Group-wide Data Protection Policy of the PHOENIX group

GGL_Corporate Data Protection_20210201

Takes effect as of:	01.02.2021
Internal publication	YES
Substitute guideline:	GGL_Group Data Protection_20171219

Coverage:

Group	X
Subgroup Germany	
PHOENIX	

Approved at: **17.11.2020**

Group-wide Data Protection Policy of the PHOENIX group

Version Control

Version	Title	Author	Date
01 EN	Group-wide Data Protection Policy of the PHOENIX group	Barbora Seigertschmid	17.11.2020

Version	Terms affected by revision	Author	Date
01 EN	first version	Barbora Seigertschmid	17.11.2020

Signatures / Approvals

Name, Department	Role	Date
Barbora Seigertschmid HCDP	Author	17.11.2020
Sven Seidel CEO	Approval	17.11.2020
Helmut Fischer CFO	Approval	17.11.2020

Corporate Data Protection Glossary

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CDP Guide	Corporate Data Protection Guide
Corporate Concept	Corporate Data Protection Concept
Data Protection Policy	Group-wide Data Protection Policy of the PHOENIX group
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
Employee	An individual who is employed by the PHOENIX group.
EU/EEA	European Union /European Economic Area
GDPR	General Data Protection Regulation (EU) 2016/679 (GDPR).
HCDP	Head of Corporate Data Protection
LSC	Local Security Coordinator
Local Concept	Local Data Protection Concept
PIA	Privacy impact assessment
PHOENIX Company	Subsidiary that belongs to the PHOENIX group
PHOENIX group	Comprises all companies in which a majority of the shares are held by PHOENIX Pharma SE or one of its subsidiaries, or which are directly or indirectly controlled by the holding company or its subsidiaries
SA	Supervisory Authority
SOPs	Standard Operating Procedures
TOMs	Technical and Organizational Measures

1. Introduction

(1) We live in a data-driven world. Our customers, employees or business partners are sharing their data with us almost within every transaction and interaction. Personal data is information that allows a living person to be directly, or indirectly, identified from data that is available like a person's name, location data, health data or it can be something that may be less obvious like IP addresses.

(2) The personal data belong to a living person (**data subject**). Data protection makes sure everyone's personal data is used properly and legally. Data protection laws establish the main principles and rules for the personal data processing.

(3) The PHOENIX group takes the data protection and privacy of its employees, business partners and customers data seriously. This Data Protection Policy aims to ensure personal data processing complies with the data protection law and thereof reflects the obligations and principles of the GDPR.

2. Scope

(1) This Policy applies to the processing of personal data and special categories of personal data, which relate to living individuals who can be identified from that data. It applies to data processed either electronically or which is paper based and stored in a relevant filing system. In countries where data of legal entities (e.g. limited companies) is protected to the same extent as personal data of individuals, this Policy applies equally to data of legal entities.

(2) This Policy applies to:

a) all employees of the PHOENIX group;
b) all PHOENIX Companies;
c) entities with which a contract has been signed specifying that this Policy has to be enforced in order to access group's information assets (partners in Joint Venture, franchise partner etc.);
d) all third parties who directly access the information assets owned by or under the direct control of the PHOENIX group (e.g. external consultants);
e) all service providers, who directly access the information assets owned by or under the direct control of the PHOENIX group. These must demonstrate a level of compliance with this Policy.

(3) Any third-party service providers and contractors, who directly access the information assets owned by or under the direct control of the PHOENIX group must be contractually required to comply with this Policy and obliged to confidentiality. Service providers considered as data processor must sign data processing agreements (see Chapter 6).

(4) The PHOENIX Company shall exercise its authority over its employees and implement this Policy into the local binding rules for employees, according the local labour law.

(5) The PHOENIX Company shall ensure that all its employees have suitable access to this Policy in their local language if necessary, in particular via the intranet. The original English version prevails.

(6) This Policy is one of the implementation activities necessary to achieve compliance with the GDPR. Further implementation activities are described in Chapter 10.

(7) National law and regulations may be stricter than GDPR and/or this Policy. All PHOENIX Companies and their employees shall comply with the relevant local legislation.

(8) Local adaptation may be set in place but must not cause the level of data protection to fall below that described in this Policy. Deviations from this Policy or from Corporate Data Protection Standards may only be granted by exception by PHOENIX Group (HCDP, PHOENIX group Executive Board). The request and the approval for an exemption shall be documented. A template for exemption request can be requested from the HCDP.

3. Organisation: Roles and Responsibilities with regard to data protection

3.1 Executive Board (Group level)

(1) The Head of Corporate Data Protection (HCDP) supports the PHOENIX group Executive Board in the organisation, implementation, maintenance, review and improvement of Corporate Data Protection. The Executive Board requests defined reports from the HCDP.

(2) For enabling the HCDP to fulfill his/her duties, the Executive Board shall automatically inform and if applicable involve the HDCP appropriately and in a timely manner about/in all international issues, projects, changes or operations, which are related to personal data processing (passive right to access information). The Executive Board shall support the HCDP in performing his/her tasks.

(3) The HCDP shall have the resources that reflect the nature and complexity of the business model in the group. The HCDP has an independent position in the organization and reports to the member(s) of the Executive Board.

3.2 Management Board (Company level)

(1) The PHOENIX Company shall review if the designation of a Data Protection Officer (DPO) is obligatory under the local law and comply with further legal requirements related hereto (e.g. inform the Data Protection Authority, publish the contact details on the local DPO etc.).

(2) If there is no legal obligation to designate a DPO according the GDPR or the local data protection law, PHOENIX Company shall designate a Contact Person for the data protection tasks and communication with Corporate Data Protection. For internal communication purposes, this person will be also internally called the DPO. This abbreviation does not mean that person is an officially appointed Data Protection Officer in accordance with the GDPR.

(3) Any third-party service providers acting as the DPO of the PHOENIX Company must be contractually required to comply with this Policy.

(4) PHOENIX Companies from one country may decide that one person will represent them in the communication with the Corporate Data Protection.

(5) The DPO – officially or internally appointed – shall have the necessary professional qualifications and knowledge of the data protection law and practices.

(6) For enabling the DPO to fulfill his/her duties the local Management Board shall automatically inform and if applicable involve the DPO appropriately and in a timely manner about/in all issues, projects, changes or operations, which are related to the regulations of the protection of personal data. The local Management Board shall support the DPO in performing his/her tasks.

(7) The DPO shall have the resources that reflect the nature and complexity of the business model in the PHOENIX Company. The DPO has an independent position in the PHOENIX Company and reports to highest management level.

(8) Management Board, whether or not performing the role of the process, is accountable for data protection. The Management Board shall ensure compliance with data protection law and this Policy, e.g. by setting up appropriate organisational structures and procedures, so that operational management is provided with the means and powers to perform the role of the Process Owner and ensure compliance effectively.

(9) All employees shall have a proper access to existing policies and procedures on data protection corresponding to the work position. Policies, procedures as well as responsibilities and functions regarding data protection shall be monitored and maintained regularly (every 2 years); responsible for this local monitoring is the Data Protection Officer.

3.3 Employees

(1) All Employees are expected to maintain confidentiality concerning personal data processed by the PHOENIX Company. This obligation shall be incorporated into the employment agreement and/or into the onboarding documentation.

(2) Adequate data protection training (online and/or in person) is obligatory for every employee in the PHOENIX group by consideration of the job function and responsibility. The training plan belongs to the implementation activities (see Chapter 10).

(3) All employees support the DPO and HCDP in the performance of their duties, for example by granting them an access to the personal data (in the case of data subjects' requests) and processing operations on request, providing information or handing over documents.

(4) All employees involve the DPO/HCDP at an early stage in all matters relating to the protection of personal data.

(5) All employees observe and adhere to data protection principles when processing data (see Chapter 4).

(6) All employees report the data breaches internally (see Chapter 9).

3.4 Process Owner

(1) The Employee in the PHOENIX Company who is conceptually responsible for a business procedure or internal process in which personal data are processed is considered to be the Process Owner.

(2) The Process Owner is responsible for the so-called Processing Activity. Processing Activity is a set of operations, such as a specific business process or an IT tool.

(3) The Process Owner is named in the Records on processing activities by name or by function (see Chapter 5).

(4) When planning, introducing and later changing the Processing activity the Process owner shall comply with following rules:

a) Involve the DPO regarding the privacy impact (pre)assessment;

b) Perform a data protection impact assessment, if obligatory (see Chapter 5);

c) Complete and maintain the records on processing activity (see Chapter 5);

d) Ensure the Information for the data subjects on the data processing;
e) Ensure that the data protection principles are observed during the processing (by involving the relevant departments);
f) Review the external service provider; if service providers process data for the PHOENIX Company on behalf of and in accordance with the company's instructions, ensure the conclusion of the data processing agreements;
g) Ensure that the rights of data subjects can be fulfilled;
h) Ensure that access rights and storage periods are defined with implementation.
i) When transferring data to non-EU/EEA countries, involve the DPO and observe the special requirements for data processing outside the EU/EEA;
j) Document everything in such a way that compliance with the regulations on data protection can be proven.

(5) The technical maintenance of the processing activity can be overhanded to an external provider (see the Chapter 6) or the IT department, but the Process Owner is still responsible for the fulfillment of the rules listed above. The DPO assists and advices to the Process Owner.

(6) The PHOENIX Company can define own appropriate organisation to manage data protection and its terminology, roles and responsibilities accordingly. The role of the Process Owner shall be covered by the defined organisation.

3.5 Data Protection Officer

(1) The main task of the DPO is the protection of privacy of data subjects in relation to the processing of personal data on the Company/Country level (data of customers, patients, employees etc.). The DPO is the official contact point for the data subjects and for the supervisory authority.

(2) The DPO is responsible for advising to the organisation and employees regarding the data protection. The DPO is responsible for monitoring compliance with the data protection law. The DPO defines the content of the Local Concept (details see Chapter 10).

(3) The main responsibilities of the DPO are:
- Raising awareness: campaigns and training programs;
- Maintaining the local policy on Data protection and related policies or instructions;
- Maintaining the Country Templates (Data Processing Agreement, Privacy Notice, Consent etc.);
- Supporting in negotiation of a Data Processing Agreement (DPA): Review of the major Data Processing Agreements & EU Model Clauses; DPO as a support for Legal and/or Procurement;
- Initial assessment of new local projects: definition of the data protection requirements and recommendations;
- Assistance in the performance of the data protection impact assessments;
- Assistance in the creation and maintenance of the record of processing activities;
- Coordination of exercising the rights of the data subject: Maintaining of the internal processes on exercising the rights of the data subject;

- Support personal data incidents management and personal data breach management: Coordination and assistance in reporting to the supervisory authority/data subjects
- Governance and Consultation: Ongoing monitoring of data protection compliance

(4) The DPO informs the HCDP on data protection issues or major projects related to the data protection in the PHOENIX Company. The DPO reports to the HCDP in the so-called Country Reports annually or on request.

3.6 Corporate Data Protection

(1) The main task of the Corporate Data Protection department is to support the PHOENIX group and the DPOs in the data protection tasks.

(2) The HCDP has the similar tasks as the DPO but in an international context. HCDP advises and monitors the compliance with data protection law in the group; HCDP coordinates and supports the international cooperation regarding the data protection.

(3) The HCDP defines the content of the Corporate Concept (details see Chapter 10).

(4) The main responsibilities of the HCDP are:

- Raising awareness: campaigns and training programs (incl. online training PHOENIX group).
- Maintaining the group-wide Data Protection Policy.
- Creation of the Corporate Data Protection Standards.
- Support in negotiation of international major Data Processing Agreement (DPA).
- Initial assessment of new local/international projects: definition of the data protection requirements and recommendations.
- Assistance in the performance of the Data Protection Impact Assessments on a group level (Corporate Templates for the local DPOs).
- Maintaining of the Data breach group reporting system: Admin for the reporting platform.
- Maintaining of the Data Breach Management: Coordination and assistance in reporting to the supervisory authority/data subjects, if international aspects occurs.
- Consultation and ongoing monitoring of data protection compliance.

(5) The member(s) of Corporate Data Protection support(s) the HCDP by his/her activities in specific areas on the local or international area. Corporate Data Protection team member is bound by the instructions of the HCDP and reports directly to the HCDP.

3.7 Information Security

(1) The Chief Information Security Officer (**CISO**) is responsible for ensuring and implementation of the information security standards in the PHOENIX group. Thereof the CISO establish appropriate security policies, guidelines, standards and defines the content of the security concept for PHOENIX group.

(2) The CISO and the Local Security Coordinator (**LSC**) are responsible for the implementation and documentation of the Technical and Organizational Measures (**TOMs**) to protect the personal data. The documentation of TOMs will be used to demonstrate compliance with the Security principle of the GDPR (see the Chapter 4).

(3) There shall be a close collaboration and communication between the CISO and the HCDP and the LSC and DPO on the local level with regard to TOMs. The HCDP/DPO shall list the major requirements on TOMs.

(4) The LSC supports the DPO within the review of services providers. The LSC checks the TOMs of service provider considered as the data processor (see the Chapter 6).

4. Legal framework for the processing of personal data

(1) The list below gives an overview of generally recognized data protection principles according to the model found in Article 5 of the GDPR.

(2) All employees are required to observe and adhere to the data protection principles when processing personal data. All employees shall follow the Data Protection Requirements accordingly to their function and role in the PHOENIX group and/or in the PHOENIX Company.

Principle 1: Lawfulness, fairness and transparency

(1) The processing of personal data must be fair; i.e. no unexpected or misleading data processing shall be undertaken. The data subject must be informed of the important details on the processing of their personal data.

(2) Personal data may only be processed if there is a legal basis for the data processing. There are six available lawful bases for processing:

(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract PHOENIX Company has with the individual, or because there are specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for an official function, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for the legitimate interests of the PHOENIX Company or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

(3) If the same purpose could be achieved without the personal data processing, no lawful basis is given. The lawful basis must be defined before the beginning of the processing and must be documented in Records on processing activity (see Chapter 5).

(4) No single basis is more important than the others – which basis is most appropriate to use will depend on the purpose/purposes and relationship with the data subject.

Special rules for the Consent

(1) Consent is not inherently better or more important than these alternatives. Consent means offering individuals real choice and control.

(2) Consent must be given voluntarily. Consent should be obvious and require a positive action to opt in. There is no set time limit for consent and the length of time consent will last for will depend on the context of the data processing.

Special rules on the Special category data according data protection law (GDPR)

(1) The GDPR defines Special category data as:
- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life;
- data concerning a person's sexual orientation.

(2) For the processing of special categories of personal data, stricter rules apply. In addition to the lawful basis one of the specific conditions in Article 9 of the GDPR must be met:
(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

(3) The DPO must be involved in every planning or projects related to the processing of the special data category.

Data Protection Requirements related to the Lawfulness, fairness and transparency
- Determine a clear lawful basis before the beginning of the processing activity. - Make sure that the processing activity does not exceed the limits of this legal basis. - Consult the lawful basis with the DPO and document the lawful basis according the local rules. - Involve the DPO, if special category data are in the scope. - Ensure that the processes, purposes and legal basis are fully documented. - Inform data subjects about the processing, e.g. its purpose and the identity of the controller in the privacy notice; communicate clearly to data subjects how, to which extent and for which purposes their personal data will be processed. - Respect the rights of individuals to access and rectify their data. - Develop procedures and instructions that clearly explain how data subjects can exercise their rights to access and to rectify their data in each phase of data processing.

- Implement functions in the system to respond to access, modification or blocking requests and to objections to processing.
- Adopt internal rules to review the validity of the legal basis in case of a change, e.g. the withdrawing of consent.

Requirements on Consent

- Consent must specifically cover the controller's name (PHOENIX Company), the purposes of the processing and the types of processing activity.
- Explicit consent must be expressly confirmed in words, rather than by any other positive action; Vague or blanket consent is not enough.
- Consent requires a positive opt-in. Do not use pre-ticked boxes or any other method of default consent.
- Keep the consent requests separate from other terms and conditions (the consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly).
- Avoid making consent to processing a precondition of a service.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.

Principle 2: Purpose limitation

(1) Personal data shall be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.

(2) If the new purpose is compatible, a new lawful basis is not needed for the further processing.

(3) If the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with your original purpose.

Data Protection Requirements related to the Purpose limitation

- Process personal data only for specified explicit and legitimate and limited purposes;
- Limit processing of data through an IT system to its primarily specified purpose.
- Ensure purpose limitation if different kinds of data are collected and processed for different purposes.
- Adopt internal rules for the assessment of compatibility needs on a case-by-case basis to allow a change of purpose.
- Specify the purpose or purposes for processing personal data within the documentation required to keep as part of the records of processing (documentation) obligations under Article 30 GDPR.
- Communicate clearly to data subjects any change of the primarily specified purpose of processing their personal data.

Principle 3: Data minimisation

(1) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.

(2) Personal data shall be deleted if it is no longer required.

Data Protection Requirements related to the Data minimization
- Identify the minimum amount of personal data need to fulfil the purpose; hold that much information, but no more. - Review regularly that the personal data is still relevant and adequate for the purposes, and delete anything that is no longer need. - Consider and make use, if feasible, of special privacy enhancing technologies that allow for avoiding excessive use of personal data or enabling the use of anonymised data. - Ensure that personal data is adequate, relevant and not excessive for the purpose.

Principle 4: Accuracy

(1) Personal data shall be accurate and, where necessary, kept up to date.

(2) Every reasonable step must be taken to ensure that personal data, which is identified as being inaccurate, having regard to the purposes for which it is processed, is erased or rectified immediately.

Data Protection Requirements related to the Accuracy
- Ensure that personal data is accurate and up to date. - Implement processes to ensure and maintain accuracy of processed data, e.g. by automatically checking the quality of information keyed into the system before processing. - Ensure that the data subject has the ability to rectify data that is no longer accurate.

Principle 5: Storage limitation

(1) Personal data shall be kept in a format, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

(2) The Process Owner determines the retention/erasure period and registers this into the Retention Policy of the PHOENIX Company.

(3) Every PHOENIX Company maintains a Retention/Erasure Policy

Data Protection Requirements related to the Storage limitation
- Keep personal data no longer than necessary for the originally specified purpose. - Determine upfront retention time for data kept in a form which permits identification of data subjects. - Ensure that required retention periods are proportionate to the purposes of data collection and limited in time. - Assign and manage separately retention time related to data collected for different purposes.

- Special caution has to be taken if personal data is stored on paper due to its existence being hard to trace.
- Design system features to manage the retention time and perform the necessary subsequent actions: deletion or anonymisation.

Principle 6: Security (Integrity and confidentiality)

(1) The PHOENIX Company shall take appropriate technical and organisational measures (TOMs) to protect personal data in a manner commensurate with the privacy risks involved.

The privacy risk for a data subject may arise in particular from
- the unplanned destruction of personal data and/or
- a loss of personal data and/or
- the unplanned modification of personal data and/or
- the unauthorised disclosure of personal data and/or
- the unauthorised access to personal data.

(2) Assessing the appropriate TOMs following shall be taken into account:
- the state of the art, and
- the costs of implementation and
- the nature, scope, context and purposes of processing and
- the risk of varying likelihood and severity for the rights and freedoms of data subjects (i.e. privacy risk for customers or employees etc.).

(3) The TOMs must ensure the 'confidentiality, integrity and availability' of PHOENIX systems and services and the personal data processed within them.

Data Protection Requirements related to the Security (integrity and confidentiality)

- Follow the Information Security Policies, Guidelines, Standards or Awareness Materials.
- Involve the LSCs or CISO into the processing activity, if obligatory according the group-wide or local policy.
- Consider things like risk assessment, organisational policies or technical measures in the planning of the processing activity.
- Based on the risk assessment, design and implement organisational and technical measures to mitigate risks to a level that is acceptable.
- Avoid processing activities for which mitigation would not be effective.
- Ensure that a clear decision is made by the responsible management of which risks are accepted and why.
- If appropriate, use measures such as pseudonymization and encryption.

Requirements related to the Information Security

Confidentiality:

Personal data must be protected against unauthorised or unintentional disclosure. Both external and internal attackers (e.g. hackers, frustrated or curious employees) as well as

negligent or structural threats (e.g. untrained employees, role based authorisation concepts) must be taken into account.

Integrity:
Personal data must be provided completely and correctly. Unauthorised changes to the data must be identified (e.g. through logging/log files) and procedures for correction must be provided.

Availability:
Personal data must be available when needed. This also requires that it can be restored in case of loss or destruction (e.g. backups).

A procedure for regularly reviewing, assessing and evaluating the effectiveness of TOMs must be in place (e.g. penetration tests, external and internal review).

Principle 7: Accountability

(1) The PHOENIX Company is responsible for ensuring it is able to demonstrate compliance with the GDPR principles listed above.

(2) Evidence is the key task for all relevant employees. When accountability mechanisms are being maintained, documentation is produced. That documentation can be used as evidence of accountability, ownership and GDPR compliance.

(3) The PHOENIX Company has to maintain a complete Record of processing activities. All employees, especially the Process Owners are required to inform the DPO in advance (before plans are put in place) about new or changed processing activity (see Chapter 5).

Data Protection Requirements related to the Accountability
- Make sure that compliance with the principles above can be demonstrated within appropriate documentation. - Inform the DPO about new or a changed processing activity in advance, with enough time to allow him/her to assess the processing activity.

5. New or changed data processing activity

5.1 Standard approach

(1) The DPO must be involved in every new processing activity in advance. The Process Owner or Project Manager is Responsible for the proper consultation with the DPO.

(2) The DPO reviews the lawful basis for the data processing. The DPO lists the major data protection requirements within the privacy impact assessment (**PIA**). The scope of the PIA is depending on the processing activity. The DPO advises, if the Data Protection Impact Assessment (**DPIA**) is obligatory (see Point 5.2).

(3) If the Processing Activity or project is international, the HCDP is to be involved as well. The HCDP performs the Corporate PIA/DPIA as a Template for the local PIA/DPIA; local data protection requirements must be reviewed on the local level by the local DPO. The

HCDP reviews also the service providers and/or prepares other documentation/templates (e.g. privacy notice). The HCDP informs the DPOs on every international data processing in advance.

(4) The result of the PIA shall provide proper details for the Records on processing activities. The obligatory content of the records is set in the Article 30 GDPR. Responsible for the fulfilment of the record is the Process Owner. The process on maintaining of the records on processing activity is in responsibility of the DPO.

5.2 Data Protection Impact Assessment (DPIA)

(1) The Process Owner is responsible for the performance of the DPIA. The DPIA must involve the DPO and the LSC (and or HCDP/CISO for the international projects) and further stakeholders (e.g. working counsel, IT architect(s), Legal, etc.).

(2) The DPIA is a process to identify and minimise the data protection risks of a processing activity; i.e. of a project. The DPIA is obligatory under the GDPR for processing that is likely to result in a high risk to individuals. This includes some specified types of processing, but it is also good practice to do a DPIA for any other major project, which requires the processing of personal data. The DPIA will be required in the following scenarios:

- introduction of new technologies,
- automated processing, including profiling, results in decision(s) being made which produce legal effects on individuals,
- large scale processing of special category data is taking place,
- processing of criminal activities,
- systematic monitoring of a publicly accessible area on a large scale etc.

(3) The DPIA must:

- describe the nature, scope, context and purposes of the processing; and
- assess necessity, proportionality and compliance measures; and
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, the PHOENIX Company must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

(4) In circumstances where a DPIA indicates that the processing would result in a high risk to the rights and freedoms of data subjects in the absence of measures taken by the data controller to mitigate the risks, the DPO shall consult with the local supervisory authority.

6. Contracts with service providers

6.1 Rules for the engagement of the data processor

(1) The services provider is considered as the data processor, if the provider acts on behalf of and only on the instructions of the PHOENIX Company.

(2) If the PHOENIX Company decides to use a services related to the data processing of a data processor, a data processing agreement (DPA) must be concluded. For the intra-group data processing applies a special DPA Template and proceeding.

(3) If the DPA of the data processor deviates from the DPA local or corporate Template, the final version must be approved by the DPO or Legal. The review is to be initiated by the Process Owner.

(4) An integral part of the DPA negotiation is the review of the TOMs of the service provider/data processor. During this review the TOMs of the provider must be checked to ensure they comply with the GDPR, in particular with regard to data security (Art. 32 GDPR). This check is coordinated by the DPO with support of the LSC.

(5) The DPA must be concluded in writing and is to be documented.

(6) There shall be a regular audit of the service providers considered as data processors. The data protection audit plan for the service provider (incl. the period for auditing) shall consider the privacy risk related to processing activity. The minimum period for auditing is 24 months. The DPO and the LSC support the Process Owner by the auditing. The plan for data protection audit belongs to the implementation activities (see Chapter 10).

6.2 Rules on the data transfer outside the EU

(1) The GDPR restricts transfers of personal data outside the EU/EEA, unless the rights of the data subjects are protected in another way, or one of a limited number of exceptions in GDPR applies.

(2) The PHOENIX Company must always know the entire supply chain (which company/ which country/ which service/ which data category). The PHOENIX Company must guarantee the level of data protection of the GDPR in the whole processing chain.

(3) The adequate level of the protection in a no EU/EEA country/provider is then ensured by certain guarantees that are predefined in the GDPR (e.g.):

- Commission's Adequacy Decision
- Binding Corporate Rules
- EU Standard data protection clauses etc.

(4) The art of the guarantee shall be used as a criterion for selecting providers. The Commission's Adequacy Decision is considered to be a reliable guarantee; it should be noted that the respective Adequacy Decisions might differ in their scope from country to country. The Binding Corporate Rules can also be seen as another strong guarantee.

(5) The DPO must be involved in every data transfer/processing outside of EU/EEA in advance.

(6) The PHOENIX Company shall maintain the evidence of data transfer to any NON-EU/EAA-provider.

6.3 Rules for other service providers

Any third-party service providers and contractors, who directly access the information assets including personal data by or under the direct control of the PHOENIX group, must be contractually required to comply with this Policy and be obliged to confidentiality.

7. Fulfilment of the rights of data subjects

(1) The GDPR provides the following rights for individuals:

a) the right to be informed

The data subject shall get the relevant information at the moment of the data collection or at first possible moment.

b) **the right of access**
The data subject has the right to request confirmation of whether data concerning him/her is being processed and, if this is the case, to request information regarding this data according to Art. 15 GDPR.

c) **the right to rectification**
The data subject has the right to request the completion or correction of inaccurate data concerning him/her.

d) **the right to erasure**
The data subject hast the right to demand that his/her personal data be deleted, if there are no legal obligations to keep the data.

e) **the right to restrict processing**
The data subject may demand restriction of the processing in accordance with Art. 18 of the GDPR.

f) **the right to data portability**
The data subject has the right to request a copy of the personal data PHOENIX Company holds about him/her and, in addition, to request that it be transmitted to other data controllers.

g) **the right to object**
The data subject has the right to object at any time to processing of his/ her personal data, especially for direct marketing, profiling and research purposes.

(2) The PHOENIX Company shall ensure, by means of appropriate technical and/or organisational measures, that the undertaking can fulfil data subject rights. The measures must be documented.

Example: IT systems are to be selected or designed in such a way that all data relating to a data subject can be printed out in order to fulfil the right of access, or a procedure is to be implemented to ensure that all data relating to a person can be manually extracted from the system.

(3) If a data subject contacts the PHOENIX Company and asserts a data subject's right, the involved employee shall immediately forward the request to the DPO and or follow the further local rules.

8. Data Protection by Design

Insofar as default settings for data processing can be made in a system, these settings must be made in such a way that, in view of the purposes of use, no more data than necessary, no longer than necessary and no more comprehensively than necessary are processed, and access by third parties is restricted as far as possible.

9. Data breach reporting

9.1 Internal reporting

(1) Every breach of personal data must be reported to the DPO immediately:

a) via the PHOENIX group portal:
https://phoenixgroup-databreach.integrityplatform.org/
OR
b) via the local tool/proceeding.
Examples:

- *Loss of a business mobile phone/laptop or data media*
- *Correspondence to the wrong recipient*
- *Unauthorised access to the customer portal or Speakap*
- *Infection of the system with malware with impact on personal data*

(2) The DPO and the LSC shall create a common proceeding to ensure the reporting. The DPO and the LSC are together responsible for the awareness on data breach reporting in the PHOENIX Company.

(3) The HCDP is to be involved if the data breach is international or massive (high privacy risk for data subjects or legal risk for the PHOENIX group).

9.2 Data breach management

(1) Based on the internal report, the DPO shall identify the responsible person/ department(s). The responsible employees/managers form an ad hoc working group with the DPO. In a critical case, the Communication Department and the Management Board join the working group as well.

(2) The working group examines the facts of the case and performs the assessment of the risk for the affected data subjects (customers, employees etc.) and for the PHOENIX Company.

(3) The working group decides on possible measures to mitigate the risks and about the notification to the supervisory authority and/or data subject(s). This decision must be met within the 72-hour deadline (as of knowledge of the data breach) and follow this protocol :

The PHOENIX Company is/is not obliged to the official notification:		
NO RISK for the Data Subject = No Notification obligations	RISK FOR RIGHTS of the data subject = Notification to the Supervisory authority within 72 hours	HIGH RISK FOR RIGHTS of the data subject = Notification to the Supervisory authority within 72 hours =Notification to the data subject within 72 hours or without undue delay.
In any case, the working group must document the data breach.		

(4) The management board shall be informed of this decision by the DPO. The DPO complies with the notifications rules of the local supervisory authority.

(5) The DPO and the LSC shall create a common detailed proceeding to ensure the data breach management on the local level.

10. Implementation Activities

10.1 Corporate Implementation Activities

(1) The Group-wide Policies, Corporate Data Protection Standards and Corporate Templates represent the main implementation activities of Corporate Data Protection.

(2) The Policy created by Corporate Data Protection is a document that outlines specific requirements or rules that must be met, approved by the Executive Board.

(3) The Corporate Data Protection Standard is not a Policy, but a minimum standard action, process or tool created or provided by Corporate Data Protection to comply with the Data Protection Policy (**Standard**). Executive board approval is not required. The Standard does not affect the Policy, but it is the implementation tool to the Policy.

(4) The collection of the Corporate Data Protection Standards is the Corporate Data Protection Guide (**CDP Guide**).

(5) The HCDP prepares the final Standard within a consultation with the relevant Corporate Stakeholders and/or DPOs, if necessary. The HCDP publishes the Standard to the DPOs and to the involved Corporate Stakeholders. The DPOs and involved Stakeholder are responsible for further publishing or forwarding of the Standard to the relevant recipients.

(6) The following stakeholders are identified on group level for the group-wide Policy or Corporate Data Protection Standards (depending on the topic):

- Chief Information Security Officer
- Enterprise Architect
- CIO Office
- Corporate Legal
- Corporate Audit
- General Procurement
- Corporate HR

(7) The PHOENIX Company shall implement the Standard in an appropriate manner (e.g. local policy, instruction, technical adjustment) taking into account the legal or organisational local specifics. Local adaptation may be set in place but must not cause the level of data protection to fall below the Standard. The local privacy rules or technical solutions must always represent the best possible data protection and protect adequately the privacy of the data subjects. The DPO reports to the HCDP about the local implementation in the Country reports annually or on request.

(8) The Corporate Template represents the data protection best practice in the PHOENIX group.

10.2 The Corporate Data Protection Concept

The Main Corporate Implementation Activities build the following Corporate Data Protection Concept (**Corporate Concept**). The DPO shall use this Corporate Concept for his/her own measures and local implementation activities:

Kind of document	Name of the document/tool
Policy	• Group-wide Data Protection Policy of the PHOENIX group

(rules that must be met)	• **Further group-wide policies on data protection topics, if necessary** • **Information Security Policies (ensuring the integrity and confidentiality of the personal data).** *Approved by the Executive Board* *Part of the Local Concept as well*
Group Data Processing Agreements & Group Join Controller Agreements	• **Result of the intra-group negotiation** *Approved by the Executive Board and the local Management Board* *Part of the Local Concept as well*
Corporate Data Protection Standards *(minimum standard for action, process or tool in the PHOENIX group)*	**Examples** • Standard on International data transfer • Standard on Life Cycle for the Data Protection Concept: • Standard on the DPIA • Standard on the Retention Concept • Reporting system for data breach • Group Online Training Platform
Awareness	Group Awareness Campaign

10.3 The Local Data Protection Concept

(1) The local implementation activities build the Local Data Protection Concept (Local Concept). The DPO supports the Management Board to define the content of the Local Concept. The framework for the Local Concept is following:

Kind of document	Name of the document/tool
Local Policies /SOPs/Instruction	Local Data Protection Policy (if needed) Local regulation based on the CDP Guide or local legal requirements: • Regulation on the PIA/DPIA • Regulation on the Retention Concept • Regulation on data breach management/reporting • Regulation on the maintaining of the Records on processing activities • Regulation on the exercise of the rights of data subjects
Local Templates	Based on the Corporate Templates • Data processing agreement • Check-lists for a privacy notice • Flyers
TOMs	• Group or local Information Security Policies • Formal and informal documentation (e.g. back up concept, log files etc.)
Awareness	Local Training & Awareness Campaign