SWISSPEARL

Personal Data Protection Policy

SWISSPEARL

Contents

1. Background and purpose

EU has adopted the General Data Protection Regulation ("GDPR"), and it has been in force in the European Economic Area ("EEA") from 25 May 2018. The GDPR applies in all member states directly, but most EEA countries have passed or will pass national/local laws to implement it. If local legislation has stricter requirements than this Policy, the local legislation shall apply.

Swisspearl strives to be compliant with regulations on the protection of personal data, in all the countries where we operate, as we are committed to protect the personal data that we are processing for our employees, potential employees, customers and partners. The protection of personal data includes own employees as well as information to be provided where personal data are collected from the data subject, ("data privacy notice") cf. GDPR Art 13. The internal and external data protection requirements are fulfilled by set of personal data protection guidelines and templates.

2. Policy statement

At Swisspearl, we are committed doing business in a responsible way and with integrity. Every day we may receive, use and store personal information about employees, potential employees, customers, partners and website users. This information must be handled lawfully and appropriately in Swisspearl in line with the requirements of the EU General Data Protection Regulation.

3. Scope

This Personal Data Protection Policy ("the GDPR Policy") applies to Swisspearl Group AG and its directly and indirectly owned, subsidiaries (collectively referred to as "Swisspearl") and all employees in those entities.

This GDPR Policy sets out the definitions and general procedures for protection of personal data. This Policy also defines the structure and content for supportive guidelines and templates required to fulfil the personal data protection requirements for Swisspearl.

4. Roles and responsibilities

Group Legal is responsible for ensuring the implementation of this GDPR Policy in Swisspearl. Furthermore, the appointed Data Privacy Administrator is the Group General Counsel. However, it is the responsibility of the Managing Directors of the Legal Entities, to ensure this Policy is followed locally. When local legislation has stricter requirements than this Policy, the local legislation shall apply. It is the local Swisspearl entity's responsibility to have local procedures aligned to comply with this overall Group Policy and add local policy amendments according to the stricter local requirements. All local amendments to this policy must be done in co-operation with Group Legal.

5. Policy areas

Definitions and general principles relating to processing of personal data

5.1 What is “personal data”?

Personal data is any information – even the simplest – if such relates to an identified or identifiable person. This means that even a name itself is personal data. Also, information regarding a person not even named can be “personal data” if it is possible to identify the person based on the given information (e.g. salary cost per entity – if there is only one employee in one of the entities the salary of this person is easily identifiable).

5.2 What means “processing” of personal data?

The term “processing” means anything you do with personal information from and including getting access to it, and until you delete it. It includes collecting, storing, organizing, registering, adaption or alteration, sharing and deleting personal data. Whether done electronically or physically in paper form, the same rules apply.

In general, Swisspearl collects and processes personal data only where the collection and processing are required for the purposes of Swisspearls legitimate and commercial interests and obligations, including for business purposes, financial purposes, purposes of IT security and access security and administration of personnel. You may only process personal data for these legitimate purposes.

As an employee in Swisspearl, you are responsible for processing of personal data in accordance with this Policy and in accordance with the following 6 principles showed in figure 1 below when carrying out work for Swisspearl.

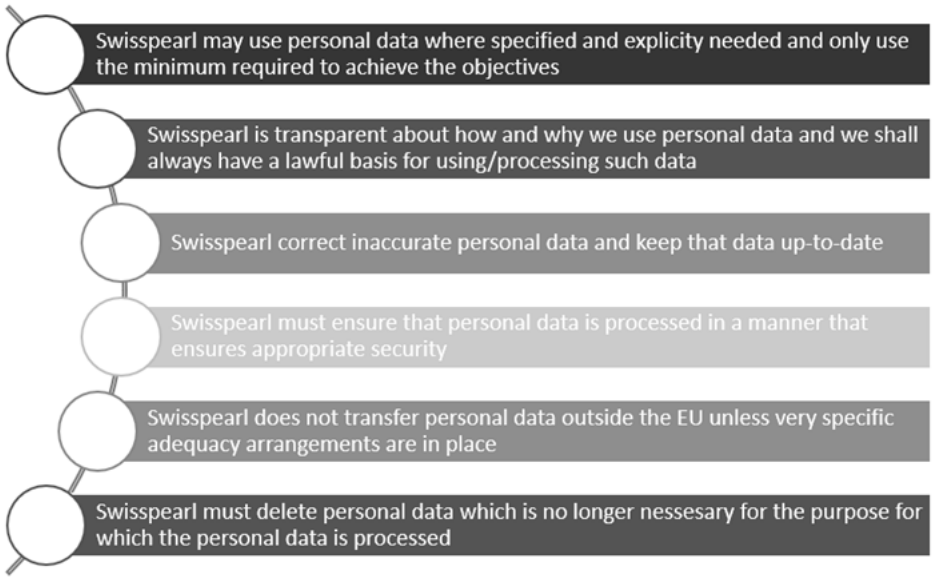

Figure 1. 6 data protection principles when carrying out work in Swisspearl

We will have to go from a “nice to have” or “just in case” way of thinking to asking ourselves “what do I actually need?”. Accordingly, collection of internal or external personal data must be limited only to data, necessary to accomplish the intended purpose and not on the basis that it could be useful at some point in the future for some unspecified purpose.

5.2.1 Supportive GDPR Policy documentation

To fulfil the personal data protection requirements, this Policy is supported by a set of guidelines and templates. The supportive guidelines address the following perspectives of the personal data protection:

- Stakeholders: employees, business partners, job applicants and external parties
- Personal data deletion when legitimate purpose for processing has expired
- Security breaches involving personal data

Table 1 summarises the supportive documentation Swisspearl has issued and defines name, purpose, location and language for each document. The documentation can be found on the Swisspearl Intranet “Speak Up”, “Group Legal” and “GDPR”.

Table 1. Data protection documentation

Document Name	Document Purpose	Target group	Location	Language
Swisspearl Group Personal Data Protection Policy	Sets out the definitions and general procedures for protection of personal data	Internal	Speak Up	English
Swisspearl Group Employee Personal Data Privacy Guideline	Information to Swisspearl's employees, regarding collection of personal data	Internal	Speak Up	English
Swisspearl Group Personal Data Processing Guideline	Practical guide for Swisspearl employees on processing of personal data	Internal	Speak Up	English
Template Personal Data Processing Agreement English	Appendix to Swisspearl Group Personal Data Processing Guideline: Agreement template if personal data is processed by external party	Internal	Speak Up	English
Template Personal Data Processing Agreement - Databehandleraftale Danish	Appendix to Swisspearl Group Personal Data Processing Guideline: Agreement template if personal data is processed by external party	Internal	Speak Up	English
Template Personal Data Protection Impact Assessment - DPIA	Appendix to Swisspearl Group Personal Data Processing Guideline: Guideline for personal data assesment of specific projects or actions before startup	Internal	Speak Up	English
Swisspearl Group Business Partner Personal Data Privacy	Guideline to business partners regarding personal data	Internal	Speak Up	English
Swisspearl Group Job Applicant Personal Data Privacy Guideline	Guideline regarding personal data of candidates applying job in Swisspearl	External	All Swisspearl Websites + Speak Uo	English and Local
Swisspearl Group External Party Personal Data Privacy Guideline	Guideline to Swisspearl's external parties, regarding personal data	External	All Swisspearl Websites + Speak Uo	English and Local
Swisspearl Group Personnel Administration Personal Data Processing Guideline	Guideline for processing of personal data relating to personnel administration	Internal	Speak Up	English
Swisspearl Group - Appendix 1. Consent form for candidates	Approval from candidate to allow Swisspearl to contact job applicant references	Internal	Speak Up	English
Swisspearl Group - Appendix 2. Consent intranet (print out)	Print out and email version of employee consent to allow Swisspearl to disclose employee's personal data on the intranet	Internal	Speak Up	English
Swisspearl Group - Appendix 2. Consent intranet (email)				
Swisspearl Group - Appendix 2a. Consent website and intranet (print out)	Print out and email version of employee consent to allow Swisspearl to disclose employee's personal data on Swisspearl websites and/or intranet	Internal	Speak Up	English
Swisspearl Group - Appendix 2a. Consent website and intranet (email)				
Swisspearl Group - Appendix 3. Procedure for handling data access request	Swisspearl procedure on how to handle request from data subject to access to his/her personal data processed or stored by Swisspearl	Internal	Speak Up	English
Swisspearl Group File-Encryption of Personal Data Guideline	Guideline for sending personal data to third parties outside Swisspearl	Internal	Speak Up	English
Swisspearl Group Personal Data Retention and Deletion Guideline	Guideline in terms of deleting personal data, when the legitimate purpose of processing has expired	Internal	Speak Up	English
Swisspearl Group Exercising Rights of Data Subjects Guideline	Definition of the data retention and deletion principles and procedures	Internal	Speak Up	English
Swisspearl Group Handling of Personal Data Breaches Guideline	Guidelines in terms of security breach involving personal data	Internal	Speak Up	English

5.2.2 Lawfulness of processing

Legal basis of personal data falls into 4 different most commonly categories that are shown in figure 2. The legal basis for processing personal data depends on its category. Please note below, that sensitive data includes only 9 specific mentioned types of data. Everything else is considered “non-sensitive” data although special requirements exist for the processing of personal data relating to criminal convictions and offences (criminal records) and the processing of national identification numbers depending on local requirements. Local requirements will vary between the different Swisspearl entities, as the member states can determine specific conditions for the processing of such.

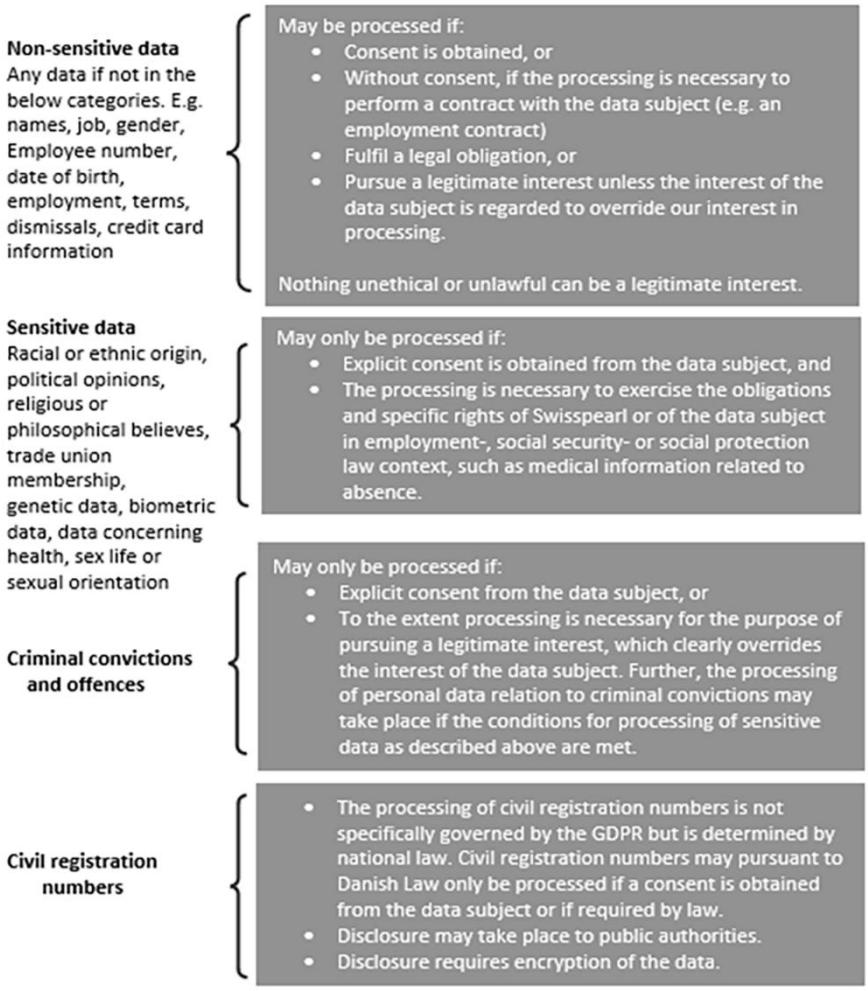

Figure 2. Legal basis of personal data

To sum up, processing of personal data will only be lawful if one of the following legal basis applies:

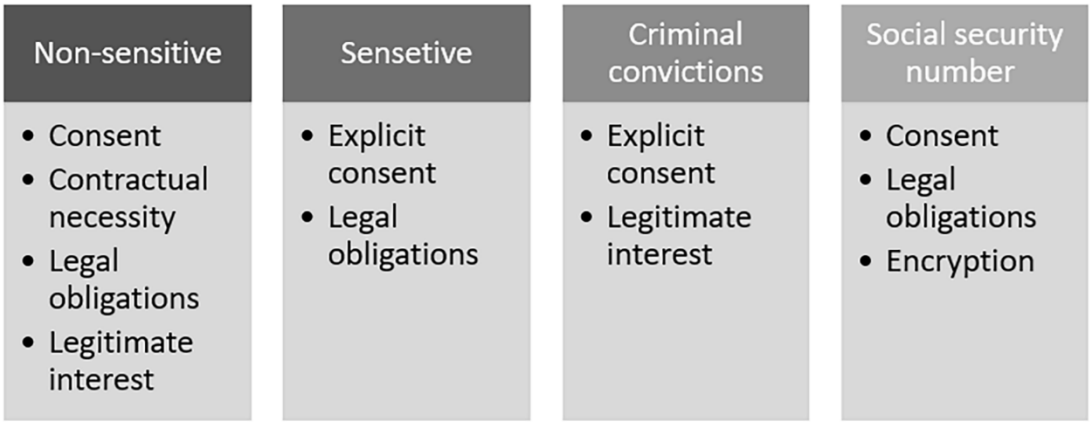

Figure 3. Summary of legal basis of personal data

Note that the difference in the processing of non-sensitive and sensitive data is, that sensitive data cannot lawfully be processed unless one of the specific legal basis for sensitive data is verified (the so called exemptions to the general prohibition of processing of sensitive data) and in addition the verification of a legal basis which also applies to the processing of non-sensitive data. However, the 6 general principles, the restrictions, and the rights of the data subjects are the same for both categories. The main difference is as illustrated above for sensitive Data, stricter requirements apply to the legal basis of processing.

5.3 Consent

When processing is based on the data subject's consent, the consent must, in order to be considered a valid consent, be a written, voluntary permission for Swisspearl to use the data subject's mentioned personal data for specific purposes. The consent must be informed and shall be presented in a manner, which is clearly distinguishable from other matters. The consent requires an affirmative, unambiguous action by the data subject indicating his/her agreement in order to be valid. Furthermore, the data subject must prior to providing the consent, be informed of the right to withdraw the consent at any time. Consents must be filed for documentation purposes.

Note that a consent from a data subject cannot stand alone. The 6 general principles described above must also be adhered to in cases where consent is given and provides the legal basis.

5.3.1 Storage and erasure of personal data

Generally, you are not allowed to store personal data longer than required or needed for the legitimate purpose you collected it for.

Ask yourself: “Is this nice to have or is it really needed?” If not really needed, you should stop the processing and delete the personal information from your computer and IT-systems.

The retention period for the personal data is determined by Swisspearls obligation under current local legislation, what is necessary to perform agreements with business partners, employees and other third parties, but also for Swisspearl to be able to document relevant information in potential complaints and other claims raised against or by Swisspearl.

It is essential that storage of personal data is kept to a minimum, and you must erase personal data from your computer and the system such as from your personal archive, including your email accounts, folders, subfolders, desktop, etc. when you are done processing these data. Remember to empty the trashcan folder.

Your desk as well as other areas within your workspace, such as copy room, must be kept free from papers containing personal data. Keep papers with personal data locked away in cabinets and drawers. Papers with personal data must be safely disposed after processing such as by shredding or discarded in a secured wastepaper basket.

Do not let papers with personal data lay in the open – use drawers and filing cabinets. Shred or otherwise dispose safely when no longer needed.

Generally, when personal data is stored in intended centralized systems or archives (such as the ERP, CRM, HR-systems, centralized drives for the purpose, etc.), it is no longer necessary for the individual employee to store the personal data. Even though there can be practical reasons that might motivate to store personal information locally or at your email folders, such practical reasons are not legitimate purposes. Figure 4 below shows cleaning up personal data files in practise.

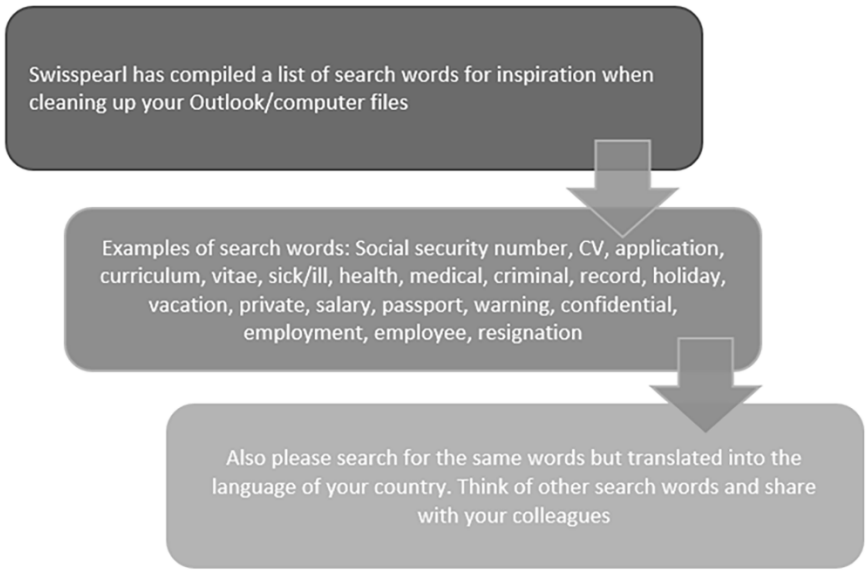

Figure 4. Practical cleaning of personal datafiles

5.3.2 Rights of the data Subjects

As Swisspearl is handling personal data as a data controller, we need to be aware of certain GDPR rights of the /data subjects which we are obliged to respond to. The rights of the data subjects are shown in figure 5.

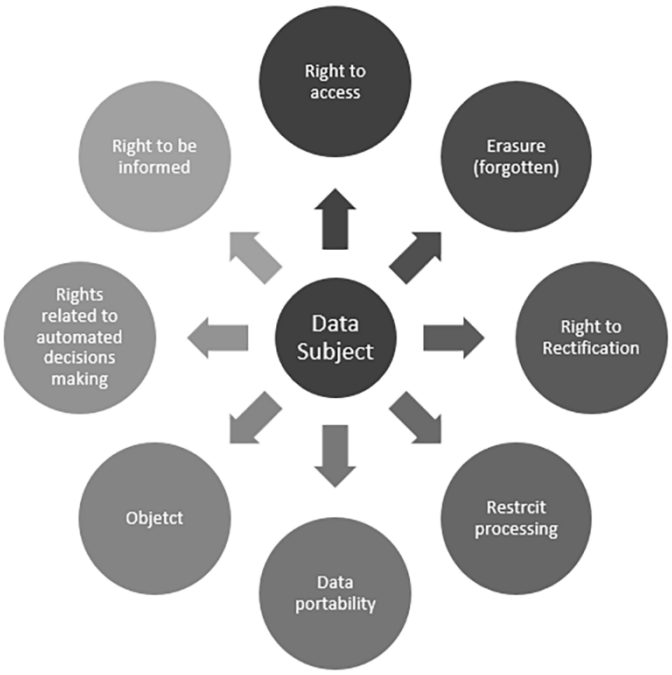

Figure 5. The rights of the data subjects

If a person (data subject) wishes to exercise his/her rights, such a request must be responded and handled following certain requirements to form and contents. The data subject must receive the response within a set time frame. To make sure that Swisspearl responde to these requests from data subjects correctly, such request must be discussed with Group Legal before replying. Please contact Group Legal immediately when receiving such a request.

5.3.3 Disclosure of personal data to third parties

You must exercise caution when disclosing personal information to third parties. In particular, you must:

- Look into the identity of the companies, organizations and authorities, who request the information and, if necessary, examine whether these are entitled to receive the requested information,
- Ask that the third party provides you with a written request in order to verify the identity and the basis of receiving the information,
- Ensure that disclosure of personal data is in accordance with this Policy.

Swisspearl may only disclose personal data to third parties if the conditions described above are met:

1. the general principles of the processing of personal data are followed
2. the processing is lawful (has a legal basis).

In general, Swisspearl only shares personal data with third parties for the purpose of:

- Performing agreements/contracts with customers, suppliers and other parties;
- Complying with legislation and regulatory requirements;
- Assisting suppliers of services and advisors in delivering services and solutions (e.g., IT solutions) and consultancy to Swisspearl.

5.4 Processing by data processors

When a third party provides certain services to Swisspearl and thereby processes data on behalf of Swisspearl, being the data controller, Swisspearl and this data processor is to enter into a data processing agreement. In such situations, Group Legal is to be contacted to firstly establish whether the third party is in fact a data processor. Examples are software suppliers with access to our systems containing personal data, cloud IT storage providers, payroll service providers, and personal profiling consultants.

When entering into a data processor agreement, please use Swisspearl's standard data processor agreement, which meets all the requirements in the GDPR. The standard data processor agreement is available on Speak Up.

5.5 Transfer of personal data to third countries

Swisspearl may only transfer personal data to third countries (countries outside the EEA), if in compliance with certain conditions. On a case-by-case basis, you must assess whether personal data is transferred to third countries, and if so, please contact Group Legal for assistance.

5.5.1 Security

Swisspearl must implement appropriate technical and organizational measures to ensure and to be able to document that the processing of personal data is performed in compliance with the applicable rules. All employees must adhere to the IT Policy. Accordingly, Swisspearl must implement procedures and systems for the purpose of i) ensuring and documenting that the collection, storage, processing and erasure of personal data are carried out in compliance with current legislation and this data protection policy, ii) protecting personal data against unintended or unlawful destruction, alteration or deterioration and iii) preventing unauthorized persons from accessing the personal data.

Swisspearl only grants access to personal data to employees who need access to such data to carry out their obligations to Swisspearl.

5.6 Risk assessment – DPIA

Before you start a new project that involves processing of personal data, you must conduct a risk analysis. Such a project could be the creation of a database, a marketing project, new CRM systems etc. If you assess that the project is likely to result in a high risk to the rights and freedoms of the registered persons related to their personal data, you must carry out a Data Protection Impact Assessment ("DPIA"), before you start the project. This is to identify and minimize the risks. You are welcome to contact Group Legal for assistance with the assessment of the risk. The risk assessment includes parameters as the amount of personal information that will be processed, the number of data subjects involved, and the character of the shared information. A template for the DPIA can be found in Speak Up. Figure 6 presents a process to assess whether a DPIA is needed for your new project.

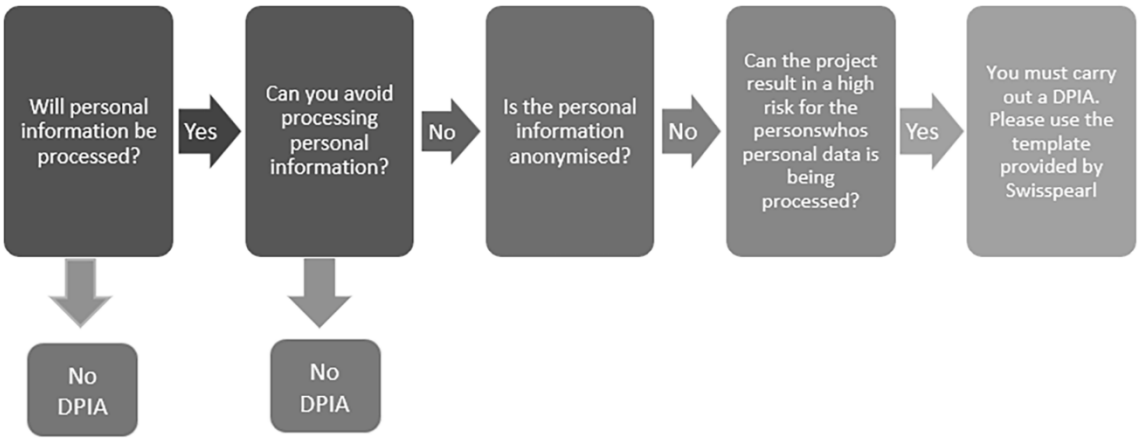

Figure 6. Assessment for the need of DPIA

5.7 Protection by default and protection by design

We have a general obligation to implement technical and organizational measures when starting a new project to integrate data protection on our processing activities.

You must therefore implement appropriate data protection by designing the system, workflows, processes, and software/hardware so that only necessary data will be processed and with appropriate safeguards such as for instance passwords, logging and firewalls.
Furthermore, you must implement data protection by default setting. This could be automatic deletion and no access unless granted for each individual.

6. Data breach

A personal data breach incident must always be reported to the local Data Protection Agency (“DPA”) unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects, such as identity theft, fraud, financial loss etc.

For instance, if you forget your laptop on the train and you get it back the next day, and the laptop only can be entered with your password, then the breach is not likely to result in a risk for the data subjects, and the breach is not to be reported to the DPA. The character of the personal data and the number of data subjects potentially affected should also be taken into account, when assessing the risk to the data subjects.

In case of a personal data breach incident, which is likely to result in a risk to the rights and freedoms of data subjects, Swisspearl must without undue delay inform the DPA and not later than 72 hours after becoming aware of it. However, do not contact any data protection authorities without the prior consultation with Group Legal.

It is not always clear whether a personal data breach occurred is likely to result in a risk as quantified above. Therefore, if you suspect that a personal data breach has occurred, you must contact Group Legal asap.

All personal data breaches, irrespective of whether they are reported to DPA or not, shall be documented comprising the facts relating to the breach, its effects and the remedial action taken. This documentation shall enable the DPA to verify compliance.

7. Related policies and guidelines

All documentation listed in table 1 of this policy and Swisspearl IT Policy

8. Violation of the personal Data Protection Policy

Failure to comply with this Personal Data Protection Policy may result in disciplinary action, including, but not limited to, the issue of a reprimand or warning, suspension or dismissal of the employee.

9. Policy Information

This Personal Data Protection Policy must be reviewed by the Group General Counsel and approved by Swisspearl Board of Directors at least every 1 year. It may be amended at any time with the approval of Swisspearl Board of Directors.

In case other language versions will be made from this policy and in the event of any discrepancies between the English version of this policy and a translated version, the English version will be binding.

10. Contact

If you have any comments or any questions about the Personal Data Protection Policy please contact Swisspearl Group Legal Counsel or gdpr@swisspearl.com

Change log

Version	Date	Description of the change	Changed by