Policy
Privacy by Design
&
Privacy by Default

Legal compliance with EU Regulation 2016/679

Document code: P012

Confidentiality: CONFIDENTIAL S'NCE GROUP – CLIENTS

REV.	DATE	DESCRIPTION	AUTHOR	VERIFICATION	APPROVAL
01	27/02/2024	Adaptation to ISO 27001:2022	Privacy team	Company Management IT team Privacy team	Company Management

History

REV.	DATA	DESCRIZIONE
00	04/07/2019	1st release
01	27/02/2024	Adaptation to ISO 27001:2022

INDEX

1 SCOPE OF THE DOCUMENT

Purpose of this document is to describe how S'NCE GROUP adopts (in its operations) the Privacy by Design and Privacy by Default principles, WHOSE application is required for compliance with EU Regulation 2016/679 (General Data Protection Regulation - GDPR).

More specifically, this document describes the processes implemented by S'NCE GROUP during the design, development, testing, release, MAINTENANCE and management of projects/systems, REQUESTED by Customers, that involve the processing of personal data, also considering the cases in which such systems, after being implemented, are accessed by S'NCE GROUP personnel to provide the services contracted with the Customers.

S'NCE GROUP delivers, upon request, this document to its customers who, as indicated by the GDPR, have the role of "Controller" or "Processor" and who need to be guaranteed by their suppliers to whom they assign the task of processing personal data on their behalf (such as S'NCE GROUP), with respect to the activities carried out and the technical-ORGANIZATIONAL measures applied, which must meet the requirements of the GDPR and effectively guarantee the security of personal data.

This document highlights the distinction of tasks and responsibilities between the Customer/Owner and the Supplier/Responsible person (S'NCE GROUP) with specific regard to the application of the principles of Privacy by Design and Privacy by Default

2 EU 2016/679 REGULATION

On May 25th, 2018, EU Regulation 2016/679 (General Data Protection Regulation - GDPR) on the protection of natural persons, with regard to the processing of their personal data and on the free movement of such data, came into force. Similarly, the new version of the Federal Data Protection Act (nFADP), which is substantially aligned with the GDPR, entered into force in Switzerland on 1.9.2023.

The GDPR (and the new FADP), while maintaining and strengthening the principles set out in European Directive 95/46 for the protection of the data subject (natural person) with regard to the processing of his/her personal data, introduces new requirements and standardises certain principles and rules. One of the highlights of the GDPR is undoubtedly the fact that the security of personal data is geared towards a governance framework rather than a list of fulfilments. The new provisions require full responsibility on the part of the *Controller* and the *Processor* to comply with the Regulation, to implement appropriate internal policies, organisational mechanisms and personal data security measures, and to demonstrate such accountability, compliance and adequacy ('accountability').

Among the most important innovations are those concerning the need to consider personal data security already at the design stage ('Privacy by Design') for any type of project involving the processing of personal data and by default ('Privacy by Default'); the need to analyse and

assess impacts and risks ('Data Protection Impact Assessment'); and the need to prepare a 'Register of Data Processing'. In the event of a personal data breach, it is necessary to notify the Control Authority and in certain cases also the data subjects ('Data Breach Notification').

The GDPR has unified the issues of personal data protection of natural persons in a new concept, aligning the requirements with international standards and best practices in information security and information technology.

This means that data controllers and data processors must not limit themselves to drawing up formal documents and applying predefined minimum security measures, but must make a real commitment to assessing the levels of risk of compromising the security of personal data (in terms of confidentiality, integrity and availability), to identifying and applying technical-organisational measures that are appropriate for risk management, to fulfilling all the formal and contractual requirements required, and thus to achieving the true objective of the law, i.e. to guarantee the security of the personal data of the persons concerned.

3 GDPR BASIC REQUIREMENTS

The GDPR sets out the rights and freedoms of natural persons with regard to the processing of their personal data and the basic principles, criteria and guidelines that must be applied to ensure the protection of personal data and the protection of the rights of data subjects.

The most important requirements are defined below.

RIGHT	DESCRIPTION
Right of access	The data subject shall have the right to obtain confirmation as to whether personal data relating to him or her are being processed and, if so, to obtain access to those data and to information on the purposes of the processing, the recipients of the data, the duration of the processing, any consequences of processing based on profiling
Right of rectification	Should personal data be inaccurate or incomplete, the data subject has the right to request their correction or supplementation
Right of deletion	Personal data files must be structured in such a way as to facilitate the execution of deletion requests, always bearing in mind that the deletion of data is not an absolute right of the data subject, but the organisation will have to verify whether the processed data should be retained for legal reasons or protection of overriding interests
Right to the restriction of processing	Personal data files must be structured in such a way that their processing can be easily restricted if the data subject eventually requests it for part/all the activities performed on the data
Right to data portability	The data subject shall have the opportunity to receive from the data controller in a structured, commonly used, and machine-readable format his or her personal data, and shall have the right to transmit them to another data controller without hindrance, where the processing is based on consent or on a contract and the processing is carried out by automated means
Right to object to the processing	The data subject may object at any time, on grounds relating to his/her situation, to the processing of his/her personal data

Prohibition of automated decision-making or profiling	The data subject has the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning him/her or significantly affects him/her.

CRITERIA	DESCRIPTION
Minimization	Implementation of technical and organisational measures to ensure that only the personal data necessary for each specific processing purpose are processed. This applies to the amount of personal data collected, the scope of the processing, the storage period and accessibility. Minimisation ensures that personal data are not made accessible to persons who, during normal business activities, have no need to process them.
Pseudonimization	Controlled modification of personal data files in such a way that personal data can no longer be attributed to the data subject, without the use of additional information (personal data must be stored separately and technical and organisational measures must be applied to ensure that they are not attributed to an identified or identifiable natural person)
Anonymization	Making personal data anonymous, i.e., making it impossible to identify the natural person to whom the data belong. Anonymised data can no longer be considered 'personal data'
Separation	Manage personal data by separating, partitioning, distributing and preventing different partitions from being rejoined
Aggregation	Process personal data at the highest possible level of aggregation, i.e., with the lowest possible degree of detail

GUIDELINE	DESCRIPTION
Consent to treatment	The consent expressed by the data subject must be based on an oral or written statement, including by electronic means. This may include, for example, checking a box on a website, filling in an electronic form, any unambiguous statement or action that clearly indicates that the data subject agrees to the proposed processing. Consent must precede the start of the processing and new consent will be required if the purpose of the processing changes.
Data limitation (appropriateness and relevance of data)	The data collected and processed must be strictly related to the purposes of the processing, in a minimum quantity, but complete and sufficient for the purposes to be achieved. Thus, the quantity of data must not exceed the purposes for which those data are to be processed.
Data retention	The definition of the 'appropriate' retention time for personal data is linked to objective criteria, the specific purposes of the processing and the retention time management policy defined by the Data Controller. Some retention periods are determined directly by law (e.g. tax purposes).

4 PRIVACY BY DESIGN & PRIVACY BY DEFAULT

Among the key principles of the GDPR are undoubtedly the following:

- Risk based approach
- Privacy by Design & Privacy by Default
- Accountability.

The risk-based approach consists in the need and opportunity to carry out, as the first activity of personal data protection management, an assessment of the level of risk for personal data to be compromised (in terms of the risk of lack of confidentiality, integrity and availability of the data) and, consequently, to adopt the technical-organisational measures that are 'adequate' to manage these levels of risk to an acceptable level.

The principle of Privacy by Design and Privacy by Default requires that security be 'thought out' beforehand ('by design'), during the conception and design phase of any new process/system that is to be activated, as well as every time that existing processes/systems are to be substantially modified, and not afterwards, once the data processing processes and systems are already in place. The principle also requires that the technical/organisational measures adopted are 'by default' capable of ensuring during processing that security is guaranteed.

Accountability requires the Data Controller and the Data Processor to be fully engaged and involved in achieving the primary objective of ensuring the security of personal data and the need to comply with the Regulation, to implement appropriate internal policies and organisational mechanisms for the management of personal data security and in demonstrating accountability, compliance and adequacy.

In EU Regulation 2016/679, it is defined that it is a clear intention of the legislator to make Data Controllers responsible and to 'shift' the responsibility for choices regarding personal data security onto them. It is therefore the Data Controllers, and not the legislators or the national Supervisory Authorities, who must determine and adopt the measures and procedures necessary to ensure the correct application of the Regulation and effective security of personal data, through a 'Risk-based' approach and by applying the principle of Privacy by Design and Privacy by Default.

We can summarise the principle of Privacy by Design and Privacy by Default in the following concepts:

- prevention: risks must be assessed in the preliminary design phase and the implemented system must prevent (not correct) the occurrence of problems
- privacy as a default setting: every feature of the process/system must guarantee 'a priori' compliance with the Regulation, with the rights of the individual and with data security requirements (e.g. by avoiding mechanisms that compulsorily require the imputation of personal data even if not strictly necessary for the purpose of processing)

- privacy built into the design: for example, through the extensive application of pseudonymisation and/or data minimisation techniques
- security throughout the product/service lifecycle
- visibility and transparency: at all operational stages of processing, verifiability and data protection must be evident
- centrality of the data subject: respecting the rights of the data subject, providing clear and timely responses to their requests, ensuring maximum transparency and functionality of the systems used by the data subject.

5 RESPONSIBILITIES OF THE PARTIES

Article 25 ('Data protection by design and protection by default') states in paragraph 1 that:

Taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of the processing, as well as risks having different probability and severity for the rights and freedoms of natural persons constituted by the processing, both at the time of determining the means of processing and at the time of the processing itself the DATA CONTROLLER shall implement appropriate technical and organisational measures... (omissis)... designed to implement effectively the principles of data protection... (omissis)... and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and to protect the rights of data subjects.

It is therefore the Data Controllers who must independently define the purposes and methods of data processing, assess the risks for the data subject that could occur as a result of a compromise of his or her personal data (in terms of lack of confidentiality, integrity and availability), implement the appropriate technical and organisational measures, ensure the lawfulness of processing and the collection of processing consents when necessary, define data retention requirements, assess when necessary and, where appropriate, carry out and document the impact assessment ('Data Protection Impact Assessment' - 'DPIA') .

Article 28 ('Data Controller') states in paragraph 1 that:

Where a processing operation is to be carried out on behalf of the DATA CONTROLLER, the latter shall have recourse only to DATA PROCESSORS providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of this Regulation and ensures the protection of the rights of the data subject.

S'NCE GROUP guarantees to its Customers/Owners the full compliance with the Regulation, the adoption of adequate technical and organisational measures in the development of the software and in the provision of its services, the application of an adequate personal data security governance process, in line with the requirements of the Regulation and provided for by the best practices and international standards on data, information and information systems security (e.g. ISO 27001:2022).

S'NCE GROUP, acting as Data Processor, guarantees the application of the fundamental principles of the "Risk based approach" and "Privacy by Design and Privacy by Default", operates in support of the Customer/Owner during the phases of defining the requirements of the requested product/service and, subsequently, governs the design of the systems and

guarantees the development of the software and the implementation of the appropriate security measures, in full compliance with the GDPR.

S'NCE GROUP shall not be held liable if the product/service does not comply with current regulations due to decisions of the Customer/owner that conflict with the advice and notices that S'NCE GROUP will send and/or in the event that the product/service has not been designed or created by S'NCE GROUP.

When applying the measures envisaged, the Controller and the Manager must always consider the nature of the data, the context and scope of the processing operations, the purposes and methods of processing, the various risks, as well as the state of the art of the technologies and their implementation costs.

6 APPOINTMENT AS DATA PROCESSOR

When the Customer (Controller) delegates to S'NCE GROUP (Controller) a processing of personal data on its behalf, a specific deed of appointment is signed, as provided for in Article 28 paragraph 3 of the GDPR.

Processing by a PROCESSOR shall be governed by a contract or other legal act pursuant to Union or Member State law, binding the PROCESSOR to the DATA CONTROLLER and stipulating the subject matter regulated and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations, and rights of the data controller... (omiss)...

As required by the law and in line with international best practices in information security management, S'NCE GROUP guarantees the selection of its suppliers and the stipulation with them of a specific "Appointment as Sub-Processor" deed that binds them to apply the same data management methods and the same types of appropriate security measures that S'NCE GROUP has agreed with the Customer/Owner.

In addition, S'NCE GROUP guarantees the selection and training of the staff employed and the stipulation, with all employees who for work purposes process personal data, of a specific deed of "Appointment as Personal Data Processing Authorised Officer" and, in case employees manage the processing systems with which personal data processing is carried out, of a specific deed of "Appointment as System Administrator".

Finally, S'NCE GROUP guarantees that all employees, or third parties, who access company information, but who do not "process" personal data, i.e., do not hold the role of Processor, sign a "Confidentiality Agreement". Access to company information is not granted before signing the NDA.

7 PRIVACY BY DESIGN & SW DEVELOPMENT LIFECYCLE

S'NCE GROUP considers a cycle of six key activities in the software development process, aligned with the principles of Privacy by Design and Privacy by Default.

A. Training

Understanding the concepts of data protection and information security is a prerequisite for the development of software based on Privacy by Design and Privacy by Default. Employees and contractors are sensitised and trained in the adoption of tools and working methodologies that enable data protection and information security.

S'nce Group organises a common, company-wide training plan, as well as specific plans for individual employees and collaborators whose roles are more involved in data protection and information security issues.

Training at a general level includes the impact and risk assessment methodology, the definition of data, information and information security requirements, the main regulatory aspects, the rights of data subjects and data protection principles and guidelines. Where necessary, the training extends to specific requirements related to the subject area, sector or industry for which an application is to be developed.

B. Requisites

For the application of the Privacy by Design and Privacy by Default principles, the requirements of the software must be defined in detail prior to development.

By identifying which categories of personal data will be collected, displayed, processed, transmitted and stored by the computer system, the correct data protection and information security requirements are established (appropriate technical and organisational measures, data retention times, risk tolerance levels, etc.).

Upstream of the requirements definition process is the assessment of risk levels. The security measures to be implemented must be 'adequate' with respect to the risk levels present.

If the risk levels are high, a specific 'Data Protection Impact Assessment' should be carried out, as required by the legislation, by the Data Controller. S'NCE GROUP, in its role as Data Processor, supports the Data Controller on request in the assessments that are specifically the responsibility of the Data Processor and, in particular, with regard to the data security measures applied by the software.

The fundamental principles and criteria that must inspire the definition of requirements are: risk assessment; limitation of processing according to the purposes; regulation of access according to the 'need to know' principle and access control needs; data minimisation; application of pseudonymisation, encryption, anonymisation; management of data storage and accessibility times; tracking of data access and processing operations; and communication security.

In addition, with regard to the definition of requirements, one must also consider the obligations that will have to be fulfilled once the software is released and used. Therefore, it is necessary to define the requirements so that the following activities can be managed: deletion of data at the end of the storage period; responding to requests from data subjects to exercise their rights (such as access to their data, rectification of data, restriction of processing, etc.); management of anomalies and incidents; etc.; activities that may be managed in a direct or assisted manner depending on the context and technical possibilities.

Examples of requirements geared towards data security and respect for the rights and freedoms of natural persons regarding the processing of their personal data are:

- Conceal and protect: personal data and their interrelationships must not be disclosed, processed or stored in an explicit form (use of pseudonymisation, encryption and/or aggregation).
- Separation: where possible, the data of a data subject should be divided into separate files. Separation is also an effective means to achieve the purpose of limitation.
- Aggregation: where possible, personal data are collected and processed with as much aggregation as possible. Examples include reducing the detail and sensitivity of personal data about individuals and removing unnecessary or excessive information.
- Information: Software must be designed and configured in such a way that the data subject is adequately informed about how personal data are processed. The application, using clear language, must provide information on what personal data are used, and how.

- Control: data subjects must have the possibility to control their personal data, either directly (where possible) or indirectly. This includes the right to access, update and/or delete one's own data.

Risk levels and requirements are considered an integral part of the project plan and monitored during the development process. Whenever the risk level is assessed to be higher than the predetermined level of acceptable risk, S'NCE GROUP shall inform the Data Controller of the need to implement measures to mitigate the risk.

C. Design

The concept of Privacy by Design is applied by the S'NCE GROUP already from the application design phase, possibly also involving third parties.

The software design activity must guarantee the implementation of the defined requirements.

Two simple examples:

- in cases where the user needs to be able to see his or her own consents, security settings and configurations, and needs to be able to manage his or her own passwords, the system must be designed in such a way as to allow identity and access management and, therefore, so that the person concerned can exercise these rights as easily as possible
- in the case of applications exposed on the Internet, proper management of input and output prevents risks such as code injection, modification of values in databases through SQL injection, installation of malware on a computer at the same time as unsafe web browsing, etc.

D. Development

S'NCE GROUP uses numerous tools and specific processes and frameworks for software development and roll-out. Sometimes, third-party tools (e.g. functions, APIs, libraries and modules) are also used, depending on need and convenience. Among the technologies used are so-called 'Privacy-Enhancing Technologies' (PETs) that foster the inherent confidentiality of personal data (e.g. encryption, protocols for anonymous communication, attribute-based credentials, etc.).

The entire software development process is governed by a specific operating procedure and provides for specific verification and approval phases, also with regard to the tools to be used.

During the development phase, static code analysis and code review activities are also foreseen, performed with a view to preventing vulnerabilities.

E. Testing

S'nce Group verifies that the requirements for data protection and data security, defined in the project analysis phase, have been implemented by carrying out appropriate tests. The verification, where applicable, also includes new components introduced after the main development process. For testing, internal guidelines provide for the use of pseudonymised, anonymised and minimal personal data.

Security tests are also planned to discover vulnerabilities and ensure that the code adequately safeguards security and data protection. Whenever possible, testing is carried out in both static and dynamic modes.

In order to detect vulnerabilities more thoroughly, S'nce Group is available to organise penetration tests and vulnerability analyses at the customer's request.

F. Systems maintenance and incident management

In order to guarantee an adequate level of protection of company information, its confidentiality, integrity and authenticity, S'NCE GROUP carries out specific system maintenance and management activities, in compliance with specific rules, guidelines and operating procedures.

Among these:

- Backup/Restore management
- Tracking of activities, anomalies and threats on systems, for particular applications and/or data (logging and monitoring)
- Management and control of the corporate network through specific tools (e.g. firewalls, etc.)

- Patch management.

In addition, the S'NCE GROUP has regulated, also at application level, a plan for the management of personal data incidents. The plan defines what comprises an incident and its lifecycle (e.g. detection, analysis, reporting, management and normalisation) and can be tailored to the specific project. Incidents are also reported to a dedicated Privacy Governance team.

S'NCE GROUP has also defined a critical incident response plan, which regulates the actions to be taken in relation to the different scenarios that might occur.

8 ISO 27001 CERTIFICATION

Article 25 of the GDPR encourages the adoption of special data protection certification mechanisms, with the precise function of enabling Data Controllers and Processors to demonstrate compliance with the Regulation.

S'NCE GROUP obtained the first ISO 27001 certification on its processes in 2019 and has been able to successfully face with inspection audits to date, getting the ISO 27001:2022 certification.

The decision to pursue ISO 27001 certification is linked to the commitment and accountability of the S'NCE GROUP's management, in order to guarantee its customers the confidentiality, integrity, availability and regulatory compliance of its services and processes and, among other things, thereby demonstrating full compliance with the principle of Privacy by Design and Privacy by Default.

In order to guarantee high levels of security, S'NCE GROUP is available to Clients to evaluate the possibility of applying the ISO 27001:2022 standard to their projects.