gründen einzubinden.

Auch wenn ein AVV nicht verpflichtend ist, müssen Informationen geschützt werden. Dies wird über Geheimhaltungsverpflichtungen (NDAs) sichergestellt. Jeder Mitarbeiter muss sich

hiermit vertraut machen und gemäß den ggfs. hinsichtlich AVVs und NDAs erlassenen Arbeitsanweisungen handeln.

4.6 Verzeichnis der Verarbeitungstätigkeiten (VVT)

Das Verzeichnis der Verarbeitungstätigkeiten ist wegen der Rechenschaftspflicht ein zentrales Dokument zum Nachweis der Rechtskonformität. Welche Informationen enthalten sein müssen ist gesetzlich geregelt, es wird elektronisch geführt und unterliegt einem bedarfsgerechten, in der Regel jährlichen Review durch den DSB. Wenn wir Auftragsverarbeiter sind müssen wir die Tätigkeit dokumentieren. Verarbeitungstätigkeiten sind allgemein zum Beispiel unsere Kundendatenverwaltung oder unsere Urlaubsplanung.

4.7 Datenschutz-Folgenabschätzung (DSFA)

Bei risikobehafteten Datenverarbeitungen ist eine DSFA durchzuführen. Das Erfordernis ist bei Einführung neuer oder Änderung bestehender Datenverarbeitungen zu prüfen. Eine typische Schwierigkeit liegt in der Bestimmung des Risikos, zumal mit zunehmender Digitalisierung. Ob eine DSFA nötig ist wird auch anhand der Kataloge der lokalen Aufsichtsbehörden und der Maßnahmen, die das Schadens- bzw. Eintrittspotential im Hinblick auf die Rechte und Freiheiten Betroffener reduzieren, entschieden. Wenn die DSFA ergibt, dass trotz Schutzmaßnahmen ein Restrisiko verbleibt, ist die Datenschutzaufsicht zu konsultieren.

4.8 Datenschutzkontrollen

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze unterliegt regelmäßigen, dokumentierten Prüfungen. Die Aufsichtsbehörde kann die Einhaltung der Vorschriften kontrollieren. Der DSB führt zudem interne Kontrollen durch, um Wirksamkeit und Angemessenheit des Datenschutz-Managementsystems sicherzustellen.

4.9 Definition und ständige Verbesserung der technischen und organisatorischen Maßnahmen

Die Verarbeitung personenbezogener Daten ist durch angemessene technische und organisatorische Maßnahmen abzusichern, die dem Risiko der Verarbeitung Rechnung tragen und dem Stand der Technik entsprechen. Hierfür müssen Datenschutzmanagement und Informationssicherheitsmanagement zusammenspielen, Risiken identifiziert und Informations- und IT-Sicherheitsmaßnahmen abgeleitet werden.

Der Risikoprozess muss den Schutzbedarf der Daten hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität berücksichtigen. Um auf dem Stand der Technik zu operieren ist ein PDCA-Zyklus zur ständigen Verbesserung der Maßnahmen, Systeme sind resilient zu dimensionieren. Resilienz meint Widerstandsfähigkeit im Störfall, Fehlerfall und unter Last.

Bei der regelmäßigen VVT-Aktualisierung wird eine verfahrensbasierte Risikoanalyse durchgeführt und es werden verfahrensspezifische Sicherheitsmaßnahmen getroffen. Bei kritischen Verfahren wird im Rahmen der DSFA besonderes Augenmerk auf die Absicherung des Verfahrens durch Ergreifung von Technik und Organisation gelegt.

4.10 Sicherstellung von "Privacy by design / by default"

Die Begriffe ‚privacy by design' und ‚privacy by default' meinen die datenschutzfreundliche Ausgestaltung von Anwendungen und Systemen. „Privacy by design" ist Datenschutz durch Technikgestaltung, also die konsequente Berücksichtigung der Datenschutzanforderungen (z.B. über Minimierung/ Pseudonymisierung, transparente Funktionen, Löschroutinen). ‚Privacy by default' meint datenschutzfreundliche Grundeinstellungen. Die Umsetzung

verlangt eine Berücksichtigung schon im Lastenheft, eine frühzeitige Einbindung des Datenschutzbeauftragten und gegebenenfalls die Einbindung weiterer (IT-) Experten.

4.11 Mitarbeitersensibilisierung

Durch zumindest jährliche Unterweisungen, die vom DSB konzipiert und/oder seitens des DSB durchgeführt werden, wird die Belegschaft für den Datenschutz sensibilisiert. Auch bei relevantem Stellenwechsel innerhalb des Unternehmens erfolgt in der Regel eine Unterweisung (vorzugsweise durch den Datenschutzbeauftragten).

5 Schlussbestimmungen

Diese Richtlinie besteht aus ihrem Text, den Anhängen und den Arbeitsabläufen, die einen integralen Bestandteil der Richtlinie bilden. Diese Richtlinie existiert in einer englisch- und einer deutschsprachigen Fassung. Im Fall von Inkonsistenzen oder Abweichungen hat die deutsche Sprachfassung Vorrang.

Diese Richtlinie ist ab dem Zeitpunkt ihrer Veröffentlichung gültig. Die Richtline lässt andere Richtlinien unberührt, sofern sie solche nicht ausdrücklich modifiziert oder ihnen vorgeht.

Die Einhaltung der in dieser Richtlinie enthaltenen Regelungen gehört zu den Arbeitspflichten jedes Mitarbeiters. Verstöße können u.a. mit arbeitsrechtlichen Konsequenzen geahndet werden.

Die Regelungen aus dieser Richtlinie gelten -soweit anwendbar- auch nach Beendigung des Arbeitsverhältnisses fort. Die Bestimmungen dieser Richtlinie lassen weitere bei Spheros bestehende Regelungen unberührt, sofern sie diese nicht ausdrücklich abändern oder ihnen vorgehen. Mit Veröffentlichung dieser Fassung treten alle früheren Fassungen außer Kraft.

Spheros Germany GmbH, Gilching, July 1st, 2024

Mark Sondermann, Geschäftsführer

Appendix 1– Anhang 1

History of Changes - Änderungshistorie

Version	Date/ Datum	Drafted by/ Ersteller	Chapters/Kapitel	Changes/ Änderungen
0.1	27.06.2024	atarax	All Alle	Draft of V 0 1 Erst-Entwurf V 0.1