SOCIETE GENERALE
Insurance

PERSONAL DATA PROTECTION POLICY SGIP

Contents

SOCIETE GENERALE
Insurance

1. The GDPR has an impact on Societe Generale Insurance Polska (SGIP) [1]

1.1. What is the GDPR?

The General Data Protection Regulation (GDPR) refers to the European Regulation No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which entered into force on 25 May 2018.

The GDPR repeals Directive 95/46/EC, which previously regulated the issue of personal data protection. It thoroughly renews the legal framework for the protection of personal data.

The GDPR protects the data of individuals used in processing operations related to the activities of an organisation (businesses, local authorities, etc.).

It complements and reinforces existing national requirements:

- Strengthens an individual's place at the heart of the legal and technical data protection regime and offers them new rights or guarantees to enable them to better control their data.
- Introduces the responsibility of companies processing personal data, including data processors. Each of them, at its own level, must protect personal data by implementing organisational and technical measures tailored to the risks to the privacy of data subjects in relation to existing or new processing operations.
- Ratifies the need for tracking activities and controls, as well as the security of personal data (obligation to keep a register) and provides a framework for new technological practices (profiling, artificial intelligence and).
- Provides a framework for the processing and transfer of personal data to countries outside of the European Union.
- Expands the scope of exchanges with supervisory authorities (obligation to notify of personal data breaches, prior consultation in the case of high-risk processing operations) and strengthens the regulator's control and sanctioning powers.

The GDPR provides a framework for:

- **collection,**
- **use,**
- **and the storage/deletion of personal data.**

1.2. What does the GDPR constitute?

The GDPR provides for a number of basic principles that require personal data to be:

- processed on one of the six legal bases provided for in the GDPR (principle of lawfulness, §3.1.2),
- processed in a transparent manner for data subjects, who must be provided with information about the processing of their data at the time of collection (principle of transparency, §3.2),

[1] SGIP understood as Sogecap Branch in Poland and/or Sogessur Branch in Poland

- adequate, relevant and limited to what is necessary for the purposes for which they are processed (principle of minimization, §3.5.1),

- stored for no longer than is necessary to achieve the purpose for which they were collected (storage limitation principle, §3.1.3),

- protected against the risk of breach of confidentiality, integrity and availability, taking into account, in particular, the type of data (sensitive or not), the anticipated risks or the context (the principle of security of processing, §3.4).

Highlights - What You Need to Know

The GDPR protects the data of natural persons, and only natural persons.

The data of legal persons are not protected under the provisions of the GDPR.

1.3. What is personal data?

According to the GDPR, personal data is any data or information relating to an identified or identifiable, directly or indirectly, natural person. To simplify their identification and classification, personal data is often categorized as follows:

- identity, examples: surname, first name, date of birth, etc.

- personal life, examples: marital status, household composition, social media data, etc.

- professional life, examples: occupation, work experience, professional contact details, etc.

- economic and financial information, examples: income, assets, debt ratio, etc.

- login data, examples: IP address, phone IMEI number, computer MAC address, etc.

- location data, examples: smart car, phone geolocation, etc.

- ...

Some data is considered sensitive (listed in Articles 9 and 10 of the GDPR or specified as such by an EU member state). Their processing is subject to the principle of prohibition of processing with certain exceptions and under certain conditions.

This includes personal data relating to:

- racial or ethnic origin,

SGIP never processes this data as part of its activities,

- political views,

SGIP never processes this data as part of its activities,

- religious or philosophical beliefs,

SGIP never processes this data as part of its activities,

- trade union membership,

SGIP never processes this data as part of its activities,

- processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,

SGIP never processes this data as part of its activities,

- the health status of the person,

SGIP may process this data in the context of subscriptions and/or claims handling related to concluded insurance contracts,

- data concerning a natural person's sex life or sexual orientation,

SGIP never processes this data as part of its activities,

- personal data related to criminal convictions,

SGIP may process this data as part of AML-CFT or concluding motor insurance contracts.

Data that is anonymous at the time of collection or has undergone an irreversible anonymization process is not personal data, as it is not possible to identify a natural person from them.

Pseudonymised data (a reversible anonymisation process, e.g. replacing a surname with a unique identifier) remains personal data as long as natural persons can still be identified.

Highlights - What You Need to Know

Some personal data is more sensitive than others, and its processing is subject to limitations and conditions.

If the data has been anonymised and can no longer be traced back to a specific person, then it is no longer personal data.

1.4. Challenges facing SGIP

SGIP's activities involve the use of large amounts of personal data, some of which are sensitive in nature, and therefore SGIP is obliged to comply with applicable laws and regulations.

In this context, the protection of individuals in the collection and processing of personal data is a fundamental right and a strategic issue, necessary to maintain the trust of each entity's customers, partners and employees, as well as to protect the reputation of SGIP.

Therefore, failure to comply with the provisions of the GDPR exposes SGIP and the SOGECAP Group to penalties from the Personal Data Protection Authority (PUODO) of up to 4% of the total annual worldwide turnover, or EUR 20 million (whichever is higher).

SGIP is also exposed to possible civil lawsuits from data subjects and therefore to reputational risks.

Highlights - What You Need to Know

Responsibility for data protection lies both with each SOGECAP Group entity towards its local Data Protection Authority and with the head of the SOGECAP Group. As a result, a data breach, in one of its subsidiaries/branches, could have consequences for the entire SOGECAP Group.

1.5. Objectives of the personal data protection policy

The personal data protection policy is part of SGIP's regulatory and operational risk control strategy.

It also follows the Code of Société Générale, which in its Book B includes Chapter 3 – Data Principles, in which Section 2 details the organization, measures and rules related to the protection of personal data. The Personal Data Protection Policy details how to implement the principles contained in the Société Générale Code.

It is reviewed annually and updated in case of a significant event.

This document summarises the obligations under the GDPR. It also outlines the corporate governance and procedures that SGIP has put in place to ensure compliance with the regulation. It sets out the guiding principles for the protection of personal data.

This policy is built into the normative framework of SGIP (procedures, operational procedures).

Highlights - What You Need to Know

The Personal Data Protection Policy sets out the principles of personal data protection at SGIP. It is supplemented by procedures and standard operating procedures.

1.6. Policy scope

The GDPR applies to all organizations (companies, administrations, associations) based in the territory of a member state of the European Union. Thus, the GDPR applies to all subsidiaries and branches of the SOGECAP Group established in EU countries, including SGIP.

The GDPR also applies to organizations that are not based in the EU when selling products and services to people in the EU.

The principles of this policy are binding, by virtue of law and/or by agreement, to all processors cooperating with SGIP.

Highlights - What You Need to Know

The Personal Data Protection Policy applies to all European entities within the SOGECAP Group and to entities outside the EU that process data of individuals in the European Union.

2. Entities involved in the protection of personal data within SGIP

Individual entities involved in the protection of personal data within SGIP have been identified in the data processing register or in internal procedures for the processing of personal data. Each processing activity is linked to an organizational structure and a legal entity.

In addition, when creating or modifying a personal data processing operation, other stakeholders are mobilised to support the project or to provide their expertise in the field of personal data protection.

The data protection stakeholders listed in this policy have the same roles and responsibilities that are listed for these stakeholders in the Société Générale Code. Data protection stakeholders and their roles are divided into two lines of defense:

- Line of Defense 1: business departments that are responsible for processing related to their business. They are accompanied by supporting functions that help the "owners" of the processing: legal, security, etc.,

- Line of defence 2: The Data Protection Officer (DPO) who supports, supervises and monitors the activities of business departments (see §2.2).

Highlights - What You Need to Know

Business lines are fully responsible for the completeness of the record of personal data processing in their area of activity, for the compliance of their processing operations with the GDPR and for documenting compliance with the GDPR.

The Data Protection Officer supports the lines of business and checks the adequacy of the information collected.

2.1. Line of Defence 1 - Business lines are responsible for the processing of personal data related to their activities

Business stakeholders (product managers, project managers, application managers, etc.) who implement the processing of personal data are responsible, as the first line of defence, for compliance of processing with the GDPR and with SGIP's systems and procedures in this regard.

The first line of defence consists within business departments mainly of processing managers and owners, who are supported by experts.

First line defence personnel are responsible for:

- Applying the principles of the GDPR and this policy when conducting your projects.
- Ensuring that the record of processing activities is kept up to date within their department or division to ensure that it is always up to date.
- Carrying out the analysis and research required by the GDPR related to the processing operations they implement and to request the implementation of appropriate security measures.
- Seeking advice from the Data Protection Officer if you have any questions, concerns or difficulties you encounter in relation to the processing of personal data that you implement or handle.
- Informing the Data Protection Officer about detected non-compliance with the GDPR, as well as in the event of changes in tools and/or methods affecting the processing of personal data within their department.

2.1.1. Directors who are responsible for processing operations performed within their department

As part of their responsibilities, each director is responsible for the compliance with the GDPR of processing operations carried out within their department, in accordance with the record of personal data processing activities.

It is also the responsibility of each director to implement the recommendations given by the Data Protection Officer:

- for each new processing operation of personal data,
- In the event of any change to an existing processing operation of personal data,
- in the event of a personal data protection incident.

If it is not possible to implement the DPO's recommendations, the matter may be referred to arbitration by the Branch Director or another authority if the level of risk so requires.

2.1.2. Process owners, responsible for the compliance of the processing operations under their control

Any processing operation recorded in the register of personal data processing activities has an associated owner of the processing, either who is a director or reporting to a director. The owner of a processing operation is the person best qualified

to describe and update the processing operations and to answer questions from the Data Protection Authority in the event of a complaint or inspection. He acts as an expert.

The owners of the processing processes are, as a first line of defense, responsible for the operational implementation of the principles of this policy.

In particular, they are responsible for assessing the risks that their processing may pose to data subjects and for carrying out the necessary analyses. These analyses make it possible to measure the level of inherent risk in the processing operation and to identify possible risk mitigation actions to be implemented.

2.1.3 Support functions assist the owners of processing operations: Legal Department, IT Security, etc.

The manager responsible for procurement at SGIP is also responsible for data protection issues in the procurement process. Ensures that new or renegotiated subcontracts contain clauses and annexes on the protection of personal data and security in accordance with applicable laws and Group practices in this regard.

The legal department is responsible for negotiating and drafting personal data clauses in contracts. It is responsible for monitoring legal and regulatory requirements related to the protection of personal data. Sets out the legal or regulatory retention period for personal data. Defines, drafts or approves legal notes, which must be included in all pre-contractual and contractual documents used under SGIP. Finally, it provides legal support to lines of business when creating or modifying processing operations.

The IT Security Manager plays a major role in ensuring SGIP's compliance with the GDPR, as he supports and advises business lines on technical measures to protect personal data and, if necessary, implements these measures.

2.2. Line of Defence 2 - Stakeholders who support and oversee the compliance of processing operations data

The main tasks of the second line of defence (LOD2) are:

- ensuring that the data protection mechanisms in SGIP comply with the regulations,
- defining and ensuring the validation of operational mechanisms related to the management of personal data in SGIP,
- supporting SGIP departments in all matters related to data protection,
- managing requests for the exercise of rights under the GDPR and personal data breaches affecting SGIP,
- managing and coordinating work related to the identification of personal data processing operations in SGIP and their supervision, including in particular conducting analyses and impact assessments required by the GDPR, as well as monitoring action plans related to these analyses,
- to be the point of contact for supervisory authorities in the event of a complaint or inspection, - to monitor data protection activities by means of risk indicators.

SOGECAP has established a second line of defence to manage data protection within the Group:

- The SOGECAP Group Data Protection Officer (hereinafter referred to as the ASSU DPO), who provides functional oversight of the SOGECAP Group's data protection officers or data protection correspondents,
- Data Protection Officers (DPOs) or Data Protection Correspondents (DPCs) appointed at subsidiary and branch level and reported to the competent data protection authorities where necessary in accordance with applicable legislation.

To ensure the effectiveness of their mission as a second line of defence, DPOs/DPCs rely on the first line of defence that contributes to the compliance of the data protection system.

GDPR compliance is part of the system of continuous and periodic control established in SGIP.

2.2.1. ASSU's Data Protection Officer, as the leader of the SOGECAP Group's data protection policy

ASSU DPO must ensure, within the area for which it is responsible, compliance with the GDPR. He/she must be involved, in an appropriate and timely manner, in all matters related to the protection of personal data.

This goal is mainly achieved through the missions described below:

- ensuring the overall management of the data protection system and ensuring the consistency of the systems across the consolidated area of all SOGECAP Group entities,
- verification of the implementation of this policy,
- alerting the data controller of any breaches or non-compliance with this policy,
- supervising individual DPOs and DPCs,
- ensuring the implementation of a plan for continuous control of the personal data protection system that will be applied by each SOGECAP Group entity,
- defining and implementing a training, awareness raising and communication plan for all those involved in the protection of personal data in the Group,
- leading the network of compliance correspondents and ensuring coordination with the lines of business and functions in their unit,
- advising the controller, owners of business lines processing data, data processors and employees who process personal data,
- leading and coordinating work on the protection of personal data, including data protection impact assessments,
- ensuring that the register of processing activities is properly kept and updated,
- responding to complaints and requests from data subjects regarding the exercise of their rights,
- investigating and documenting personal data breaches and, if necessary, reporting them to the data protection authority,
- to be the point of contact for supervisory authorities in case of complaints, requests or inspections,
- ensuring proper documentation of activities carried out in the context of personal data protection management (DPO's opinions, recommendations, control of the implementation of action plans, etc.).

2.2.2. The DPO/DPC of international entities, responsible for data protection within their entity

The Data Protection Officer at SGIP performs the same tasks as the ASSU DPO within the SOGECAP Group. Under the functional supervision of the ASSU, the DPO coordinates the activities in matters that require it.

His/her tasks in this area are similar to those of ASSU DPO, to which it is functionally subordinated: ensuring compliance of its unit with the GDPR and locally applicable personal data protection regulations, and implementing the personal data protection policy and related procedures.

2.3. Authorities and functioning of the personal data protection system

SOGECAP has established a governance structure for its data protection system, which includes several committees, the members, frequency and objectives of which are described below. These committees are headed by ASSU DPO.

2.3.1. SOGECAP internal committees

GDPR Strategic Committee

This committee meets ad hoc when issues arise that need to be referred to the Management Board. DPO and Chief Compliance Officer presents progress in GDPR implementation and data protection risk areas to the SOGECAP Executive Committee, as well as the main quantitative and qualitative indicators needed for decision-making.

Personal Data Protection Committee

This committee gathers, on a monthly basis, the Secretary-General, representatives of the Legal Department and the Compliance Department, including the Data Protection Department, members of the Executive Committee responsible for business development, the Director of Marketing and the Director of DATA HUB, to discuss issues related to the use of data for the following purposes:

- business development, both within the SOGECAP Group and in cooperation with distributors,
- Improving customer knowledge, both within the SOGECAP Group and in cooperation with distributors.

Depending on the agenda, other participants may be invited.

Committees with the participation of the DPO/DPC of subsidiaries and branches of the SOGECAP Group

The purpose of DPO/DPC SOGECAP Group's Data Protection Committee is to inform and discuss data protection issues with the DPOs and the DPC. In particular, the Committee leads the implementation of the GDPR in subsidiaries by responding to the problems they face.

This committee, chaired by the ASSU DPO, brings together the DPOs and the DPC. Meetings are held every two months.

Quarterly Compliance Committee

ASSU DPO and SGIP DPO attend quarterly meetings of the Compliance Committee. During the meeting, the SGIP DPO presents the most important issues regarding the protection of personal data in their branch.

2.3.2. External committees to SOGECAP Group

The DPO Committee of the SOCIETE GENERALE Group

ASSU DPO participates in committee meetings, which are held monthly and are designed to oversee and inform local DPOs and DPCs of the SOCIETE GENERALE Group.

Bilateral meetings of ASSU DPO/distributors' DPO

ASSU DPO organizes regular meetings, exchanges with the DPO of its main distributors.

The aim of these meetings, which take place every two months, is to exchange views on current events or specific topics of common interest.

3. Main challenges related to the personal data protection

3.1. Supervision of the processing of personal data

3.1.1. Having an up-to-date record of data processing activities in order to obtain a comprehensive knowledge of the processing operations carried out by SGIP

The register of data processing activities contains a list and description of all personal data processing operations carried out by SGIP. It must be kept up to date and can be reviewed by the supervisory authorities at any time. Each processing operation must be entered in the register of processing activities with all the information before it is carried out for the first time.

The register shall detail the essential characteristics of each processing operation. In particular, the register must contain at least the following information for each processing operation:

- name and contact details of the owner of the processing, i.e. the person who can best answer questions about the processing and the data being processed,
- purposes of processing (e.g. performance of insurance contracts),
- legal basis for the processing and its justification (see §3.1.2 below),
- description of the categories of data subjects (e.g. customers, prospects, employees, job seekers) and the categories of personal data (e.g. identity data, financial data, geolocation),
- recipients of this data, especially outside the EU,
- data retention periods (repository available on SGIP SharePoint),
- general description of the technical and organisational security measures.

SOGECAP as a whole and SGIP have identified all data processing operations related to its business.

Highlights - What You Need to Know

The register of data processing activities contains all information related to personal data processing operations. This information must be entered in the register before processing and updated at least once a year.

3.1.2. Lawful processing of data within the legal framework of the GDPR

In order for data processing to comply with the principle of lawfulness, it must be based on one of the six legal bases provided for in the GDPR:

- performance of a contract with the data subject (from proposal to termination of the contract),
- processing is necessary to fulfil a legal obligation of the controller,
- implementation of the legitimate interest of the Administrator or a third party, provided that this interest is precisely defined and documented, communicated to the data subjects and outweighs their interests, freedoms and fundamental rights,
- consent given by the data subject,
- protection of 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 the public authority entrusted to the controller.

For each processing operation, the processing basis chosen must be justified.

Where the legal basis for the processing operation is legitimate interest, the controller must assess the risks and benefits of the conditions under which the processing is to be carried out.

This analysis should be formalised in a document called the assessment of legitimate interest (LIA).

Highlights - What You Need to Know

Each data processing operation must be based on one of the six legal bases provided for in the GDPR. The choice of legal basis must be documented.

3.1.3. Determination of data retention periods in accordance with the purposes of processing

Data retention periods are most often determined by reference to legal or regulatory obligations or rules regarding legal limitation periods. They must necessarily be identified in accordance with the purpose of each processing operation and documented.

They cannot be unlimited. The SGIP Legal Department has developed, together with the owners of processing operations, a repository of data retention periods, available in a dedicated document on SGIP SharePoint.

Most processing operations are included in the retention period repository.

In the case of a specific retention period that does not appear in the repository, or where the data controller needs to retain data outside of legal obligations, the selected retention period must be justified and communicated to the DPO team for validation.

The retention periods listed in the repository are the periods used to implement technical mechanisms leading to the deletion or anonymisation of personal data, the implementation of which is supervised by the Data Protection Officer.

Highlights - What You Need to Know

SGIP must delete or anonymize personal data for which the retention period has expired.

3.1.4. Carry out a privacy risk assessment of each of the processing operations listed in register

Where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the controller must carry out a privacy impact assessment (PIA).

Therefore, for each new processing operation or significant update of a processing operation, the owner of the processing operation should verify whether it is necessary to carry out a PIA.

To this end, the owner of the processing, with the participation of the project manager, fills in a document called PRE PIA, which allows for an analysis of the privacy risks associated with the processing of personal data, using a tool provided by the SOGECAP Group. The PRE PIA contains nine questions defined by the European Data Protection Board, which is an association of European data protection authorities, to which the process owner provides a Yes or No answer. Each answer must be justified.

The PRE PIA is then sent to the DPO for approval and decision on whether or not to conduct the PIA.

If a PIA is required, the processing owner fills in a document provided by the SOGECAP Group, which consists of 4 tabs numbered from 0 to 3. The processing owner should fill in tabs 0 and 1 for the description of the processing operation. IT security should fill in tab 2 and describe the security measures used. The Data Protection Officer is responsible for Sheet 3 corresponding to the risk analysis.

The DPO gives an opinion on the processing and may define action plans if necessary.

If the PIA reveals that the residual risk remains high, the DPO issues an opinion against the implementation of the processing, informs the owner of the processing and escalates to the appropriate persons if necessary.

Highlights - What You Need to Know

For each processing operation, a privacy risk analysis must be performed: Initial Privacy Risk Assessment (PRE PIA)

If the risk is considered high, a detailed analysis is carried out: PIA.

3.1.5. Regulation of cross-border processing and transfers of data through the adoption of specific measures

The transfer of personal data from an organisation located in the European Economic Area (EEA) to an organisation located in a non-EEA country (a third country) must be accompanied by one of the appropriate safeguards listed in the GDPR.

This legal obligation is intended to ensure that the data transferred is provided with a level of protection equivalent to that applicable in the European Union. Data transfers within the EEA are not subject to this obligation.

SGIP ensures that the necessary safeguards are implemented whenever the processing operation requires the transfer of data outside the EEA. These provisions apply to the transfer of personal data between entities of the Société Générale Group, as well as the transfer of data by the same entities to a third party located outside the EEA (e.g. service providers).

With regard to data related to human resources: The Société Générale Group drew up Binding Corporate Rules and had them approved on 16/07/2013 by the French regulator CNIL. These rules in themselves constitute an appropriate safeguard under the GDPR. The transfer of this data may take place without a specific contractual framework, provided that it falls within one of the purposes set out in this document.

For data other than HR data: it is necessary to provide a framework for replacement through the guarantees recommended by the Société Générale Group.

Highlights - What You Need to Know

Any transfer of personal data outside the EEA must be supported by specific legal and IT measures.

3.2. Providing data subjects with all information related to the processing of their personal data

The GDPR expresses obligations to inform persons whose personal data are processed by SGIP. These persons may be employees, customers, potential customers or any other natural person who is a third party.

Persons whose personal data are processed must be informed of the:

- conditions for the use of their data: purpose, legal basis,

- recipients of their data,

- data retention period,

- their rights,

- the possibility of lodging a complaint with the competent data protection authority.

This information must be provided by the data controller at the time of the data collection. The information is mainly provided through contractual documentation or a website. They may also be transferred by the data processor on the basis of a contract.

There are 2 types of data collection:

- direct collection, where data is collected directly from individuals (e.g. form, subscription, etc.),

- indirect collection, when data is collected from a third party (e.g. data obtained from a partner, broker, public service).

SGIP communicates in a concise, transparent, understandable and easily accessible manner. In particular, it ensures that it uses terms that are clear and understandable to the people to whom the information is communicated.

In the case of indirect data collection, SGIP informs data subjects about the categories of processed data and the source of their origin, if they do not have this information at the time of its use (e.g. information on beneficiaries in life insurance at the time of death).

Highlights - What You Need to Know

Whenever SGIP collects personal data, it must inform the data subjects of

how they are used and their rights.

3.3. Responding to requests to exercise rights from data subjects

The data subjects affected by the processing of personal data may be customers, employees, service providers, potential customers, contact persons, suppliers, company directors, etc.

These entities have the right to:

- access to your data,

- rectification of erroneous data,

- to data erasure ("right to be forgotten)"),

- for data portability,

- object to the processing of their data

- restrict the processing of their data,

- not to be a subject to purely automated decisions, including profiling of the.

Each of these rights has a specific scope of application, which may sometimes limit or delay their implementation.

And so, the customer cannot request the erasure of their data immediately after the termination of the contract, nor can they demand the rectification of another person's data.

The deadline for responding to requests for exercise of rights is 30 days from receipt of the request, but it may be extended by 60 days for complex requests. The Data Protection Officer keeps a register of requests for GDPR rights.

Highlights - What You Need to Know

SGIP must respond to requests for the exercise of rights within 30 days

3.4. Implementing the measures necessary to ensure the security of personal data

3.4.1. Minimization of the use of personal data - the principle of minimization

The principle of minimization states that personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

Compliance with the principle of minimisation means processing only the personal data that is necessary to achieve the purpose, both in terms of the duration of the processing and the amount of data processed or the number of persons having access to the personal data.

Therefore, SGIP may not use surnames/names/dates of birth if it can use a computer identifier instead. Similarly, the number of persons who can access the data must be limited, only to those whose task requires it, and only for the time necessary to process the data.

SGIP is committed to the principle of minimisation.

Highlights - What You Need to Know

The personal data processed and the number of persons having access to these PDs should always be limited to the necessary minimum.

3.4.2. Data protection by design and by default

Privacy by design means taking into account, already at the development and design stage of any new products, services or applications involving the processing of personal data, all the principles applicable in the GDPR, in particular security measures and the adoption of mechanisms to protect the rights of data subjects.

Compliance with the principle of data protection by default requires the application of the highest level of protection of personal data collected and processed, in particular limiting the scope of processed personal data to what is necessary to achieve the purpose.

SGIP is committed to implementing the principles of data protection by design and by default to limit the processing of data to what is strictly necessary to achieve the given purpose.

3.4.3. Implementation of appropriate technical and organisational measures

SGIP shall implement appropriate technical and organisational measures to guarantee a level of security adapted to the risk, in accordance with SGIP's information security and information systems security policy. Those measures must ensure

adequate security and confidentiality of the data, in particular to prevent them from:

- transfer (disclosure or disclosure) to unauthorized third parties,

- modification (changes, etc.),

- damage (accidental or unlawful destruction, loss, etc.).

These measures and ways are determined by information systems security managers. These are documented in regularly updated reference documents.

Therefore, SGIP takes into account the protection of personal data already at the design stage of contracts, products and IT systems. It ensures that the security of personal data is guaranteed during all operations for which it is collected, processed and stored, until it is deleted or anonymized.

Highlights - What You Need to Know

Processors must ensure that the applications they use have security measures appropriate to the sensitivity of the data being managed, or that the processes in place allow personal data to be processed with the required level of security.

3.4.4. Preventing and managing personal data breaches

A personal data breach is a security event, whether intentional or unintentional, in which the confidentiality, integrity or availability of personal data is compromised.

SGIP has built a normative corpus for managing personal data breaches that identifies stakeholders involved in dealing with a breach and their roles, available on SGIP SharePoint.

If a SGIP staff member finds himself in a situation where they:

- can access, change or delete personal data,

- and if they believe that they should not be able to do so, they shall notify the Data Protection

Officer without undue delay.

Any incident concerning the processing of personal data must be immediately reported to the Data Protection Officer, who analyzes the incident and assesses the level of risk.

The DPO makes a recommendation to the heads of the affected departments regarding the need to notify the competent supervisory authority or even the data subjects. If necessary, the competent supervisory authority shall be notified as soon as possible and no later than 72 hours after becoming aware of the breach.

The data owners involved (personal data breach within their scope), implement the necessary remediation actions as soon as possible and are responsible for notifying data subjects, if necessary, together with the Data Protection Officer.

The ASSU DPO must be informed prior to any notification to the supervisory authority by one of the subsidiaries or branches located in European territory and acts as liaison with the SOCIETE GENERALE Group DPO.

In the event of a breach affecting several data controllers in the SOGECAP Group, it is the responsibility of ASSU DPO to coordinate the analysis of the breach and its level of severity, which ensures that the responses given to the various Protection Authorities are uniform and coordinated.

Once an incident has been reported to the DPA, it is presented to the "Compliance Incident Committee" of the Société Générale Group.

Highlights - What You Need to Know

Personal data breaches should be immediately reported to the DPO.

Any reports to the Polish DPA must be made within 72 hours of the incident being discovered.

3.5. Managing relationships with service providers and processors

SGIP has a contractual framework for relations with partners processing personal data. Updates agreements with its partners on an ongoing basis and defines the roles and responsibilities of the partners.

An analysis is carried out systematically to determine whether SGIP is a "data controller", "joint controller", "separate data controller" or "processor".

- The Controller clearly and precisely defines the purposes and means of each of the personal data processing operations that it carries out. It instructs its processor(s) regarding, among other things, the retention period and deletion of personal data. Assesses the level of security of the processing of this data before concluding the contract.

- Where SGIP is a "Processor", it collects and processes personal data in strict accordance with applicable laws or a contract and in accordance with the instructions given to it by the Data Controller.

- If the purposes and means of a processing operation are determined jointly by two or more entities acting as controllers, they may be considered joint controllers of that processing operation. They should then define, in a transparent manner and in writing, their respective roles and responsibilities in relation to the processing operation.

SOGECAP Group provides a tool to help business lines define the line of relationship with their partner.

Appendixes

Appendix 1 Intranet link

The GDPR Intranet of the SOGECAP Group is accessible at https://sg-insurance.safe.socgen/fr/rgpd

Appendix 2 Documents

	Nazwa dokumentu	Status
1	Personal data protection policy	Validated
2	Personal data breach management procedure	Validated
3	Non-employee rights request management procedure	Validated
4	Employee rights request management procedure	Validated
5	Non-employee rights request management standard operating procedure	Validated
6	Employee rights request management standard operating procedure	Validated
7	PIA tool with user guide	Validated
8	Pre-PIA tool with user guide	Validated