



DATA PROTECTION BY DESIGN AND DPIA POLICY



TABLE OF CONTENTS

1.	Legal framework and purpose of the policy	3
2.	Scope of application of the policy	3
3.	Definitions	4
4.	Roles and responsibilities	4
5.	General principles of data protection by design and by default	6
6.	Methodology	7
A.	Detection of risky data processing: eligibility study	7
B.	Conduct a full dpia	8
7.	Compliance adapted to the risk level	10
8.	Policy update	11
9.	Reference	11
10.	Revision history	11



1. Legal framework and purpose of the policy

Streff - Data Protection Services (PSF) S.à r.l. and **Albert Streff S.à r.l. et Cie SECS** (hereinafter « **Streff** ») collects, handles, stores, and processes Personal data about employees, clients, partners, and suppliers. Data protection aims to protect individuals against unauthorised or unlawful uses of their Personal Data. This protection is intended to be proactive and preventive.

The GDPR imposes on data controllers the obligation to implement appropriate measures and necessary safeguards that provide effective implementation of the data protection principles and, consequently, data subjects' rights and freedoms by design and by default. This obligation is set out in the following articles of the GDPR:

- art. 25: Data protection by design and by default,
- art. 32: Security of processing,
- art. 35: Data protection impact assessment,
- art. 36: Prior consultation of the supervisory authority.

In particular, if the data Processing presents a high level of risk for the data subject, a Data Protection Impact Assessment (DPIA) must be carried out and documented with the aim to identifying and implementing adequate data protection measures.

The purpose of this Data Protection by Design and DPIA policy (hereinafter the "Policy") is to:

- describe the operational principles of Data Protection by Design and by Default.
- define a simple, pragmatic methodology adapted to Streff's environment for effective and documented follow-up of new projects involving personal data.
- ensure the identification of risks to the rights and freedoms of data subjects and perform a Data Protection Impact Assessment when the identified risks are high.

2. Scope of application of the policy

This Policy covers all Personal data, regardless of the format of storage (paper or digital), wherever stored or in transit on any type of media, and all Streff's information Processing systems.

It applies to all new Processing activities of personal data, and to the modification of existing data Processing.

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



3. Definitions

In this Policy, the following terms have the following meanings:

- **CNPD** (Commission Nationale pour la Protection des Données) is the Luxembourg data protection supervisory authority.
- **Controller**: the natural or legal person, public authority, department, or other body which determines the purposes and means of processing personal data.
- **Data subject**: identified or identifiable natural person.
- **DPO**: Data Protection Officer, as defined in Article 37 of the GDPR.
- **Personal data**: any information relating to an identified or identifiable natural person (hereinafter referred to as data subject).
- **Processor**: the natural or legal person, public authority, agency, or other body which processes Personal data on behalf of the controller.
- **Processing**: any operation or set of operations which is performed on Personal data or on sets of personal data, whether or not by automated means, such as 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.

4. Roles and responsibilities

Responsible member of the management board:

- formally approves this Policy and all related documents.
- is responsible for the compliance of all Streff Personal data Processing activities.
- approves the result of a DPIA.
- following the DPO's analysis, takes the decision to consult the supervisory authority prior to the Processing, if the DPIA shows that the Processing would result in a high risk for the data subject due to the absence of appropriate measures to mitigate the risk to an acceptable level.

Accountable Managers

For each project or data Processing within their scope, each Accountable Manager shall:

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



- ensure that the DPO is informed of all new projects involving Personal data or changes to existing data Processing operations;
- Actively support the DPO in performing the DPIA
- ensure that its service and staff communicate and cooperate with the DPO in an efficient and satisfactory manner in the management of the data protection analysis;
- following analysis carried out to determine whether a Data Protection Impact Assessment is either required or recommended, ensure such DPIA is carried out.

The IT Manager:

- analyses risks related to Personal data including in case of DPIA;
- defines organisational and technical measures to mitigate the risks;
- controls the implementation and effectiveness of organisational and technical measures;
- designs the action plan(s) aimed at improving the coverage of risks to the rights and freedom of the data subjects.

Data protection Officer (DPO)

The DPO ensures that Streff complies with its obligations regarding the protection of personal data. To this end, the DPO:

- advises Streff on the implementation of this Policy;
- ensures the proper integration of the data protection principles upstream of new data Processing projects and the modification of existing data Processing activities;
- helps project owner/processing owner to perform analysis to determine whether a DPIA is recommended or requested;
- assists the project owner/processing owner for the performance of DPIAs;
- analyses the results of the DPIAs and when necessary, recommends the consultation of the supervisory authority;
- cooperates with the CNPD as the designated contact point for Streff;
- keeps this Policy up to date.

Project owner/data processing owner

The processing activity owner or project owner is responsible for:

- informing the DPO in due time of every new project involving Personal data or of any significant changes to existing data Processing activities;
- supporting the DPO in analysing Processing activities to determine requirements and to ensure their implementation;

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



- carrying out DPIA eligibility study with the help of the DPO;
- when necessary, carry out DPIA;
- implementing of the risk treatment plan.

Streff personnel

Streff personnel shall take all necessary measures to respect this Policy.

5. General principles of data protection by design and by default

Data Protection by Design and by Default means to integrate data protection into the Processing activities and business practices, from the design stage right through the lifecycle to control the risks to the rights and freedoms of natural persons that may arise from the Processing of Personal data by Streff. It is built on the following general principles:

1. **Ensure the implicit protection of privacy:** in particular by disabling unnecessary functions and modules, as well as insecure options for a product/technology, by activating by default the mechanisms to protect privacy of data subjects (examples: blocking of advertising cookies in a browser or mobile application, activation of HTTPS by default when collecting personal data), by performing all the necessary tests for the validation of the security and conformity of the product or service before its release into production.
2. **Secure data from end-to-end:** guarantee level of security appropriate to the risk throughout the retention period of personal data, from collection to deletion, through appropriate technical and organisational measures such as the encryption of communications or even stored data, pseudonymization, data access control, authorization management, traceability (logs), deletion and anonymization measures of data, etc.
3. **Ensure transparency:** ensure that actions relating to the Processing of Personal data are documented (RoPA updating, privacy questionnaire, DPIA compliance deliverables, compliance deliverables in simplified monitoring, proof of consent from data subjects, compliance verification, test and reports, etc.), to be able to demonstrate compliance with data protection rules on request. It is necessary to make the elements of privacy 'visible' to take advantage of them and to create a climate of lasting trust with the data subject.
4. **Have a 'person-centric' approach (respect the privacy of data subjects):** the interests of the data subjects must be systematically considered and supported by strict and appropriate measures, so that no breach is made of the protection of their privacy. The important measures here are clear and transparent information to the data subject on the Processing operations carried out on his data (privacy notices, terms and conditions, clear consent forms, etc.); the establishment of an appropriate legal basis for the Processing (contract, legal obligation, legitimate interest, consent, etc.), the implementation and correct management of

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



the consent of the data subject when necessary and ensuring the exercise of the rights of the data subject.

6. Methodology

Before setting up a new Processing of personal data, it is necessary to analyse the risks for the data subjects and for Streff. To this end, a methodology that will enable Streff to implement the principle of Privacy by Design in the context of the development of new data Processing or the modification of existing Processing has been defined. It is structured as follows:

1. **Conduct an eligibility study.** This analysis ensures a systematic detection and scoring of projects, to detect Personal data Processing that may generate a high risk to the rights and freedoms of data subjects and for which a regulatory obligation to carry out a full DPIA applies.
2. **Conduct a full DPIA** if required;
3. **Conduct a simplified compliance** where a DPIA is not mandatory;
4. **Define, document, and follow-up an action plan** adapted to the level of risk of the Processing activity.

A. Detection of risky data processing: eligibility study

Description

The GDPR provides for the obligation to conduct a Data Protection Impact Assessment when Processing of Personal data is likely to result in a high risk to the rights and freedoms of data subjects. For existing Processing activities, this obligation applies when there has been a change of the risks, for example, if a new technology is used or the organisational or societal context for the Processing activity has changed and new vulnerabilities have arisen.

Note: a DPIA is not required in the following cases:

- the Processing is not likely to result in a high risk,
- when the nature, scope, context, and purposes of the Processing are very similar to a Processing for which a DPIA have been carried out,
- the Processing has been authorised prior to May 2018 by a supervisory authority and has not changed since its implementation,
- the Processing is based on a legal obligation or when it is necessary for the performance of a task carried out in the public interest and has a legal basis in Union or Member State Law and a DPIA has already been carried out as part of the establishment of that legal basis,
- the Processing is in the list established by the supervisory authority of Processing activities for which a DPIA is not required.

Tasks

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



The preliminary step of Streff's data protection by Design and by Default process is precisely to detect projects that fall within this obligation. This is the 'eligibility study'.

To be effective, the eligibility study must take place upstream, from the design phase of the new data Processing. This analysis will enable the project manager to describe the processing activities with all its component (categories of personal data, categories of data subjects, purpose of the Processing, involvement of processor, etc.). This will help the DPO to determine the risks of the processing activities and the need for a DPIA.

If the new Processing is eligible for DPIA, a DPIA have to be conducted and will be subject to rigorous monitoring by the DPO.

IMPORTANT: Any new Personal data Processing project is required to carry out a DPIA eligibility study at the early stages ('Design' and 'Plan' phases of the project lifecycle) under the responsibility of the project owner. The development of the project must be conditioned by the result of this study.



The project owner is responsible for carrying out the eligibility study. To do so, he will have to fill out the eligibility questionnaire (annex 1) and keep it as a project deliverable.

If the result of the eligibility study is positive, a complete DPIA must be carried out and the project will be the subject to rigorous support and monitoring given the associated regulatory issues and risks.

If the result of the eligibility study is negative, the project is not exempt from the compliance obligation. Indeed, since the project involved a new Processing of Personal data (or modification of an existing Processing), it is still mandatory to integrate into its development cycle the measures for the protection of personal data, under the responsibility of the project owner.

B. Conduct a full DPIA

For all projects where the eligibility study indicates a requirement to conduct a DPIA, the DPIA must be carried out and documented by the relevant project owner, assisted by the DPO.

The DPIA identifies and analyses in detail the risks to the rights and freedoms of data subjects in the context of the envisaged data Processing operation, with a view to defining and implementing an effective action plan to reduce those risks.

The validation of the action plan and the residual risks after application of the proposed measures, all properly documented, is a prerequisite for the data Processing implementation or the "go-live" phase of the project.

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



The project owner will carry out the analysis using the appropriate tools provided in this procedure and will document his project, accordingly, assisted in this task by the head of Information Security for the "risks and security measures" part. The DPO may at this stage be consulted on any questions relating to the methodology and implementation of the DPIA.

The results of the analyses will then be submitted for review by the Accountable Manager. At this stage, the DPO will give his opinion on the adequacy of the measures to be implemented, as well as on the residual risk levels after implementation of the measures. The DPO will issue additional recommendations if the residual risks are deemed too high. If the recommended measures could not reduce the risk to an acceptable level, then it belongs to the Controller through the Managing Director to ask the **DPO to consult the CNPD (art. 36 GDPR)**.

Finally, when the final risk treatment plan is validated and implemented, the project owner ensures that the measures adopted is properly implemented (level 1 internal control). In this step, he may request the assistance of the Head of Information Security for any security checks that may be necessary.

DPIA content

A complete DPIA must include:

- A study of the context of the project: description of the Processing operations as well as the intended purposes, the categories of data concerned, their source, the categories and number of persons concerned, the categories of recipients;
- An analysis of the principles and fundamental rights set by law, which must be respected and cannot be subject to any modulation: a description of the legal basis underlying the Processing envisaged, the planned retention period, a description of the necessity and proportionality of the data in relation to the purpose of the Processing; the measures provided for the collection of consent if necessary, the means implemented to guarantee the exercise of the rights of data subjects, the measures to regulate any subcontracting or transfer of data outside the EU;
- A qualification of the existing security measures to protect the personal data;
- A study of the risks to the privacy of the data subjects in the event of disclosure, alteration or destruction of personal data;
- The choice of measures envisaged addressing the identified risks: the various organizational and technical measures will be chosen with the Head of Information Security;
- A risk treatment plan validated by the Accountable Manager;
- Compliance deliverable: the validation of the impact assessment or the revision of some of the previous steps considering the recommendations of the DPO must be documented in a deliverable

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



before the project is launched. This deliverable will be proof of project's compliance and respect of the DPIA methodology.

Consultation of supervisory authority in case of high residual risk

Where a DPIA reveals high residual risks, the data controller is required to consult the supervisory authority. In this case, the DPIA must be fully provided to the CNPD, which will then issue an opinion on the planned Processing operation and the risk management. Processing may only be carried out after implementing the recommendations of the CNPD.

An example of an unacceptable high residual risk includes cases where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).

7. Compliance adapted to the risk level

Where the data Processing project is not eligible for the DPIA, it will still be subject to compliance with the provisions of the GDPR and Streff's general data protection policy. The project owner will ensure that the general data protection principles are considered at the design stage and by default during the development of the project. The project owner will be assisted by the DPO in analysing the data Processing and identifying measures to comply with the data protection principles.

The project owner will then ensure to:

- fill privacy questionnaire to provide the DPO with all necessary information about the project and the Processing activities concerned;
- be diligent in the selection of processors and any undertakers involved in the Processing activities, by sending the processor due diligence questionnaire;
- consult the DPO with all findings;
- implement the measures identified;
- document their implementation in the project deliverable;
- verify the effective implementation of the measures before launching the new Processing operation;
- validate with the DPO the correct implementation of the measures.

Data protection by design and DPIA policy	Max Neumann	Approbation	1.0	05.02.2023	
---	-------------	-------------	-----	------------	--



8. Policy update

The rules set out in this Policy are based on the European and Luxembourg regulations and laws in force at the date of its publication. The Policy will be reviewed every year by the DPO, as part of the annual report on compliance.

9. Reference

- Regulation (EU) number 679/2016 of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data (GDPR).
- Article 29 Data protection Working party – Guidelines on DPIA and determining whether Processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679 (document reference number wp248rev.01).
- European data protection board – Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
- CNPD's information: <https://cnpd.public.lu/en/professionnels/obligations/AIPD.html>
- CNIL information: <https://www.cnil.fr/en/privacy-impact-assessment-pia>

10. Revision history

Version	Description	Date	Author
0.1	Drafting of the policy	19.11.23	Edith Sijou
0.2	Validation review	05.02.23	Max Neumann