启动和管理数据处理项目的指导原则

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。

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。

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。

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. 申请会处理个人资料吗？

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。

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…

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。

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。

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。

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。

关键规则：明确列出与项目相关的个人数据

1. 为什么你的项目需要处理个人数据？

个人数据只能用于特定、合法和明确说明的目的。

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。

一旦定义了目的，为其他目的处理个人数据是非法的！

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。

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. 为了确定目标，严格需要哪些个人数据？

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。

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）。

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。

有些个人数据比其他数据更敏感！

所谓“敏感个人数据”的清单取决于你的国家法律。例如，在欧洲：

|  |  |  |
| --- | --- | --- |
| 种族起源 | 政治意见 | 宗教或其他信仰 |
| 身心健康 | 性生活 | 刑事定罪 |
| 工会会员 | 生物特征数据 |  |

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。

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. 我的法律依据是什么？

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。

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：

* NEXANS的合法利益
* Nexans与自然人之间的合同基础（如雇佣合同）
* 法律或当局对Nexans施加的法律义务
* 自然人的同意（如通讯中的选择退出机制）

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。

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…

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. 什么是适用的保留期？

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。

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. 谁可以访问应用程序处理的个人数据？

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。

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。

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. 现在的应用程序有多安全？

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。

始终向您的服务提供商提供以下文档：

* 如何保证数据安全（密码、数据加密、物理安全……）？
* 什么是数据泄露事件管理？
* 是否有备份和业务连续性计划？
* 您的服务提供商是否通过了ISO认证（如ISO 27001…）？

为此，获得数据处理协议的完成和签署。

在项目开始时，您应：

* 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）。
* 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。
* 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. 个人数据被转移到哪里？

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。

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。

根据欧盟法规，除非符合某些法律依据，如：

* 目的国被欧盟当局宣布为提供了充分的保护。
* 适用于欧盟委员会批准的服务提供商的标准合同条款；
* 约束您的服务提供商的公司规则（权威机构批准的规则集）。

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. 您如何确保员工了解处理过程？

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。

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. 你如何处理个人信息的请求？

自然人（雇员、商业伙伴等）有权提出以下要求：

|  |  |  |
| --- | --- | --- |
| 处理通知权 | 访问个人数据的权利 | 个人资料更正权 |
| 删除个人资料的权利 | 限制处理个人数据的权利 | 反对加工权 |

有关此类权利的所有请求应在1个月内予以答复。

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. 我们在哪里跟踪这些处理活动的细节？

Nexans需要保留文档作为证明我们责任的证据。

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注册。

1. 在项目的生命周期中，我如何跟踪个人数据的重要性？
   1. 在合同有效期内确保足够的安全

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。

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. 确保安全事故时的快速补救

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。

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。

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. 处理和/或目的的演变

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。

如果是这样的话，你将不得不回答上述部分或全部问题。

|  |
| --- |
| 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。  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。 |