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

启动和管理数据处理项目的指导原则

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.

隐私是尊重个人的：虽然数字化有助于数据传输，但每个利益相关者都有责任保护自然人的个人数据，并为此目的监控和保护这些数据的流动。

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

在这种情况下，Nexans负责其所有员工/客户/业务合作伙伴的个人数据。

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.

考虑到个人数据并不是一个“最佳实践”，而是在一个项目的开始和之后要解决的先决条件。

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

这些指导方针是为了确保每个相关项目的政策都能被衡量、监控和执行。

1. WILL the application process personal data?

申请会处理个人资料吗？

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.

在项目的一开始，您必须问自己和您的服务提供商，您打算部署的应用程序是否会处理个人数据。

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…

什么是个人数据？个人数据是与自然人有关的任何数据，其可用于识别自然人，如（i）个人姓名，（ii）电子邮件（iii）身份证（iv）自然人的照片，（v）银行详细信息（vi）和IP地址…

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.

请记住，使用各种能够共同识别自然人的非个人数据被视为个人数据的处理。

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.

这对Nexans意味着什么？当您将数据用于统计目的时，您需要确保这些数据是匿名的，并且它们不允许识别自然人。

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).

什么是处理？对个人数据（如个人数据的收集、使用、保存和/或删除）执行的任何（一组）操作。

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

它可以以任何形式完成：电子数据库、Excel表格、Word文件、纸张、笔记等。

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

关键规则：明确列出与项目相关的个人数据

1. WHY your project requires processing of personal data?

为什么你的项目需要处理个人数据？

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

个人数据只能用于特定、合法和明确说明的目的。

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

目的不一定是唯一的：您可以有几个明确的目的来处理个人数据。

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

一旦定义了目的，为其他目的处理个人数据是非法的！

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.

示例：视频监控系统用于Nexans网站的安全和访问控制。不得用于任何其他用途，如监视员工的工作或出勤。

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

关键规则：目的是任何处理的基石，请确保将正确的目的分配给正确的处理。

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

为了确定目标，严格需要哪些个人数据？

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.

关键词是“设计隐私”：任何处理个人数据的应用程序应从一开始就应进行设计，以确保处理的个人数据是提供应用程序所提供服务的严格必要数据。

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.

示例：旅行应用程序要求用户填写必填字段以打开个人资料。如果情况紧急，申请需要家庭成员的联系方式（电话号码和地址）。

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

预订旅行时不需要这些个人数据——默认情况下，“很好拥有”个人数据将被排除在外。

Some personal data are more sensitive than others!

有些个人数据比其他数据更敏感！

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

|  |  |  |
| --- | --- | --- |
| racial origin  种族起源 | political opinions  政治意见 | religious or other beliefs  宗教或其他信仰 |
| physical or mental health  身心健康 | sexual life  性生活 | criminal convictions  刑事定罪 |
| trade union membership  工会会员 | biometric data  生物特征数据 |  |

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.

通常无法处理此类敏感的个人数据，除非在非常有限的情况下：（i）履行法律义务；（ii）保护个人的切身利益；或（iii）获得收集数据的每个人的明确明确同意。

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

关键规则：不要处理不完全必要的个人数据，并始终确保您能够证明为什么需要特定的个人数据。

1. WHAT is my legal basis for such processing?

我的法律依据是什么？

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

哪种法律依据最适合您的处理将取决于您先前确定的目的。

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

一般来说，要合法处理个人数据，必须证明以下法律依据之一：

* Legitimate interest of Nexans

NEXANS的合法利益

* Contractual basis between Nexans and the natural person (e.g. the employment contract)

Nexans与自然人之间的合同基础（如雇佣合同）

* Legal obligation imposed on Nexans by law or authorities

法律或当局对Nexans施加的法律义务

* Consent of the natural person (e.g. opt-out mechanism in newsletters)

自然人的同意（如通讯中的选择退出机制）

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

大多数情况下，法律义务或合法利益将是处理个人数据的一个令人满意的基础。

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…

当需要同意时，可以根据应用程序的结构以各种形式提供：签署同意声明，发送电子邮件，单击在线选择加入按钮…

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

关键规则：始终确保您记录处理个人数据所依据的法律依据。

1. WHAT is the retention period applicable?

什么是适用的保留期？

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

与法律依据一样，个人数据的保存期限在很大程度上取决于目的。

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.

关键规则：个人数据只能在有限的保留期内保留，无论是法律规定的还是为确定的目的而严格需要的时间。

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

谁可以访问应用程序处理的个人数据？

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

只有少数员工和/或服务提供商有权访问、显示和/或删除个人数据。

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.

在任何情况下，您都需要确保有一个安全的文档化流程，以便只有授权人员才能访问个人数据。

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.

关键规则：在启动数据处理时，确定内部和外部（服务提供商或其分包商）有权访问个人数据的人员，并记录程序。

1. HOW secure is the application today?

现在的应用程序有多安全？

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.

IT部门将协助您确定Nexans和服务提供商应采取哪些适当的技术和组织措施，以防止未经授权或非法处理个人数据以及意外丢失或损坏个人数据。

Always document with your service provider the following:

始终向您的服务提供商提供以下文档：

* how data are secured (Passwords, encryption of data, physical security…)?

如何保证数据安全（密码、数据加密、物理安全……）？

* what is the data breach incident management?

什么是数据泄露事件管理？

* Is there a back-up & business continuity plan?

是否有备份和业务连续性计划？

* Is your service provider ISO certified (eg. ISO 27001…)?

您的服务提供商是否通过了ISO认证（如ISO 27001…）？

For that purpose, obtain completion and signature of the Data Processing Agreement.

为此，获得数据处理协议的完成和签署。

At the outset of your project you shall:

在项目开始时，您应：

* Fill out the IS letter of intent: this document describes the purpose of project, its benefit and value to the Group and generally its context (including whether personal data are processed).

填写意向书：这份文件描述了项目的目的、它的益处和价值，以及它的上下文（包括个人数据是否被处理）。

* Fill out the “sensitivity assessment” tool for the application: it will help you to measure the risks associated with the application, including the personal data risk.

填写应用程序的“敏感性评估”工具：它将帮助您衡量与应用程序相关的风险，包括个人数据风险。

* Send to your service(s) provider(s) the Information security guidelines issued by IS. They set the basic security principles that Nexans expects from its service providers.

将IS发布的信息安全指南发送给您的服务提供商。他们设定了Nexans期望其服务提供商提供的基本安全原则。

1. WHERE personal data are transferred?

个人数据被转移到哪里？

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.

始终记录服务提供商的合并位置和个人数据的存储位置。Nexans政策是将欧盟公民的个人数据存储在欧洲的数据中心。

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

如果服务提供商希望将个人数据传输到您的国家以外（或如果您在欧洲、欧洲以外），请小心。

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

根据欧盟法规，除非符合某些法律依据，如：

* the country of destination is declared as offering an adequate level of protection by the EU authorities

目的国被欧盟当局宣布为提供了充分的保护。

* the standard contractual clauses applicable to the service provider approved by the European Commission;

适用于欧盟委员会批准的服务提供商的标准合同条款；

* Binding Corporate Rules (set of rules approved by authorities) of your service provider.

约束您的服务提供商的公司规则（权威机构批准的规则集）。

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

关键规则：如果将个人数据转移到国外，请确保获得当地数据保护代理的批准。对于欧盟以外的个人数据传输，请确保您从一开始就参与本地数据保护通讯员和集团DPO。

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

您如何确保员工了解处理过程？

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.

NEXANS必须确保在其个人数据被收集之前或在其雇员和业务伙伴处提供清晰和简明的信息通知。

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).

例如，这些信息包括：（i）处理的目的；（ii）处理的个人数据类别；（iii）个人数据的任何接收者的身份（内部和/或外部）。

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

你如何处理个人信息的请求？

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

|  |  |  |
| --- | --- | --- |
| Right to be informed of the processing  处理通知权 | Right of access to the personal data  访问个人数据的权利 | Right to rectification of the personal data  个人资料更正权 |
| Right to erasure of the personal data  删除个人资料的权利 | Right to restrict processing of personal data  限制处理个人数据的权利 | Right to object to the processing  反对加工权 |

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

有关此类权利的所有请求应在1个月内予以答复。

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.

这是一个非常短的截止日期：您需要确保服务提供者提供的应用程序包含从技术上回答此类请求的机制。

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

我们在哪里跟踪这些处理活动的细节？

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

Nexans需要保留文档作为证明我们责任的证据。

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.

问责意味着我们必须在当地数据保护通讯员的帮助下记录个人数据的各种处理（什么类型的数据，它们去哪里，目的是什么…）。数据保护通讯员的职责之一是在项目经理的帮助下维护个人数据的登记册。

1. HOW do I keep track of the personal data matters during the life of the project?

在项目的生命周期中，我如何跟踪个人数据的重要性？

* 1. Ensure adequate security throughout the life of the contract

在合同有效期内确保足够的安全

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.

记录服务提供商的安全程序和措施是一个好的开始，但是项目管理需要通过审计权限定期测试安全措施。

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.

安全程序必须在实践中通过漏洞测试、渗透测试来挑战，这些测试将由NEXANS或由服务提供商定期执行。

* 1. Ensure swift remediation in case of security breach

确保安全事故时的快速补救

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.

在欧洲，如果发生个人数据泄露（数据泄露或损坏），Nexans应在意识到泄露后72小时内通知其国家数据保护监督机构。

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.

当法规要求时，Nexans还将在可能对个人权利和自由造成高风险的情况下，立即告知受个人数据泄露影响的个人。

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

如果发生数据泄露，请立即联系本地数据保护代理和DPO组。

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

处理和/或目的的演变

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.

应用程序通常会受到新的模块或更新的影响，这可能意味着新的处理和/或新的目的：始终询问您的服务提供商这些新功能对个人数据处理的影响。

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  在个人数据处理开始时，集团DPO或本地数据保护通讯员和企业IS应始终预先参与。  Any question? Please contact the DPO or local Data Protection Correspondent or the Legal Department  有什么问题吗？请联系DPO或当地数据保护通讯员或法律部门。 |