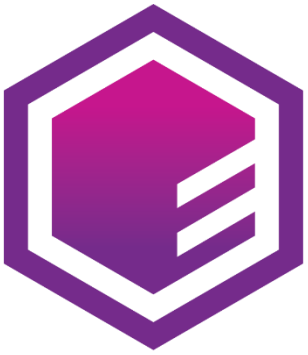

ENTRUST

全球个人数据保护政策

文件版本	1.6
日期	2023 年 9 月 5 日

ENTRUST

目录

1. 引言

Entrust Corporation 及其子公司和附属公司（统称为“Entrust”或“公司”）作为数据控制者处理本公司同事、临时工、合作伙伴、供应商和客户的个人数据，以及作为数据处理者处理本公司的客户及其最终用户的个人数据。在 Entrust 处理个人数据时，我们会遵守法律、合同和道德义务，并且秉承完全透明的原则。

2. 目的

本政策规定了公司全球数据隐私计划的要求和要素，以确保我们遵守相关法律与合同义务以及符合认证和审计要求。本政策在全球范围内适用于由以下两者执行的所有个人数据处理：Entrust 直接执行；代表 Entrust 处理个人数据的第三方间接执行。

3. 定义

“数据控制者”是指确定个人数据处理目的和方式的实体，其与 ISO 27701 定义的“个人可识别信息控制者”具有相同含义。

“数据处理者”是指代表数据控制者处理个人数据的实体，其与 ISO 27701 定义的“个人可识别信息处理者”具有相同含义。

“数据保护影响评估”是指数据控制者或数据处理者评估以下情况的隐私风险时所进行的记录分析：数据处理很可能会给数据主体的权利和自由带来高隐私风险。

“**数据保护法律**”是指适用于 Entrust 的所有个人数据保护和隐私法律法规，包括但不限于欧盟《通用数据保护条例》(GDPR)、英国《通用数据保护条例》(UK GDPR)、加拿大《个人信息保护和电子文件法》(PIPEDA) 以及美国各州的隐私法律，在每种情况下都可能被修正、取代或替换。

“数据主体”是指与个人数据相关的已识别或可识别的个人或家庭，其与 ISO 27701 定义的“个人可识别信息负责人”具有相同含义。

“数据传输影响评估”是指数据控制者或数据处理者针对以下内容所进行的记录分析：向欧洲经济区（即 GDPR 所涵盖的国家/地区）以外没有得到欧盟委员会充分认定的国家/地区传输个人数据所产生的影响和安全问题。

“合法利益影响评估”是指数据控制者或数据处理者针对以下内容所做的记录分析：合法利益是否可用作处理个人数据的法律依据。该评估包括一项三重检验，分析以下三个方面：个人数据处理的目的是否在于追求合法利益、个人数据处理对达成上述目的是否有必要，以及数据主体的利益是否优先于合法利益。

“个人数据”具有“个人可识别信息”、“个人信息”或数据保护法律定义的同等术语的含义。

“个人数据事件”具有数据保护法律定义的“安全事件”、“安全漏洞”或“个人数据泄露”或同等术语的含义，并包括 Entrust 了解到个人数据已遭或可能已遭访问、披露、更改、丢失、销毁或经未授权人员以未经授权的方式使用的任何情况。

“处理”是指对个人数据进行的任何操作或一系列操作，无论是以自动方式进行（例如，收集、记录、结构设置、存储、改编或更改、检索、咨询、使用以及通过传输、传播披露）还是以其他方式提供、排列或组合、限制、删除或销毁。处理还包括向第三方传输或披露个人数据。

“敏感个人数据”是个人数据的一个子集，是指有关数据主体且如果丢失、泄露、被访问或不当披露，可能会对数据主体造成伤害、尴尬、不便或不公平，因此需要加强保护的信息。

“特殊类别数据”是个人数据的子集，是指有关个人种族或民族血统、性生活或性取向、政治见解、宗教或哲学信仰、工会会员资格、遗传学数据、生物特征数据（例如，眼睛颜色、头发颜色、身高、体重）、病史或刑事定罪、犯罪有关的信息。

4. 个人数据处理核心原则

Entrust 在处理个人数据时遵循以下核心原则：

- **合法性和适当性**：我们确保收集个人数据的目的合法、相关且必要。
- **准确性和保留期**：我们不断更新系统，提供用于更新或删除不准确的个人数据的机制，并且保留个人数据的时间不会超过实现合法处理目的所需的时间。
- **保密性和完整性**：我们确保个人数据在处理过程中始终安全并受到保护，但如果确实发生安全事件和数据泄露事件，我们会迅速而适当地做出响应，包括根据要求及时提供通知。
- **透明**：当我们处理数据主体的个人数据时，我们会详细告知他们。我们很清楚这些个人数据的使用目的、使用方式，以及相关的处理和保护措施。

我们都有责任妥善处理和保护个人数据，并明白如果做不到这一点，不仅有可能损害客户对 Entrust 的信心，还可能导致公司面临巨额罚款和处罚。

5. 数据分类

Entrust 保留其处理活动的集中记录。所有个人数据都归入以下类别之一：

6. 合法性与适当性

6.1 处理个人数据的法律依据

公司仅在法律允许的情况下处理个人数据，并向数据主体发出适当通知。Entrust 主要依赖以下法律依据进行数据处理：

- 履行合同；
- 遵守法律义务，包括但不限于执法部门的合法要求；
- 合法利益，除非数据主体的利益或基本权利和自由优先于此类利益；以及
- 同意书。

如果同意书是数据处理的法律依据（例如，出于营销目的），Entrust 确保该同意书是具体数据主体知情、自由给予，并明确表示数据主体的意愿。数据主体有权出于任何原因随时撤回同意书。

6.2 隐私评估

6.2.1 “通过设计保护隐私”评估

Entrust 在设计和开发新产品和服务或对产品和服务进行重大修改时，以及启动供应商云托管解决方案（包括在第三方软件应用程序中获得许可的解决方案）时，会根据核心原则评估个人数据处理。Entrust 的开发和供应商准入流程中包含“通过设计保护隐私”评估，并由合规与信息安全部门进行审查。未经批准，开发流程不得向前推进。

6.2.2 数据保护影响评估 (DPIA)

当预期个人数据处理会对个人的权利和自由构成高风险时，Entrust 会填写一份正式的 DPIA，以记录和评估处理的目的、Entrust 采用哪些措施来遵守相关数据保护法律以及降低对数据主体权利构成的潜在风险。

6.2.3 数据传输影响评估 (DTIA)

如果 Entrust 打算将个人数据传输到欧洲经济区 (EEA) 以外不会受益于欧盟委员会充分认定的国家/地区，Entrust 会填写一份正式的 DTIA，以分析传输带来的的影响和安全问题，特别是在接收国/地区的法律可能允许政府访问正在传输的个人数据的情况下。

6.2.4 合法利益影响评估 (LIIA)

如果 Entrust 依赖合法利益作为处理个人数据的法律依据，公司会填写一份正式的 LIIA，以记录和评估合法利益，确定是否有必要进行处理，并评估数据主体的权利是否大于合法利益。

6.2.5 敏感和特殊类别数据的处理标准

作为数据控制者，Entrust 代表不同业务系统的同事处理敏感的个人信息，并在自愿的基础上和当地法律允许的情况下处理一些有限制的特殊类别数据。公司制定了适当的控制措施，并在适用的 DPIA、《敏感和特殊类别数据的访问控制标准》中进行了概述，并且对处理这些敏感和特殊类别数据的同事专门进行了强化隐私培训。

6.3 合同保护

6.3.1 集团内部数据传输协议 (IGDTA)

Entrust 集团内的公司（即所有公司实体和子公司）签订集团内部数据传输协议，以确保在欧洲经济区以外但在 Entrust 集团内部，且不会受益于欧盟委员会充分认定的国家/地区传输个人数据时，采取适当的保护措施。

6.3.2 数据处理协议 (DPA)

Entrust 集团以外的公司如果为 Entrust 或代表 Entrust 处理个人数据，必须与 Entrust 签订数据处理协议，以确保第三方（例如，提供商、供应商、渠道合作伙伴）采取适当的技术和组织措施来遵守相关的数据保护法律。如果 Entrust 通过标准的客户 DPA 充当数据处理者，Entrust 将做出同等承诺。

6.3.3 一般隐私条款

与客户、供应商和合作伙伴签订的标准协议以及 Entrust 的标准保密协议 (NDA) 中也包含有关隐私的合同用语。

7. 准确性和保留期

7.1 记录管理

全球记录管理计划确保正式定义处理个人数据的保留期，旨在保证个人数据仅在所需时间内保留，并且在指定的保留期结束时删除、销毁或匿名化个人数据。全球记录管理政策规定了所有记录的处理要求（不仅限于包含个人数据的记录），随附的记录保留时间表定义了公司保存的每种记录的保留期。

7.2 个人数据的存储和备份

Entrust 在公司直接或间接管理的多个服务器位置存储和备份个人数据。公司向 IT 和相关供应商（适用于非 IT 管理的云托管应用程序）提供了标准指导，引导他们如何正确处理这些服务器上的个人数据，包括存储和备份。

在商业上不可行的情况下，Entrust 不会在保留期结束时从其备份媒体和服务器中删除个人数据的副本；但是，Entrust 以这种方式保留的个人数据在使用过程中会受到相同安全标准的保护，并且个人数据仍然受到保密条件的约束，只能在适用法律要求的情况下访问。

7.3 删除或销毁个人数据

《全球记录管理政策和信息分类处理标准》说明了在规定的保留期结束时妥善处理所有类型的记录的相关要求。以下原则尤其适用于包含个人数据的记录：

- 除非为了达到指定的处理目的，否则不应复制个人数据，并且复制的任何副本都应保留所有原始的机密或专有标记。
- 当不再需要保留纸质记录并且不得以任何其他方式处置时，必须将其粉碎并安全地处置。
- 如果不再需要电子版的个人数据，应将其删除或匿名化。
- IT 部门负责根据相关信息安全政策和标准销毁或删除包含个人数据的电子设备（例如，笔记本电脑、台式电脑、公司拥有的移动设备以及自带设备 (BYOD) 上的工作数据）。

8. 保密性和完整性

8.1 信息安全

公司在处理个人数据时，会采取相应措施来确保个人数据安全，并保护其免遭未经授权或非法处理、意外丢失、销毁或损坏。Entrust 可通过以下方式做到这一点：

- 在法律或合同要求以及商业上可行的情况下，对静态和传输中的个人数据进行加密；
- 通过定期测试或实施的正式业务恢复和灾难恢复计划，确保用于处理个人数据的系统和服务的持续保密性、完整性、可用性和恢复能力；
- 确保在发生物理或技术事故时，及时恢复对个人数据的访问；
- 定期测试、评估和评价保护个人数据的技术和组织措施的有效性；
- 制定强制执行的人身安全标准，要求存放个人数据的办公桌和橱柜保持上锁，不允许路过的人通过个人显示器/屏幕看到个人数据，在无人看管时将电子设备（例如，计算机、平板电脑）上锁或退出公司的系统。

在评估适当的安全控制时，Entrust 会考虑与处理相关的风险，特别是被意外或非法销毁、丢失、更改、未经授权披露或访问已处理的个人数据的风险。

如果 Entrust 聘请第三方代表公司处理个人数据，此类第三方将根据 Entrust 的书面指示进行处理，并遵守合同条款（例如 DPA），以至少等同于公司对自身安全要求的适当技术和组织措施来妥善处理个人数据。如果没有设置这些机制，个人数据不会在 Entrust 外部共享。配备各种安全工具（例如 DLP），以确保个人数据不会在未经授权的情况下离开组织。

8.2 测试

如果没有事先批准的正式安全例外情况，在任何 Entrust 测试环境中都不能使用个人数据。所有测试环境都必须遵守生产环境的现行标准和制定的控制措施，测试完成后，必须立即删除所有获准用于测试环境的个人数据。 如需更多详情，请查看安全软件开发生命周期 (S-SDLC)。

8.3 报告个人数据事件

个人数据事件可能有多种形式，包括但不限于：

- 丢失包含个人数据的移动设备或硬拷贝文件（例如，意外将设备丢在公共交通工具上）；
- 包含个人数据的移动设备或硬拷贝文件遭盗窃；
- 人为错误（例如，同事意外向非计划收件人发送包含个人数据的电子邮件，或者意外更改或删除了个人数据）；
- 网络攻击（例如，打开来自未知第三方的电子邮件附件，其中包含勒索软件或其他恶意软件）；

- 允许未经授权的使用/访问（例如，允许未经授权的第三方访问 Entrust 办公室或系统的安全区域）；
- 物理销毁和损失（例如，火灾或洪水）；或
- 第三方通过欺骗手段（例如，网络钓鱼或诈骗攻击）从 Entrust 获取信息。

以下情况可能与发生个人数据事件有关：

- 与活跃用户帐户有关的活动异常登录和/或系统活动过多；
- 异常的远程访问活动；
- Entrust 的工作环境中存在或可访问欺骗性无线 (Wi-Fi) 网络；
- 设备故障；或
- 连接至或安装在 Entrust 系统中的硬件或软件键盘记录器发生故障。

如果有同事意识到或出于任何理由怀疑可能已经发生或即将发生个人数据事件，请立即发送电子邮件到 SOC@entrust.com 联系 Entrust 安全运营中心。

8.4 个人数据事件响应

如果发生实际或即将发生的个人数据事件，Entrust 将实施公司事件响应和处理程序（由信息安全部门维护），以最大限度地减少事件的影响，并根据法律和/或合同的要求通知监管机构、数据主体和/或其他各方。响应通常会涉及以下方面：

- 调查事件，以确定已经或可能造成的损害或伤害的性质、原因和程度；
- 采取必要措施阻止事件继续发生或重复发生，并限制对受影响数据主体的伤害；
- 评估是否有义务通知其他各方（例如，国家数据保护机构、受影响的数据主体和合同方）并及时发出相关通知；以及
- 记录有关个人数据事件和所采取的应对措施的信息，包括记录是否通知监管者或受影响方的决定。

9. 透明

Entrust 通过强大的内部和外部登录页面为公司全球数据隐私计划提供透明度。

9.1 隐私声明

Entrust 作为数据控制者和数据处理者向数据主体提供有关其个人数据处理的通知。这些信息可通过 Entrust 针对网络用户、求职者和同事的各种隐私声明以及此处提供的个人产品隐私声明获得。此类声明提供以下信息：

- Entrust 处理的个人数据类型；
- 处理的目的和法律依据；
- 进行处理的第三方（如果适用）；
- 处理的地点和持续时间；

- 个人数据的任何跨境传输；
- 处理期限；
- 数据主体权利；以及
- 任何人工智能/自动决策过程的详细信息

9.2 培训

Entrust 每年为同事提供有关数据保护责任的强制性培训。入职之时以及入职后每年开展“数据隐私入门培训”。除了面向全体同事提供的“数据隐私入门培训”之外，Entrust 还做了以下规定：处理敏感和特殊类别数据的同事每年要完成“进阶版数据隐私培训”，开发和设计软件产品和服务的同事每年要完成“通过设计保护隐私培训”。根据需要，Entrust 会持续制定和安排其他特定职能的隐私培训。

9.3 数据主体权利

当 Entrust 处理个人数据时，数据主体享有数据保护法律规定的某些权利。尽管这些权利因司法管辖区而异，但数据主体通常有权：

- 要求提供与他们有关的个人数据的信息；
- 更正有关他们的任何不准确的个人数据，并将不完整的个人数据填写完整；
- 如果 Entrust 只为追求自身合法利益，反对公司处理他们的个人数据。但如果公司的合法利益大于数据主体的合法利益，或者如果 Entrust 出于法律原因需要处理个人数据，则即使数据主体反对，Entrust 仍可继续处理个人数据；
- 要求 Entrust 销毁所持有的与数据主体有关的个人数据。如果个人数据对于处理目的而言仍为必需，并且 Entrust 有继续处理的法律依据，公司可以拒绝此请求；
- 在某些情况下，要求 Entrust 对其个人数据的处理仅限于存储。

Entrust 将逐案评估数据主体在数据保护法律下的权利，并遵守数据主体请求程序来确定如何满足请求。一般而言，Entrust 将利用数据主体在欧盟《通用数据保护条例》下的权利作为满足所有访问请求的基准，并根据适用于数据主题的数据保护法律，在对数据主体更有利的情况下应用额外权利。如果数据主体行使了上述权利，并且 Entrust 已向第三方披露了相关个人数据，公司将竭尽全力确保第三方也遵守数据主体的意愿。

希望获取 Entrust 所持有的有关他们个人数据信息的数据主体，应该通过提交正式的数据主体请求 (DSR) 取得信息。如果同事直接收到请求（无论是口头还是书面形式），请立即将请求转发至 privacy@entrust.com。

9.4 监管机构

相关数据监管机构的联系信息因地点而异。欧洲数据保护委员会主管机构的列表可从此处获取。英国 (UK) 信息专员办公室 (ICO) 相关信息可从此处获取。加拿大隐私专员办公室相关信息可从此处获取。

10. 遵守规定

所有员工和临时工都应遵守本政策。此外，所有业务部门都必须确保制定适当的当地标准和程序，以遵守本政策及其司法管辖区内适用的数据隐私法规。违反本政策将受到严肃对待，可能导致纪律处分，严重者会遭解雇。本政策可能随时更新或修订。

11. 例外情况

本政策不存在任何例外情况。

12. 所有权和审查

本政策归首席法律与合规官所有，且应每年进行审查。

12.1 联系人信息

如对本政策或 Entrust 的个人数据处理有任何疑问，可以直接联系 privacy@entrust.com。