**GUIDELINES TO START AND MANAGE A DATA PROCESSING PROJECT**

Privacy is about respecting individuals: while digitalization facilitates the transfer of data, it is the responsibility of each stakeholders to protect personal data of natural persons and for that purpose monitor and secure the flow of these data.

In this context, Nexans is accountable for the personal data of its all employee / customer / business partner.

Taking into account personal data is not a “best practice” but a prerequisite to be addressed **at the very beginning of a project and thereafter**.

These guidelines are here to ensure that for each relevant project our policies can be **measured**, **monitored** and **enforced.**

1. **WILL** the application process personal data?

At the very beginning of a project you must ask yourself and your service provider whether personal data will be processed by the application you are contemplating to deploy.

**What is a personal data?** A personal data is any data related to a natural person that can be used to identify a natural person such as (i) an individual's name, (ii) e-mail (iii) ID Card (iv) a photograph of a natural person, (v) banking details (vi) an IP address…

Please bear in mind that the use of various non-personal data that could, **together**, enable the identification of a natural person is considered as a processing of personal data.

What does it mean for Nexans? When you use data for statistical purpose you need to make sure these data are anomymized and that they cannot allow to identify a natural person.

**What is processing?** Any (set of) operation(s) which is performed on (sets of) personal data (e.g. the collection, use, conservation and/or deletion of personal data).

**It can be done in any form: electronical database, excel sheet, word file, paper, handnotes,etc.**

**KEY RULE: make a clear list of personal data associated with your project**

1. **WHY** your project requires processing of personal data?

Personal Data shall be only used for purpose(s) that are specific, lawful and clearly stated.

Purpose does not have to be **unique**: you can have several purposes clearly identified for processing personal data.

Once purpose(s) are defined, processing personal data for another purpose is unlawful !

*Example: video-surveillance system is for security and access control of Nexans’ sites. It shall not be used for any other purpose, such as monitoring the work of employees or their attendance.*

**KEY RULE: Purpose being the cornerstone of any processing, make sure you allocate the right purpose to the right processing.**

1. **WHAT** personal data are strictly needed for the purpose identified?

The key word is **“Privacy by Design”:** *any application that processes personal data shall be designed, from the outset, to ensure that personal data processed are those strictly necessary for the provision of the service offered by the application.*

*Example: A travel application requires it users to fill-in mandatory fields to open one’s profile. The application requires the contact details of a family member (phone number and address) in case of urgency.*

*This personal data is NOT strictly needed to book a travel – “nice to have” personal data are to be excluded by default*

Some personal data are more **sensitive** than others!

The list of so called “sensitive personal data” depends on your national law. For instance in Europe:

|  |  |  |
| --- | --- | --- |
| racial origin | political opinions | religious or other beliefs |
| physical or mental health | sexual life | criminal convictions |
| trade union membership | biometric data |  |

Such sensitive personal data generally **cannot be processed**, except in very limited circumstances (i) to fulfil a legal obligation, (ii) to **protect the vital interests of the person** or (iii) if the explicit unambiguous consent of each individual whose data is collected is obtained.

**KEY RULE: Do not process personal data that are not strictly necessary for the purpose and always make sure you can justify why a specific personal data is necessary**

1. **WHAT** is my legal basis for such processing?

Which legal basis is most appropriate for your processing will depend on the purpose you have previously identified.

In general to lawfully process Personal Data one must demonstrate one of the following legal basis:

* Legitimate interest of Nexans
* Contractual basis between Nexans and the natural person (e.g. the employment contract)
* Legal obligation imposed on Nexans by law or authorities
* Consent of the natural person (e.g. opt-out mechanism in newsletters)

***Most of the time, legal obligations or legitimate interest will be a satisfactory ground to process personal data.***

When consent is required, it can be provided in various forms depending on the architecture of the application: signing a consent statement, sending an email click on an opt-in button online…

**KEY RULE: Always ensure you document the legal basis underlying the processing of personal data**

1. **WHAT** is the retention period applicable?

Just like the legal basis, the retention period of personal data heavily depends on the purpose.

**KEY RULES: Personal data should only be retained for a limited retention period, either defined by law or limited in time to what is strictly necessary for the identified purpose.**

1. **WHO** will have access to the personal data processed by the application?

Only a minimum number of employees and/or service providers shall have the right to access, display and/or remove personal data.

In any event, you need to make sure a secure documented process is in place so that only authorized people can have access to personal data.

**KEY RULE: When launching a data processing identify the persons who will have access internally and externally (the service provider(s) or their subcontractors) to the personal data and document the procedure.**

1. **HOW** secure is the application ***today*?**

IT department will assist you to determine what **appropriate technical and organizational measures** shall be taken by Nexans and the service provider against unauthorised or unlawful processing of personal data and against accidental loss or damage to personal data.

Always document with your service provider the following:

* how data are secured (Passwords, encryption of data, physical security…)?
* what is the data breach incident management?
* Is there a back-up & business continuity plan?
* Is your service provider ISO certified (eg. ISO 27001…)?

For that purpose, obtain completion and signature of the Data Processing Agreement[[1]](#footnote-1).

At the outset of your project you shall:

* Fill out the **IS letter of intent**[[2]](#footnote-2): this document describes the purpose of project, its benefit and value to the Group and generally its context (including whether personal data are processed).
* Fill out the “**sensitivity assessment**”[[3]](#footnote-3) tool for the application: it will help you to measure the risks associated with the application, including the personal data risk.
* Send to your service(s) provider(s) the **Information security guidelines[[4]](#footnote-4)** issued by IS. They set the basic security principles that Nexans expects from its service providers.

1. **WHERE** personal data are transferred?

Always document where your service provider is incorporated and where personal data are to be stored. Nexans policy is to have personal data of citizen of the EU to be stored in data centers within Europe.

Be careful if the service provider wants to transfer personal data outside of your country (or if you are in Europe, outside Europe).

Under the EU regulation, transfers **outside the EU are forbidden** unless certain legal basis is met such as:

* the country of destination is declared as offering an adequate level of protection by the EU authorities[[5]](#footnote-5)
* the standard contractual clauses applicable to the service provider approved by the European Commission[[6]](#footnote-6);
* Binding Corporate Rules (set of rules approved by authorities) of your service provider.

**KEY RULE: if a transfer of personal data outside your country, make sure you get your local Data Protection Correspondent approval. For transfer of personal data outside the EU, make sure you involve at the outset both local Data Protection Correspondent and Group DPOs**

1. **HOW** do you ensure persons are well informed of the processing?

Nexans must ensure that a clear and concise information notice is provided to its employees and business partners **before or at the time** their personal data is collected.

Such information includes for instance: (i) the purpose of the processing, (ii) the categories of personal data processed, (iii) identity of any recipient of the personal data (internal and/or external).

1. **HOW** do you deal with requests from persons on their personal information?

Natural persons (employees, business partners…) have the rights to make the following requests:

|  |  |  |
| --- | --- | --- |
| **Right to be informed of the processing** | **Right of access to the personal data** | **Right to rectification of the personal data** |
| **Right to erasure of the personal data** | **Right to restrict processing of personal data** | **Right to object to the processing** |

All requests with respect to such rights are to be answered within a **1-month period**.

This is a very short deadline: ***you need to make sure that the application offered by the service provider contains mechanisms to technically answer such requests.***

1. **WHERE** do we keep track of the details of such processing activity?

Nexans need to maintain documentation as evidence to demonstrate our accountability.

Accountability means we must document the various processing of personal data (what kind of data, where do they go, what is the purpose…) with the help of the local Data Protection Correspondent. One of the Data Protection Correspondent’s role will be to maintain a register of personal data with the help of the project manager.

1. **HOW** do I keep track of the personal data matters during the life of the project?
   1. **Ensure adequate security throughout the life of the contract**

Documenting the security procedures and measures of your service provider is a good start, but project management calls for **regular testing** of security measures via audit rights.

Security procedures must be challenged in practice via Vulnerability Testing, Penetration Testing that are to be carried out either by Nexans or by a service provider on a regular basis.

* 1. **Ensure swift remediation in case of security breach**

In Europe, in case of personal data breach (where data are leaked or damages), Nexans shall inform its national data protection supervisory authority no later than 72 hours after having become aware of the breach.

When required by the regulation, Nexans will also inform directly individuals affected of the personal data breach when it is likely to result in a high risk to the rights and freedom of individuals without delay.

Always involve immediately your local Data Protection Correspondent and Group DPO in the event of a data breach.

* 1. **Evolution of the processing and/or the purpose**

Applications are often subject to new modules or updates which may **imply new processing and/or new purposes**: always ask your service provider about impact of these new features on the processing of personal data.

If it does, you will have to go through part or all of the above-mentioned questions.

|  |
| --- |
| **At the beginning of a personal data processing the Group DPO or local Data Protection Correspondent and Corporate IS shall always be involved upfront**  **Any question? Please contact the DPO or local Data Protection Correspondent or the Legal Department** |

1. Available at <http://intranet.nexansdomain.global/intranet/document/Download.nx?documentId=121732> [↑](#footnote-ref-1)
2. Available at <http://intranet.nexansdomain.global/intranet/navigation/NavigateEditorialContent.nx?editorialId=115779&navigationId=25079> [↑](#footnote-ref-2)
3. Available at <http://intranet.nexansdomain.global/intranet/document/Download.nx?documentId=121658> [↑](#footnote-ref-3)
4. Available at <http://intranet.nexansdomain.global/intranet/document/Download.nx?documentId=121614> [↑](#footnote-ref-4)
5. List of countries offering an adequate level of protection as of February 16, 2018: U.S., Switzerland, Andorra, the Faroe Islands, Guernsey, Jersey, the Isle of Man, Argentina, Canada, Israel, New Zealand and Uruguay [↑](#footnote-ref-5)
6. Accessible on-line at : <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en> [↑](#footnote-ref-6)