Getinge 全球政策

数据隐私全球政策

文档所有者	安娜·龙伯格
版本	v3
董事会通过	2023 年 4 月 26 日

1. 概括

本全球数据隐私政策（“**全球政策**”）的目标是制定主要的数据隐私要求，并为 Getinge 管理层、员工和顾问提供涉及个人数据处理的日常工作指南。

Getinge 致力于根据适用的数据保护法律和法规处理个人数据。在我们的日常运营中，隐私始终是重中之重。

本全球政策适用于代表 Getinge 行事的所有员工、董事和业务合作伙伴。

2. 定义

在本全球政策中，下列术语具有以下含义：

数据控制者	单独或与其他实体共同决定个人数据处理的目的和方式的法人实体。
数据处理器	代表数据控制者处理个人数据的法律实体。
数据保护影响评估	评估项目、过程或解决方案对数据保护的影响的系统过程。
数据保护法	任何和所有适用的数据保护法律和法规，包括但不限于 GDPR。
数据主体	与个人数据相关的个人。
通用数据保护条例	欧洲议会和理事会 2016 年 4 月 27 日关于在处理个人数据和此类数据的自由流动方面保护自然人并废除指令 95/46/ 的 (EU) 2016/679 号条例欧共体。
个人资料	与数据主体相关的任何信息。数据主体是指可以使用姓名、身份证号码、位置数据、在线标识符或特定于自然人的身体、生理、遗传、精神、经济、文化或社会身份的因素来直接或间

	接识别的人人。个人数据还包括员工的联系方式，例如工作电子邮件地址和联系人。
个人数据泄露	导致意外或非法破坏、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的个人数据的安全漏洞。
个人资料的处理	对个人数据或个人数据集执行的任何操作或一组操作，无论是否通过自动方式，例如收集、记录、组织、结构化、存储、改编或更改、检索、咨询、通过传输使用披露、传播或以其他方式提供、对齐或组合、限制、删除或销毁。处理还包括查看个人数据。
特殊类别的个人数据-	所有直接或间接表明在世自然人的种族或族裔出身、政治观点、哲学或宗教信仰、性取向、工会会员资格和活动、遗传或生物特征数据以及有关健康或性生活的数据的个人数据。
监管机构	一个独立的公共机构，负责监督数据保护法的遵守情况。

3. 范围和目标

本全球政策适用于所有 Getinge 公司、其子公司和联合运营机构（统称为“ **Getinge** ”），适用于我们的所有员工，以及在 Getinge 场所工作或在 Getinge 指导下工作的顾问和代理人员（统称为“ Getinge ”）在本全球政策中称为“**员工**”）。一般规则是本全球政策适用于 Getinge 内部的所有个人数据处理。例外情况仅适用于本全球政策中规定的情况。

本全球政策的目标是提供：

a) 有关个人数据和适用的数据保护法的一般知识
b) 对 Getinge 至关重要的法律要求指南
c) 处理个人数据时对 Getinge 的要求
d) Getinge 处理个人数据时必须遵守的说明

通过本全球政策，我们承诺根据数据保护法保护个人数据。

4. 应用领域

具体适用性

本全球政策适用于：

a) 在业务流程中处理个人数据
b) 用于处理个人数据的 IT 功能、解决方案或服务
c) Outlook、PowerPoint、Word 和 Excel 等工具
d) Getinge 提供的产品或服务包括代表第三方处理个人数据的情况，例如向医院提供的 IT 解决方案

e) Getinge 是本全球政策中所述的数据控制者、数据处理者和/或联合控制者的所有其他情况

特定操作可能需要除本全球政策中规定的要求之外的其他要求，例如有关 IT 安全的要求。除本全球政策外，可能还有适用于特定 Getinge 团队的处理个人数据的其他说明和指南。

适用法律、当地要求和偏差

本全球政策基于欧洲数据保护法律法规，但也适用于 Getinge 在欧盟/欧洲经济区以外的所有个人数据处理。例如，欧洲数据保护法律和法规适用于此类处理的原因可能是：

a) 处理涉及位于欧盟/欧洲经济区内的 Getinge 总部采用的程序、系统、例程或决定
b) 处理涉及向欧盟/欧洲经济区内的数据主体提供的商品和服务，或监控他们的行为
c) 欧盟/欧洲经济区以外的实体被视为在欧盟/欧洲经济区成立，例如，由于在欧盟/欧洲经济区有雇员

当当地数据保护法律法规规定的要求与本全球政策规定的要求不同或更严格时，Getinge 应遵守此类法律法规。如果法律和/或法规与本全球政策相冲突，则应以更严格的要求为准。如需进一步指导，请联系数据隐私团队。

匿名和假名数据

本全球政策不适用于*完全*匿名的信息，即无法与可识别个人关联的信息。由于当今市场上可用的技术解决方案，有许多不同的方法可以通过使用正确的技术工具来识别个人。请注意，匿名化在实践中可能很复杂。

本全球政策适用于经过所谓假名化处理的信息，即可以通过使用另一组信息（例如“密钥”）与个人相关联的信息。假名数据仍被视为个人数据。

笔记！

当 Getinge 公司持有的数据与另一家 Getinge 公司或第三方持有的其他数据可能与个人相关时，个人数据不被视为匿名。例如，静态和动态 IP 地址都被视为个人数据，因为如果 IP 号码与互联网运营商持有的信息相结合，则可能与个人相关。Getinge 无法访问第三方持有的信息并不重要，即它仍然被视为个人数据。

5. 合规责任

数据隐私团队

数据隐私治理指令中描述了 Getinge 的数据隐私组织和数据隐私团队。数据隐私团队应在数据隐私领域保持必要的专业知识。

数据隐私团队应被视为 Getinge 内部的讨论伙伴，数据隐私团队的意见应在数据隐私事务中得到应有的重视。

进一步了解：数据隐私治理指令

Getinge 公司的责任

遵守本全球政策中概述的法律、法规、Getinge 内部决策、流程和程序是 Getinge 每家公司的最终责任。另请参阅第 19 节有关角色和职责的内容。

报告风险

Getinge 应努力完全遵守所有数据保护法，并主动解决和纠正导致或可能导致违规的商业行为。我们鼓励并期望每位员工报告任何事件或不合规的嫌疑，并保证不会对善意行事的人进行报复或其他负面后果。员工应向数据隐私团队提出对数据隐私风险和/或疑似违规行为的担忧。也可以随时根据第 18 条提出疑虑。

6. Getinge 公司作为控制者处理个人数据时的一般要求或共同控制人

控制器

当 Getinge 公司处理个人数据时，它可能会自行决定处理个人数据的原因和方式。如果 Getinge 公司决定处理个人数据的方式（方式）和目的（原因），则它被称为数据控制者。

例子

如果 Getinge 出于每月支付工资的目的收集其员工的个人数据，Getinge 将确定处理的目的和方式，因此被视为个人数据处理的数据控制者。

共同控制人

在某些情况下，两个或多个数据控制者可以共同确定处理个人数据的目的（原因）和方式（方式）。例如，Getinge 公司可以与一个或多个内部和/或外部实体共享数据控制器的角色。这被称为联合控制权。

当存在共同控制者关系时，法律要求签订共同控制者协议以确定数据控制者各自的责任。Getinge 公司应确保使用内联网上可用的适用模板。

例子

如果 Getinge 公司与医院一起进行研究，Getinge 公司和医院合作确定在项目中处理个人数据的原因和方式，那么 Getinge 公司和医院可以被视为联合控制者，并且将这种情况需要签订共同控制人协议。

收集和处理个人数据的基本要求

个人数据只能用于特定、明确和合法的目的。为了使目的被视为合法，计划的处理必须，无论数据主体是否同意处理：

a) 具有合法的商业目的，不得违反任何数据保护法或其他法律；
b) 与实现目的相称且必要；
c) 不得以对数据主体产生不合理的不利影响的方式使用；和
d) 仅以数据主体合理期望的方式处理数据主体的个人数据。

对个人数据的所有处理都必须是实现处理目的所必需的，并且不得在处理个人数据的目的或范围方面误导或欺骗数据主体。不得以任何与已通知数据主体的目的不相符的方式处理个人数据。此外，Getinge 公司处理的个人数据应准确无误，并在必要时保持最新。

处理个人数据的法律依据

法律依据概述

Getinge 可能仅在以下至少一项适用时处理个人数据：

a) **同意。**数据主体已事先同意为特定目的进行处理。请参阅下文第 6 节中有关同意和撤回同意的内容。

b) **法律义务。**Getinge 必须处理个人数据以履行 Getinge 所承担的法律义务（例如向税务机关提交税收收入信息）。

c) **合同的履行。**处理个人数据对于 Getinge 履行其与数据主体签订的合同中的义务是必要的（例如保留银行账户详细信息以根据雇佣合同支付工资）。

d) **Getinge 的合法权益。**Getinge 可能出于其业务的一部分出于合法目的处理个人数据（例如保留有关其客户或业务合作伙伴的信息数据库，或为其员工收集紧急联系人的姓名和电话号码），除非此类利益被数据主体的利益或基本权利和自由。当应用此法律依据时，必须确定相关的特定利益，并应将此告知数据主体。

e) **其他。**处理个人数据还有其他罕见的理由，即保护数据主体的切身利益或为公共利益执行的任务。

同意和撤回同意

只有在无法使用其他法律依据时，Getinge 公司才能使用同意书。如果将同意作为法律依据，Getinge 公司必须能够证明数据主体已同意处理个人数据，并且此类同意有效。预先勾选的方框、沉默或不活动绝不构成同意。如果合适，应针对不同的处理目的获得单独的同意。

同意应为：

a) 在不受其他条件约束的情况下给予；
b) 知情（见本节下文关于向数据主体提供的信息）；
c) 自愿提供（数据主体不得被迫提供同意）；和
d) 具体且明确（数据主体必须了解同意的范围）。

必须以书面或电子方式给予同意。如果数据主体接受拟议的个人数据处理，则必须明确指出。不能通过沉默或不作为来表示同意。

数据主体可以随时撤回提供的同意。当撤回同意时，有关的 Getinge 公司应停止处理有关数据主体的个人数据，前提是处理是基于同意。这意味着必须删除或匿名化有关撤回同意的个人的所有个人数据，包括任何备份中的个人数据。

处理特殊类别个人数据的附加要求

特殊类别的个人数据（通常称为“敏感个人数据”）受到特殊保护，除特殊情况外不应由 Getinge 处理。

只有在本第 6 节中所述的处理具有法律依据的情况下，才能对特殊类别的个人数据进行处理。此外，只有在至少满足以下条件之一的情况下，才能处理此类数据：

a) 数据主体已明确同意为特定目的进行处理；
b) 在国家法律或集体协议授权的范围内，为了履行数据控制者或数据主体在劳动法领域的义务和行使权利，处理是必要的；
c) 处理对于建立、行使或捍卫合法索赔是必要的；或者
d) 为了预防或职业医学的目的，为了评估员工的工作能力、医学诊断、提供医疗保健或治疗，处理是必要的。

Getinge 通常应避免处理特殊类别的个人数据，并且只有在上述一种或多种情况适用时才可以这样做。本地例外情况也可能适用。

笔记！

明确同意包含上述第 6 节中关于同意和撤回同意的定期同意的要求。此外，应清楚地向个人提供同意或不同意拟议的个人数据处理的选项。

刑事犯罪和定罪范围内的个人数据

Getinge 不得处理与刑事犯罪或定罪有关的任何个人数据，包括怀疑，除非适用法律法规允许或要求。请注意，一般禁止处理此类个人数据。但是，国家法律法规可能会规定豁免。

不同的 Getinge 部门可能需要处理与刑事犯罪、定罪或相关怀疑有关的个人数据。例如，在调查和/或尽职调查的背景下，法律、合规和治理部门要求（在适用法律法规支持的情况下）对公司和/或相关职位的人员进行事实调查、背景调查。

笔记！

在处理任何有关犯罪记录、刑事犯罪、定罪或相关怀疑的个人数据之前，应始终咨询数据隐私团队。

给数据主体的信息

Getinge 应向数据主体发出书面通知，并提供以下信息：

a) 作为数据控制者的实体的名称和联系方式；
b) 处理的个人数据类型和处理的相关目的；
c) 处理的法律依据；
d) 个人数据将保留多长时间；
e) 个人数据的接收者或接收者类别；
f) 根据本节规定的数据主体权利的信息 8 以下;和
g) 如果适用：
    i. 负责数据保护官的联系方式；
    ii. 从哪里获得个人数据；
    iii. 数据主体不提供其个人数据的后果；
    iv. Getinge 打算根据第 9 以下;和
    v. 有关分析的信息。

数据隐私团队提供模板隐私声明，当 Getinge 公司需要通知数据主体有关个人数据处理时，应始终使用这些模板。模板包含有关必须提供给数据主体的信息的进一步说明。

每个 Getinge 公司都有责任确保并证明其隐私声明是充分和完整的，并且遵守数据保护法。此外，Getinge 公司应在必要时将隐私声明翻译成当地语言。

关于员工，有关个人数据处理的信息通常在员工与雇佣合同一起收到的员工隐私声明中提供。每家 Getinge 公司都应确保员工可以轻松访问其员工隐私声明并及时更新，并提供有关公司如何处理员工个人数据的充分信息。

个人数据处理目的变更

在更改个人数据处理目的之前，Getinge 公司应：

a) 评估个人数据处理的合法性并根据下文第 7 节记录评估结果；
b) 向数据主体提供描述处理目的修改的书面信息；和
c) 如果处理基于同意，请从数据主体处获得新的同意。

分析和自动决策

关于概要分析的一般信息

分析需要对个人数据进行任何形式的自动处理，涉及评估与数据主体相关的个人方面或预测或分析该数据主体的工作表现、经济状况、位置、健康、个人偏好、兴趣、可靠性或行为、驾驶员行为、客户行为、位置或移动。

分析通常用于通过使用来自各种来源的数据对个人进行预测并进行统计推论。处理的目的可能是分析数据主体的特征或行为模式，以便将他们归入某个群体或类别。这使数据控制者能够预测数据主体的兴趣、执行任务的能力或可能的行为。

例子

例如，分析可能包括通过 cookie 标识符或 IP 地址分析个人在网站上的行为，以便发送有关特定产品或服务的个性化广告。分析的另一个例子涉及分析以前的购买以预测未来的购买。因此，分析是一种常用于直接营销和社交媒体的方法，但也可用于其他处理活动，例如研究。

基于分析的决定

Getinge 公司基于分析做出的决定仅在以下情况下才被允许：

a) 绝对有必要在数据主体和数据控制者之间签订或履行协议（这种例外情况应狭义解释）；
b) 法律明确授权，包括根据机构或国家监督机构的规定、标准和建议进行的欺诈和逃税监控和预防目的，并确保 Getinge 提供的服务的安全性和可靠性；或者
c) 数据主体已明确表示同意。

要求

Getinge 公司在进行分析时应确保以下几点：

a) 仅处理必要的个人数据以实现目的；
b) 根据第 6 节向数据主体提供有关分析的充分信息。如果分析涉及自动决策，数据主体有权获得有关已达成决定的解释以及有关反对此类决定的权利的信息；
c) 使用适当的数学或统计程序进行分析；
d) 根据第节实施适当的技术和组织措施 0;和
e) 以考虑到数据主体的权益所涉及的潜在风险的方式保护个人数据，并且除其他外，防止基于特殊类别的个人数据对个人产生歧视性影响或导致采取此类措施影响。

笔记！

分析应在进行前由数据隐私团队预先批准。

个人数据的数据保留、存储和删除

Getinge 公司应确保个人数据的处理时间不超过：

a) 与处理目的相关的必要信息；和
b) 数据保护法允许。

Getinge 公司应实施处理以确保满足本节中的要求。

笔记！

一些国家（例如俄罗斯和中国）要求所有关于其公民的个人数据都存储在本国境内。在其他国家/地区，如果出于特定目的处理特定个人数据，则可能需要在本地存储特定个人数据（例如瑞典要求将会计信息存储在其境内）。如果有必要，本地化要求通常不会阻止 Getinge 在其他地方存储个人数据的副本。

7. 处理的评估和记录

处理活动记录

根据数据保护法的要求，Getinge 公司负责保存公司处理活动的记录。所有记录都应保存在数据隐私团队选择和处理的合规工具中。更多信息可以在数据隐私内联网页面上找到。

当 Getinge 公司作为数据控制者和数据处理者时，本节中的要求均适用。

在开始新的处理活动之前评估合法性

在进行新的处理活动或对正在进行的活动进行更改之前，Getinge 公司应评估个人数据处理的合法性并记录评估结果。这也适用于之前未评估和/或记录的任何正在进行的处理活动。

当 Getinge 公司作为数据控制者和数据处理者时，本节中的要求均适用。

数据保护影响评估

如果个人数据的处理可能对数据主体的权利和自由造成高风险，Getinge 公司应在启动此类设想的处理之前，评估处理操作对保护个人数据的影响（数据保护影响评估）。当 Getinge 公司使用新技术并考虑处理的性质、范围、背景和目的时，数据保护影响评估可能特别相关。

数据保护影响评估应始终由数据隐私团队代表 Getinge 公司执行。Getinge 公司应在评估过程中配合数据隐私团队，包括但不限于提供必要的信息。

8. 数据主体权利

数据主体请求的处理

以下适用于数据主体的请求：

a) 来自数据主体的所有请求应立即转发给数据隐私团队并由其处理。
b) 数据主体在行使数据主体权利时可能不会面临负面后果。
c) 所有数据主体请求均应保密处理。
d) Getinge 公司应与数据隐私团队合作，以便数据隐私团队能够及时答复请求。

请注意，数据主体权利不是绝对的，可能存在例外情况。

处理数据主体权利的流程

Getinge 公司负责实施流程以协助数据隐私团队处理数据主体的以下权利：

a) 请求访问个人数据。这包括数据主体有权接收有关个人数据处理相关信息的权利，并确保数据可移植性的权利。
b) 要求更正不准确的个人数据。
c) 请求删除个人数据。
d) 当处理基于 Getinge 的合法利益时，包括当处理涉及分析时，随时反对处理个人数据。
e) 获得对个人数据的限制。

9. 个人数据的传输

关于转账的一般信息

个人数据只能为实现处理目的而转移。个人数据的传输不仅包括通过电子邮件等电子信息发送个人数据，还包括何时可以访问或查看个人数据。个人数据被视为已传输，即使只是临时访问、查看或以其他方式处理。

例子

当法国的一家 Getinge 公司将个人数据存储在一个文件夹中时，个人数据将被转移，Getinge 在中国的员工可以访问该文件夹（另请参阅本第 9 节关于将个人数据从欧盟/欧洲经济区转移到欧盟/欧洲经济区以外的国家/地区）。

将个人数据从欧盟/欧洲经济区传输到欧盟/欧洲以外的国家/地区 EA

作为主要规则，位于欧盟/欧洲经济区的 Getinge 公司不得将个人数据传输到欧盟/欧洲经济区之外。此类转移只能在绝对必要的情况下进行。

如果绝对有必要将个人数据从欧盟/欧洲经济区国家/地区传输到欧盟/欧洲经济区以外国家/地区，Getinge 公司应确保：

a) 根据数据保护法，此类传输受到充分的保护，包括但不限于基于以下方面的传输：
    i. 欧盟委员会做出的充分性决定；
    ii. 欧盟委员会采用的欧盟标准合同条款；或者
    iii. 明确同意。
b) 如有必要，已进行转移影响评估。

在传输个人数据之前，数据主体有权根据第 6 条接收有关传输和适用的充分保护措施的信息。

10. 在 Getinge 内部共享和披露个人数据

Getinge 员工和顾问只能向 Getinge 内部需要此类数据以执行工作任务的个人共享和披露个人数据，并且出于合法的商业目的共享或披露此类个人数据。个人数据只能在实现处理目的所需的范围内共享或披露。不得共享或披露个人数据，因为它可能对接收者来说“很高兴拥有”。

11. 数据处理器

协议条款的一般规定

如有必要，Getinge 公司有责任在 Getinge 的标准业务和雇佣协议中包含个人数据处理条款和/或数据处理协议。

如果现有协议已经存在，Getinge 公司应在必要时更新此类协议，包括个人数据处理条款和/或相关数据处理协议。

笔记！

在需要数据处理协议的情况下，应始终使用数据隐私内联网页面上提供的数据处理协议模板。

Getinge 作为第三方的数据处理者

如果 Getinge 公司代表第三方（例如客户）处理个人数据，Getinge 和第三方应签订数据处理协议。Getinge 公司应确保使用内联网上可用的适用模板。

例子

在大多数情况下，Getinge 在向医院提供我们的软件解决方案时充当数据处理者。当我们提供软件支持时，Getinge 需要访问或以其他方式处理个人数据就是这种情况。对于这些情况，医院将充当数据控制者。

与外部数据处理器签约

如果第三方（例如供应商）将代表 Getinge 处理个人数据，则 Getinge 和第三方应签订数据处理协议。Getinge 公司应确保使用内联网上可用的适用模板。

例子

如果 Getinge 购买新的 IT 系统/解决方案，其中包括 IT 系统/解决方案的供应商代表 Getinge 处理个人数据（例如存储个人数据和/或在提供支持时访问个人数据），Getinge 和供应商应进入进入数据处理协议。在这种情况下，Getinge 是数据控制者，供应商是数据处理者。

Getinge 作为与其他 Getinge 公司相关的数据处理者

如果一家 Getinge 公司代表另一家 Getinge 公司处理个人数据，双方应签订集团内部数据处理协议。Getinge 公司/职能部门应确保：

a) 使用数据隐私内联网页面上可用的适用模板；或者

b) 已经签订了集团内部数据处理协议。

例子

如果 Getinge IT 协助 Getinge HR 提供支持，包括 Getinge IT 代表 Getinge HR 处理个人数据，则应签订集团内数据处理协议。在这种情况下，Getinge IT 是数据处理者，Getinge HR 是数据控制者。

12. 技术和组织安全措施

所有 Getinge 公司都应遵守 Getinge 关于信息安全的政策和指令。Getinge 公司还应实施适当的技术和组织措施，以确保与风险相适应的安全级别。实施此类措施时应考虑以下因素：

a) 最先进的技术；
b) 实施成本；
c) 处理的性质、范围和目的；和
d) 数据主体的权利和自由的可能性和严重性风险。

每个 Getinge 公司都有责任确保个人数据的处理符合数据保护法，包括采取适当的技术和组织措施，例如访问权限、标记个人数据以供删除、自动删除和记录数据。关于访问权限，Getinge 公司应确保对个人数据的访问反映员工和顾问的角色，包括在 Getinge 内部角色发生变化的情况下。

13. IT 解决方案处理个人数据

每个 Getinge 公司都有责任确保用于处理个人数据的新的和现有的 IT 功能、解决方案和/或服务符合数据保护法，包括但不限于以下方面的要求：

a) 隐私设计和默认；
b) 数据保留；
c) 数据主体请求，包括数据可移植性；
d) 足够的技术和组织安全措施；和
e) 访问权。

在使用新的 IT 解决方案之前和对现有 IT 解决方案进行更改之前，Getinge 公司应及时将隐私风险、目的和正在处理的个人数据告知数据隐私团队。还应向数据隐私团队提供有关在现有 IT 解决方案中处理个人数据的信息。

进一步参见：信息安全指令

14. 隐私设计和默认

在 Getinge 开发、设计、选择和使用包含个人 Pata 处理的应用程序、服务和产品时，应考虑设计和默认隐私原则。这些原则应在确定处理方式和处理本身时实施。

Privacy by design 是系统工程的一种概念和方法，它在整个工程过程中都考虑了数据保护。隐私设计侧重于确保隐私从一开始就嵌入到信息技术、业务流程、物理空间和网络基础设施中。

Getinge 应确保其系统和流程在设计时特别考虑到数据保护。数据保护不应该是事后的想法，而应该融入实体开展业务的方式中。

默认情况下的隐私意味着数据控制者应实施机制，以确保在默认情况下仅针对处理的每个特定目的处理必要的个人数据，尤其是不会收集或保留超出这些目的所需的范围，无论是在数据量和存储时间。特别是，已实施的机制应确保默认情况下个人数据不会被无限数量的个人访问。

例子

例如，当 Getinge 构建用于存储或访问个人数据的新 IT 系统、制定具有数据隐私影响的政策或策略、启动个人数据共享或用于新目的时，默认情况下考虑隐私是相关的。

设计项目、流程、产品或系统时，在设计之初就默认考虑到隐私，这有几个好处，包括：

a) 在早期阶段发现潜在问题的可能性，解决这些问题往往更简单，成本更低；
b) 提高整个组织的数据隐私意识；
c) 履行数据保护法义务的可能性增加，同样，违规的可能性降低；和
d) 项目、流程、产品或系统不太可能侵犯隐私并对个人产生负面影响。

尤其是当 Getinge 设计和开发与个人数据相关的产品和服务时，应定义有关 Getinge 应如何通过设计和默认要求遵守隐私要求的相关细节。

15. 个人数据泄露

所有个人数据泄露均应根据数据隐私内联网页面上描述的流程立即报告。

Getinge 公司应：

a) 确保用于处理个人数据的所有解决方案都能够报告个人数据泄露；
b) 实施支持检测个人数据泄露的措施；
c) 记录个人数据泄露的情况，包括影响、可能的风险以及已采取或计划采取的补救措施；和
d) 在调查和补救个人数据泄露事件时与数据隐私团队合作。

进一步了解：个人数据泄露指令

16. 监管机构

与监管机构的所有联系均应由数据隐私团队处理。Getinge 公司应根据要求与监管机构合作。

17. 偏差

偏离本全球政策的行为应获得与最初批准全球政策时相同的授权级别。

18.违反全球政策 – 发言向上

不要犹豫，提出问题。任何怀疑违反本全球政策的 Getinge 员工都应向其直属经理、道德与合规办公室或使用 Getinge 举报热线举报并提出问题。Getinge 举报热线可在 Getinge 内部和外部网页上找到。在 Getinge，我们不接受对直言不讳、表达疑虑或意见的人进行任何形式的报复。

进一步了解：全球畅所欲言和禁止报复指令

19.角色和职责

所有 Getinge 员工均有责任阅读、理解并遵守本全球政策。每位员工都有责任按照本全球政策行事。

每位直线经理都有责任确保每位团队成员都能访问本全球政策和相关指令、说明和指南。

日常强化，包括数据隐私领域的定期信息和培训，以及合规跟进，是每位经理职责的一部分。

违反本全球政策可能导致纪律处分，直至并包括解雇。

二十、指导与协助

就 Getinge 在数据隐私领域的立场而言，为了指导我们的行为，制定了本全球政策和若干指令和说明。如果您对本全球政策有疑问或不确定适用哪些规则，请联系数据隐私团队。

21.有用的链接

标题

个人数据泄露指令

数据隐私治理指令

信息安全指令

全球畅所欲言和禁止报复指令