ALPIQ

Policy

Data Privacy

D-GR-13

Document Reference	
Classification (Internal / Confidential)	Internal
Status	Final
Author, OU	GDPO
Owner, OU	Head Group Security & BCM
Scope	Alpiq Group
Languages available	EN, DE, FR
Filename / Version	D_GR_13_Alpiq_Policy_Data_Privacy_EN_V1_0
Number of Pages	27
Version / Date	V1.0 / 12.04.2018

Change History

Version	Date	Name	Changes/Remarks
V1.0	12.04.2018	Friedrich Bohl	First release (replacing «Weisung Datenschutz für Mitarbeiterdaten (D-FI-02)»)

Approvals

Version	Date	Person/Board
V1.0	12.04.2018	Executive Board

Referenced Documents

Ref.	Title	Author	Doc. No.
[1]	Alpiq Group Risk Policy	Head Group Risk Management	R-GRP
[2]	Policy Group Security and Business Continuity Management	Head Group Security & BCM	D-GR-08
[3]	Handbook MIK, V1.0	Head Group Security & BCM	-
[4]	Policy Information & Cyber Security	Head Group Security & BCM	D-GR-06

Table of Contents

1 Introduction

Alpiq is committed to conducting its business in accordance with all applicable Data Protection Laws and regulations and in line with the highest standards of ethical conduct.

This Policy sets forth the expected behaviours of Alpiq employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to individuals having contact with any legal entity of Alpiq Group. This Policy defines also the organisation, the responsibilities and the internal processes to ensure compliance with Data Protection Laws (EU General Data Protection Regulation and Swiss Federal Data Protection Law).

Personal data are subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. All Alpiq legal entities, as Data Controller, are responsible for ensuring compliance with the Data Protection requirements outlined in this Policy and corresponding national data protection laws. Non-compliance may expose Alpiq to complaints, regulatory action, fines and/or reputational damage.

Alpiq's Executive Board is fully committed to ensuring continued and effective implementation of this Policy, and expects all Alpiq employees and third parties to share in this commitment. Any breach of this Policy will be taken seriously and may result in disciplinary action or business sanction.

2 Scope

This policy is mandatory to all group companies in which Alpiq has a controlling interest or vote, wherever this is possible within the boundaries of the applicable law. By way of explanation, group companies shall be used from now on as the collective term for controlled companies covering other commonly used terms such as subsidiaries or majority interests.

This Policy applies to all Alpiq entities where personal data is processed:

- In the context of the business activities and internal administration of the Alpiq entity
- For the procedure or offer of goods or services to individuals (including those offered free-of-charge) by an Alpiq entity
- To actively monitor the behaviour of individuals
- Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with the intention to make a decision about them

- Analysing or predicting their personal preferences, behaviours and attitudes

This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals (data filing systems). This Policy has been designed to establish a group wide baseline standard for the processing and protection of personal data by all Alpiq entities. It regulates the main Data Privacy topics on general level. Please refer for details and templates to the appropriate implementation provisions.

Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this Policy, the relevant national law must be adhered to by the concerned legal entity.
If there are conflicting requirements in this Policy and national law, please consult with the GDPO for guidance.

3 Definitions

Alpiq Entity: An Alpiq Corporation, including subsidiaries and joint ventures over which Alpiq exercise management control

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Contact: Any past, current or prospective Alpiq customer, visitor or employee as individual

Data Controller: A natural or legal person, Public Authority Agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Data Processors: A natural or legal person, Public Authority, Agency or other body which Processes personal data on behalf of a Data Controller

Data Protection Authority: An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law

Data Protection: The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction

Data Subject: The identified or identifiable natural person to which the data refers

Employee: An individual who works part-time or full-time for Alpiq under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes temporary employees, trainees and independent contractors

Identifiable Natural Person: Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical (photo), physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Personal Data: Any information (including opinions and intentions) which relates to an identified or identifiable natural person

Process, Processed, Processing: Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Profiling: Any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement

Pseudoanonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified

Special Categories of personal data: Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data

Third Country: Any country outside EU and Switzerland not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of personal data (countries, not on the list of Appendix B)

Third Party: An external organisation with which Alpiq conducts business and is also authorised to, under the direct authority of Alpiq, Process the personal data of Alpiq Contacts

4 Group Security Framework

4.1 Embedding Privacy in the Alpiq Security Framework

Privacy is one of the Security Management domains on operational Level of Alpiq Security Framework (see Figure 1).

This document, the "Data Privacy Policy", is the commitment of Alpiq to Privacy and Data Protection directed towards both internal as well as external parties.

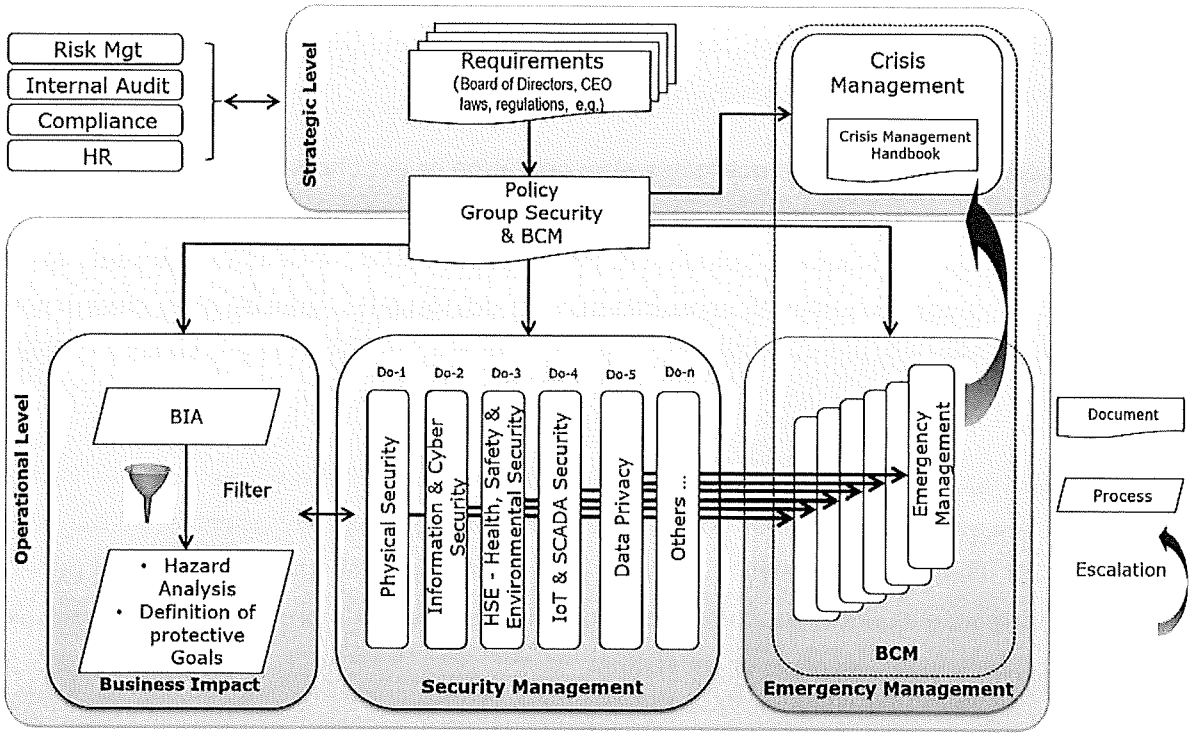

Figure 1: Alpiq Framework Group Security

4.2 Relevant Alpiq Parent Documents

- Alpiq Group Risk Policy [1]
- Policy Group Security and Business Continuity Management [2]

4.3 Relevant Subordinate Alpiq Documents

For better understanding of privacy requirements addressed to every legal entity of the Alpiq Group Data Protection Officer will publish Group Implementation Provisions that shall support legal entities to implement all organizational and technical measures to be compliant with data privacy regulations, see Figure 2. This implementation provisions, templates and checklists are created based on the given Alpiq security framework and are tailored to specific target-groups at Alpiq Entities. They establish the specifications for any further operational level documents.

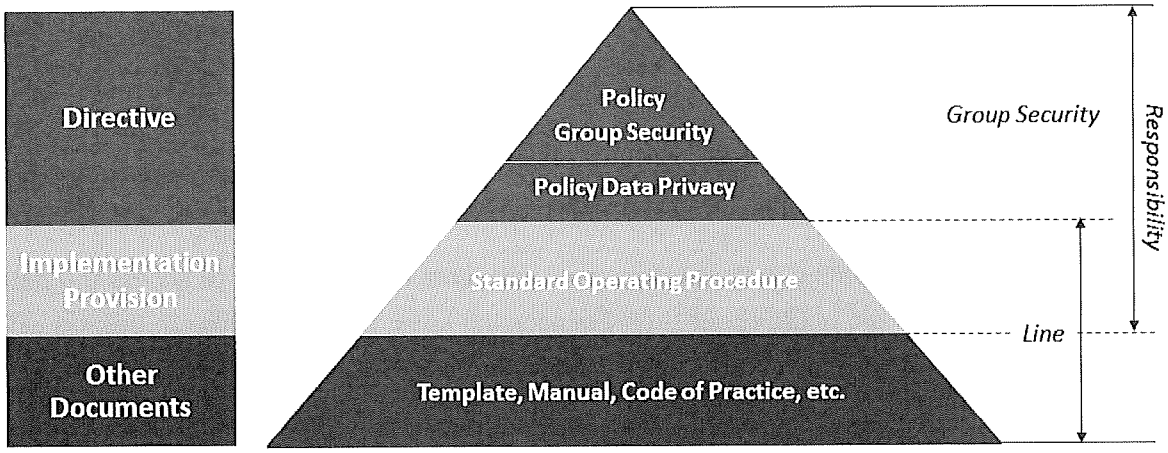

Figure 2: Privacy Document Framework

5 Responsibilities

5.1 Executive Management of the Group

The Responsibility for Group Compliance with Data Privacy Regulations ultimately lies with the CEO and senior management. Based on reporting and advice of the GDPO, the CEO takes decisions to enforce Data Privacy Compliance within Alpiq Group.

5.2 Senior Management of Legal Entity

The primary responsibility for Data Privacy Compliance of Alpiq's legal entity in accordance with European Union and national data privacy law lies with the senior management of this legal entity. To ensure and support compliance with data privacy regulations the senior management nominates a Local Privacy Partner (LPP), who assures data privacy based on Alpiqs Group Data Privacy Policy and further national data privacy requirements, who reports and advises senior management. The management team of each Alpiq entity must ensure, that all Alpiq employees responsible for the processing of personal data, are aware of and comply with the content of this Policy.

5.3 Group Data Privacy Officer (GDPO)

To demonstrate commitment to Data Privacy, and to enhance the effectiveness of our compliance efforts in privacy area, Alpiq has nominated a GDPO. The Officer operates with independence and is staffed by suitably skilled individuals with all necessary authority. The GDPO reports to Alpiq's Group Security Officer who has direct access to the Risk Management and to the CEO.

The GDPO is responsible for:

- **Governance**
  - Establishing group-wide Data Privacy Governance
  - Reviewing all Data Privacy procedures and related directives on the group level
- **Services**
  - Providing Data Privacy training content and giving advice for management, Local Privacy Partner (LPP) and employee
  - Dealing with requests from residents in Switzerland to access the data Alpiq holds about them; supporting Local Privacy Partner in dealing with such requests in their countries
  - Acting as a point of contact for and cooperating with Data Protection Authority in Switzerland (FDPIC); supporting LPP and local Data Privacy Officers in case of request from local Data Protection Authority
  - Leading and managing major Data Breach Notification
- **Monitoring & Reporting**
  - Keeping the board updated by regular reporting about Data Privacy responsibilities, risks and issues
  - Supporting preparation of internal audits and privacy risk analyses
  - Acting as second line of defence by driving regular assessments of privacy compliance of Alpiq Group

5.4 Local Privacy Partner (LPP)

The Local Privacy Partner (LPP) acts as single point of contact for privacy issues of the legal entity he is assigned to. On a local level the Local Privacy Partner duties are:

- Keeping the management of the legal entity updated by regular reporting about data privacy risks and issues
- To act as a first contact person for management and employees for privacy questions and coordination of implementation of internal and external privacy requirements

- Keeping the management of the legal entity as well as the GDPO updated by regularly reporting about data privacy risks and issues in his area
- Contact Person for local Data Protection Authorities (DPA) and for external Individuals in case of their request. Dealing with requests from residents in local country to access the data Alpiq holds about them
- Support training and rise awareness for local management and associates in privacy
- Overseeing local privacy requirements coming from national regulators; periodical reporting to GDPO and to local entity Management (privacy status, problems, data breaches, risks)
- Supporting local privacy controls and Data Privacy Impact Assessment (DPIA)

6 General Processing Principles, Processing Special Categories, Profiling and Automated Decision Making

6.1 General Data Processing Principles

Alpiq has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Alpiq must tell the Data Subject what processing will occur (transparency).

The processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the General Data Protection Regulation (lawfulness).

Alpiq will not process personal data unless at least one of the following requirements is met:

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which Alpiq is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by Alpiq or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the Personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from GDPO before any such processing may commence.

Principle 2: Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Alpiq must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Alpiq must not store any personal data beyond what is strictly required.

Principle 4: Accuracy

Personal data shall be accurate and, kept up to date. This means Alpiq must have in place processes for identifying and addressing out of date, incorrect and redundant personal data.

Principle 5: Storage Limitation

Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. This means Alpiq must, wherever possible, store personal data in a way that limits or prevents identification of the Data Subject. Personal data will not be retained by Alpiq for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which Alpiq entities need to retain personal data must be defined. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Principle 6: Integrity & Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Alpiq must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability

Alpiq shall be responsible for, and be able to demonstrate compliance. This means Alpiq must demonstrate that the six previous Data Privacy Principles (outlined above) are met for all personal data for which it is responsible.

6.2 Consent of Personal Data Processing

Alpiq will only process special categories of data (also known as sensitive data) where the Data Subject expresses consent to such processing or where one of the following conditions applies:

- The processing relates to personal data which has already been made public by the Data Subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior Data Privacy Impact Assessment shall be conducted and the basis for the processing clearly recorded in the data inventory.

Where special categories of data are being processed, Alpiq entity will adopt additional protection measures. Each Alpiq entity may also adopt additional measures to address local custom or social expectation over the processing of special categories of data.

7 Data Privacy Obligations

7.1 Data Inventory

In order to keep the overview about personal data processing and personal data flow across and outside of company every Alpiq entity is obliged to maintain a data inventory in the centralized data privacy tool "OneTrust".

The mandatory records in such data inventory are stated in the Article 30 of GDPR and shall be entered in a data privacy tool.

Every Alpiq entity management is responsible to keep the records of its data inventory complete and up to date. To ensure this, the data inventory must be assessed regularly, at least on a yearly basis. Local Privacy Partner shall support entity management with this task. Any kind of new data processing shall be added without delay to the data inventory.

7.2 Company Duties at Point of Data Obtaining

Each Alpiq entity shall obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned.

7.2.1 Data Subject Notification

Personal data should be collected only from the Data Subject unless one of the following applies:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following applies:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a Data Subject is required, a list of disclosures need to be made available to the Data Subject is provided in the Appendix A.

Notification should occur promptly at time of starting data processing.

Each external website provided by an Alpiq entity will include an online privacy notice and an online cookie notice fulfilling the requirements of applicable law. All privacy and cookie notices must be approved by the GDPO prior to publication on any Alpiq external website.

7.2.2 Data Subject Consent

Where a need prevails to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, Alpiq is committed to seeking such consent. The consent must be properly managed.

The proper consent management includes the following elements:

- Determining what disclosures should be made in order to obtain valid consent (provide Data Subjects with information as to the purpose of the processing of their personal data)
- A consent of the Data Subject must be able to be evidenced by the Alpiq entity seeking this consent
- A consent must be obtained before the first processing of personal data
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language
- Ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the processing of personal data that is unnecessary for the performance of that contract)
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given
- Providing a simple method for a Data Subject to withdraw their consent at any time

The management of every legal entity is obliged to ensure above mentioned principles for consent management.

7.2.3 Digital Marketing

Alpiq entity shall not send promotional or direct marketing material to an Alpiq contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any Alpiq entity wishing to carry out a digital marketing campaign without obtaining prior consent from the Data Subject must first have the approval from the GDPO.

Where personal data processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the Data Subject puts

forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

Where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing to individuals, provided that they are given the opportunity to opt-out.

7.2.4 Logging and Monitoring of Communications

For IT-Security and availability purposes the digital traffic and usage of Internet and email communication is often logged and monitored. For some trading floors at Alpiq the voice recording is necessary due to contractual and legal needs. It is very important, that employees are informed in written form about it.

If such communication monitoring or voice recordings are in place, Alpiq entity shall create a written guideline with the following content:

- If applicable, the conditions for usage of corporate network for private communications
- The purpose of using monitoring and logging
- The nature and the scope of monitored data
- The retention time for keeping records
- The rules for access to this monitoring data and for making evaluations.
- The rights of the company
- The rights of employee

It is essentially important that such guideline complies with General Data Privacy Processing Principles (see Chapter 6) and with local labour law. Appropriate collaboration on this topic with trade union shall be considered if required by local law.

The employee shall be informed about the content of this guideline prior to employment. It is recommended to ensure the proof of this knowledge by asking employee for confirmation by a signature.

7.2.5 Video Surveillance

In case of using video surveillance by an Alpiq entity, the visitors and the employee must be informed about by signs or pictograms. Where possible the individuals shall be informed also about the responsible department and contact possibilities.

The responsible department within the Alpiq entity shall create a site video surveillance concept with information about location, scope and purpose of video surveillance, the responsible controller with contact details, the rules to access the recorded data, technical

and organisational measures to protect the video data, the third parties using this video data (if applicable) and the retention time of data storage.

7.3 Data Privacy Impact Assessment

Risk assessments are an intrinsic part of the GDPR, and a Data Privacy Impact Assessment (DPIA) is a way of assessing the likely risks to individuals, and for identifying the measures that need to be implemented to comply with the GDPR's accountability requirements.

The DPIA describes

- the processing operations and purposes
- the necessity and proportionality of the processing operations in relation to the purpose
- the risks to the person concerned
- the measures planned to mitigate identified risks, including safeguards and procedures

Prior to implementation of new IT systems/-applications or technologies that processes personal data, each Alpiq entity must determine in a early stage of any project if a Data Privacy Impact Assessment (DPIA) have to be conducted.

If the result of DPIA pre-check indicates that the planned processing would result in a high risk to the rights and freedoms of individuals, the Process Owner has to conduct a full DPIA considering the compliance risk dimension and the information security risk dimension. All risks must be evaluated from the perspective of the Data Subject (individual).

A DPIA must be conducted in cooperation with the relevant LPP. In case of further doubts, the GDPO can support additionally. Where applicable, the Information Technology (IT) department will assess the impact of any new technology. Security impacts should be assessed by the Information Security Responsible. The result of a DPIA is a documentation of all risks and appropriate mitigation measures have to be taken into account to reduce the risks.

If the results of a full DPIA show that high risks to individuals cannot be reduced by mitigation measure, the relevant Data Protection Authority has to be informed about it and asked for further recommendations. Where the Data Protection Authority decides that the intended processing is likely to infringe the GDPR, the supervisory authority will provide written advice to the data controller within 8 weeks.

To conduct DPIA refer to implementation provision, providing DPIA methology and checklists guidance.

DPIA shall be repeated at least every 3 years or after any significant changes on applications with personal data to revaluate the risk level caused by given personal data processing. Any documented results of every DPIA should be reported to the GDPO by the relevant LPP of the legal entity.

7.4 Managing Personal Data Breach

Any employee who suspects that a Personal Data Breach has occurred due to theft or exposure of personal data must immediately notify the LPP or the GDPO providing a description of what occurred. Every legal entity provides contact name and contact phone number or email to report the breach in the local language.

The GDPO will coordinate investigatoins all reported major incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach with **risk** or **high risk** to individual`s rights and freedoms is confirmed, the relevant authorised procedure based on the criticality and quantity of the personal data involved has to be performed.

In case of a Personal Data Breach with risks to rights and freedoms of individuals, Alpiq entity shall without undue delay and, where feasible, **not later than 72 hours after having become aware** of it, **notify** the Personal Data Breach to the relevant Data Protection Authority. Where the notification to the supervisory authority is not made **within 72 hours**, it shall be accompanied by reasons for the delay. GDPO must be involved in the notification process.

When the Personal Data Breach is likely to result in a **high risk** to the rights and freedoms of individuals, the Alpiq legal entity shall **communicate** the Personal Data Breach to the Data Subject **without undue delay**. Communication can be made individually (e.g. by sending e-mail) or by using public channels. For Personal Data Breaches with high potential risk on rights and freedoms of individuals the GDPO will initiate the Crisis Management Team (MIK) to coordinate and manage the Personal Data Breach response according to Handbook MIK [3].

Data Breach **Notification** and Data Breach **Communication** are highly sensitive cases, which could have impact on the image/reputation of the Alpiq Group. Therefore every Alpiq legal entity shall have emergency plan to manage such Data Breach on professional way. Every Personal Data Breach (with no risk, with risk or with high risk) must be documented by the responsible LPP. The mandatory roles and responsibilities defined in this Implementation Provision must be appointed by each Alpiq entity. This is requested for appropriate Emercency Organisation. A Data Breach Notification and Communication must be trained and tested.

7.5 Personal Data Transfer

7.5.1 Data Transfers

Alpiq entities may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism.

Alpiq Entities may only transfer personal data where one of the scenarios list below applies:

- The Data Subject has given consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

For a list of countries recognised as having an adequate level of legal protection see Appendix B. If a country is not on this list, it has to be considered as "third country".

For a list of third country transfer mechanisms recognised as providing adequate protection see Appendix C.

7.5.2 Data Transfer to Third Parties and Personal Data Processing Agreements

Each Alpiq entity will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, each Alpiq entity will first identify if, under applicable law, the third party is considered a Data Controller or a Data Processor of the personal data being transferred.

Where the third party is deemed to be a Data Controller, the Alpiq entity will set an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the personal data transferred (e.g. by Model Clauses, see Appendix B).

Where the third party is deemed to be a Data Processor, the Alpiq entity will set an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with Alpiq instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification in case of Personal Data Breaches.

When an Alpiq entity is outsourcing services to a third party (including Cloud Computing services), they shall identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case, it will make sure to include, in cooperation with the GDPO, adequate procedures in the outsourcing agreement for such personal data processing and third country transfers. In addition, each Alpiq entity will make sure all third parties engaged to process personal data on their behalf in the premisses of Alpiq are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Alpiq.

7.5.3 Cross Border Data Transfer Between Alpiq Entities

In order to carry out Alpiq's operations effectively across its various entities, there might be occasions when it is necessary to transfer personal data from one Alpiq entity to another, or to allow access to the personal data from an abroad location. Should this occur, the Alpiq entity sending the personal data remains responsible for ensuring protection for that personal data.

Alpiq handles the transfer of personal data between entities, where the location of the recipient entity is a third country, using the "Data Transfer Agreement". Data Transfer Agreement provides legally binding and enforceable rights on Data Subjects with regard to the processing of their personal data.

When transferring personal data to another Alpiq entity located in a third country, it shall be ensured that:

- The recipient Alpiq entity signed already the Data Transfer Agreement
- Transfer only the most necessary personal data for the particular purpose of the business (for example, to fulfil a transaction or carry out a particular service) is transferred
- Adequate security measures are applied to protect the personal data during the transfer (including password-protection and encryption, where necessary)

7.6 Data Subject Rights

7.6.1 Cross Data Subject Requests

The GDPO (GDPO) provides a privacy tool to enable and facilitate the Alpiq entities in the exercise of Data Subject Rights related to:

- Information access
- Objection to Processing
- Objection to automated decision-making and profiling
- Restriction of Processing
- Data rectification
- Data erasure

If an individual makes a request relating to any of the rights listed above, Alpiq entity shall consider each such requests in accordance with all applicable Data Protection laws and regulations.

To enable Data Subject requests Alpiq entity shall provide on every privacy notice the contact details for requests (postal address, email or internet link to the request form).

All requests received for access or rectification of personal data must be directed to the internal department responsible for data processing. LPP or in complex cases the GDPO supports respond to the request.

7.6.2 Law Enforcement Requests and Disclosures

In certain circumstances, it is permitted that personal data are shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law

If an Alpiq entity processes personal for one of these purposes, then it may apply an exception to the processing rules outlined in this Policy but only to the extent that not doing so would be likely to prejudice the case.

If any Alpiq entity receives a request from a court or any regulatory or law enforcement authority for information relating to an Alpiq contact, the GDPO must be notified immediately.

7.6.3 Profiling and Automated Decision-Making

Alpiq will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform a contract with the Data Subject or where it is authorised by law.

Where an Alpiq entity utilises profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view
- Obtain an explanation for the automated decision
- Review the logic used by the automated system
- Supplement the automated system with additional data
- Have a point of contact to review of the automated decision by Alpiq's person
- Contest the automated decision
- Object to the automated decision-making being carried out

Each Alpiq entity must also ensure that all profiling and automated decision-making relating to a Data Subject is based on accurate data.

7.6.4 Complaints Handling

Data Subjects with a complaint about the processing of their personal data should address the matter in writing to the LPP or GDPO. The LPP or GDPO will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period of time.

If the issue cannot be resolved through consultation between the Data Subject and LPP, then the Data Subject may, at its option, address the complaint to the Data Protection Authority within the applicable jurisdiction.

7.7 Privacy by Design/by Default

To ensure that all Data Privacy requirements are identified and addressed when designing/purchasing new applications/services/products or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an Data Privacy evaluation process at the early stage of the project. Each project concerning personal data processing should go through this gate of "Privacy by Design", which will be part of Alpiq Project Management Policy.

7.8 Security and Data Protection Classification

Each Alpiq entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised

alteration, access to personal data or processing, and other risks to which it may be exposed either by virtue of human action or the physical, natural environment or malware.

For more Details about Cyber & Information Security at Alpiq refer to Alpiq [4] and related implementation provisions.

Where the relation between the person and data is not necessary for the output of data processing anonymization or at least for pseudonymisation technics shall be applied. The access to the key code for pseudoanonymisation must be kept very restrictive.

Each private personal data of employee and customers, which was not previously opened to public shall be classified at Alpiq as "P2", which corresponds to confidentiality level C2 (Confidential). The personal data related to business (e.g. business phone number, e-mail, business address, etc.) and personal data used as security control like username (User ID) shall be classified at Alpiq as "P1", which corresponds to confidentiality level C1 (Internal). The special categories of personal data (sensitive personal data) at Alpiq shall be classified as "P2", which corresponds to confidentiality level C2 (Confidential). The classification of non-personal data "P0" must be done according to corresponding Information Security implementation provision for Information Classification.

7.9 Assessment and Monitoring

To confirm an adequate level of compliance that is being achieved by all Alpiq entities in relation to this Policy, the GDPO will carry out an annual Data Privacy compliance assessment for chosen entities.

The GDPO, in cooperation with key business stakeholders from each Alpiq entity, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Alpiq Executive Management.

7.10 Awareness and Trainings

All Alpiq employees having access to personal data will have their responsibilities under this Policy outlined to them as part of their staff introduction training. In addition, each Alpiq entity will provide regular Data Privacy training and procedural guidance for their staff. The training content can be defined by LPP in coordination with GDPO.

8 Exception Handling

Each exception from this Policy must be justified in writing. It will be accepted or rejected in a first instance by the GDPO.

In the case of disagreement on the handling of exceptions, the Head of Group Security & BCM takes the final decision.

Exceptions are granted only temporarily and will be periodically reviewed by the GDPO.

In case of non-compliance by employees and third parties, line management at appropriate level reserves the right to pronounce or induce appropriate sanctions or demand liability claims.

Appendix A Information Notification Duties to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not data has been obtained directly from the Data Subject.

Information Elements	**Data obtained directly from Data Subject**	**Data <u>not</u> obtained directly from Data Subject**
Identity and contact details of the controller (and where applicable, the controller's representative) and the (Group) Data Privacy Officer	X	X
Purpose of the processing and the lawful basis for the processing, no open-ended set of processing activities (not relevant for withdrawal but for policies)	X	X
The legitimate interests of the controller or third party (where applicable) (not relevant for withdrawal but for policies)	X	X
Categories of personal data	---	X
Any recipient or categories of recipients of the personal data	X	X
Details of transfers to third country and safeguards	X	X
Retention period or criteria used to determine the retention period	X	X
The existence of each of Data Subject's rights	X	X
The right to withdraw consent at any time (where relevant)	X	X
The right to lodge a complaint with a supervisory authority	X	X
The source the personal data originates from and whether it came from publicly accessible sources	---	X
Whether the procedure of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data (not relevant for withdrawal but for policies)	X	---

Appendix B Adequacy For Personal Data Transfers

The following list contains countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of their personal data:

- EU Countries: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK
- Iceland
- Liechtenstein
- Norway
- Andorra
- Argentina
- Canada (commercial organisations)
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay

Appendix C Adequacy For Personal Data Transfers

The following reflects a list of third country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

- Appropriate safeguards:
  - Model Clauses
  - Binding Corporate Rules
  - Codes of Conduct
  - Certification Mechanisms
- Derogations:
  - Explicit Consent
  - Compelling Legitimate Interests
  - Important reasons of Public Interest
  - Transfers in response to a foreign legal requirement
  - DPA approved contracts between Data Controllers and Data Processors

--- End of Document ---