全球个人数据保护政策

文件版本	1.4
日期	2021 年 12 月 10 日

目录

1. Introduction 3
2. Purpose 3
3. Policy Requirements 3
3.1 Definitions 3
3.2 Our Responsibility 4
3.3 Processing Personal Data 4
3.4 Sensitive and Special Category Data Processing 4
3.5 Legal Grounds for Processing Personal Data 4
3.6 Data Records Management 5
3.7 Erasure or Destruction of Personal Data 5
3.8 Information Security 6
3.9 Reporting a Personal Data Incident 6
3.10 Personal Data Incident Response Plan 7
3.11 International Data Transfers and Transfers to Third Parties 7
3.12 Notifying Data Subjects 8
3.13 Privacy by Design and Data Protection Impact Assessments 9
3.14 Data Subject Rights 9
3.15 Data Subject Access Rights 9
3.16 Training 10
3.17 Data Protection Officer 10
4. Compliance 10
5. Exceptions 10
6. Ownership and Review 10
6.1 Contact Information 10
6.2 Document Properties and Revision History 10

1. 简介

作为企业和雇主，Entrust 公司及其子公司和关联公司（统称为“Entrust”或“公司”）有必要收集、存储和处理有关我们员工、临时工、客户、供应商及我们与之合作并代表我们提供产品或服务的其他第三方的个人数据。

随着 2018 年 5 月 25 日欧洲《通用数据保护条例》（“GDPR”）以及其他关于数据保护的适用法律的出台，我们在收集、使用和存储个人数据方式方面必须遵守更高的要求。

2. 目的

本政策旨在帮助我们所有人遵守法律义务，让我们所持有其个人数据的个人对我们有信心。 本政策适用于所有 Entrust 员工、临时工以及代表 Entrust 处理数据的第三方。 除非另有说明，否则本政策适用于 Entrust 运营和/或开展业务的所有国家/地区。

3. 政策要求

3.1 定义

“数据控制者”或**“个人身份信息控制者（PII 控制者）”**是指确定处理个人数据的目的和方式的实体。

“数据处理者”或**“个人身份信息处理者（PII 处理者）”**是指代表控制者处理个人数据的实体。

“数据保护法”是指所有适用的数据保护和数据隐私法律法规，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《个人信息保护与电子文件法》(PIPEDA) 以及《加州消费者隐私法案》(CCPA)。

“数据主体”或**“个人身份信息负责人（PII 负责人）”**是指与个人数据相关的已识别或可识别的个人或家庭。

“数据用户”术语用于描述其工作涉及为 Entrust 处理个人数据的任何员工、顾问、独立承包商、实习生、临时工或代表 Entrust 行事的第三方（包括数据处理者）。

“个人数据”应具有“个人身份信息”、“个人信息”、“个人数据”或数据保护法定义的同等术语的含义。

“个人数据事件”应具有数据保护法赋予“安全事件”、“安全漏洞”或“个人数据泄露”等术语的含义，并应包括供应商了解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，无论是否以自动方式进行，例如收集、记录、结构设置、存储、改编或更改、检索、咨询、使用、通过传输、传播或其他方式披露提供、对齐或组合、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。

“特殊类别数据”或**“特殊类别个人信息”**是个人数据的子集，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（眼睛颜色、头发颜色、身高、体重）、病史或刑事定罪和犯罪行为或相关安全措施。

3.2 我们的责任

根据具体情况，Entrust 可以为数据控制者或数据处理者。 作为数据控制者，Entrust 负责制定符合数据保护法的实践和政策。 同样重要的是，Entrust 能够证明遵守这些法律。 公司可通过以下方式做到这一点：

- 实施使公司能够遵守数据保护法的政策，例如本政策、有关文档保留和数据安全的政策以及 Entrust 的隐私声明；
- 就数据保护要求向员工、临时工和代表 Entrust 行事的第三方传达并进行培训；
- 调查未遵守 Entrust 数据保护政策的情况，并采取适当的补救措施和/或进行纪律处分；
- 调查、补救以及在某些情况下提供个人数据事件的通知；
- 在需要时，针对新类型的处理操作进行数据处理影响评估；
- 定期对 Entrust 的数据保护政策和程序进行内部审计；以及
- 在新产品设计之初就考虑到数据保护。

3.3 处理个人数据

公司处理或代表 Entrust 处理的任何个人数据必须：

- 以公平、合法且透明的方式处理；
- 仅出于特定、明确且合法的目的进行处理；
- 与处理数据的合法目的相关，并且仅限于为处理数据的合法目的所必需；
- 准确无误并保持最新状态，确保在合理可行的情况下，立即删除或纠正不准确的个人数据；
- 保留时间不得超过为实现数据收集的目的所必需的时间；以及
- 以确保个人数据适当安全的方式进行处理，包括防止未经授权或非法处理、意外丢失、销毁或损坏。

3.4 敏感和特殊类别数据处理

Entrust 代表各业务系统中的同事处理敏感信息，以及 Workday 中有限的特殊类别数据。 特殊类别数据、福利和薪资 DPIA 以及敏感和特殊类别数据访问控制标准中已规定并概述了相应的控制措施，详情可见于 Entrust 合规网站。

3.5 处理个人数据的法律依据

公司只能在数据保护法允许的情况下处理个人数据。 以下是 Entrust 处理个人数据所秉持的依据：

需要处理数据：

- 为履行数据主体为当事一方的合同，或在签订合同前应数据主体的要求采取措施；
- 为遵守 Entrust 所承担的法律义务，包括但不限于执法机构的法律要求；和/或
- 为追求 Entrust 的合法利益，除非数据主体的利益或基本权利和自由凌驾于此类利益之上。

除上述依据外，Entrust 还可以在数据主体同意出于一个或多个特定目的处理的情况下，处理个人数据，前提是数据主体自愿同意且该同意具体、有根据且明确表示了数据主体的意愿。 若 Entrust 利用此同意作为处理依据，数据主体有权出于任何理由随时撤回该同意。

Entrust 有时还可能需要为客户、员工或临时工处理特殊类别的个人数据（例如，安全雇用实践所要求）。 当 Entrust 处理或通过第三方代表其处理特殊类别的个人数据时，Entrust 将确保在适用的情况下满足以下条件：

- 数据主体明确同意出于一个或多个特定目的处理特殊类别的个人数据；
- 为履行雇用法、社会保障或社会保护法或劳资协议规定的义务，必须进行处理；
- 出于预防或职业医学的目的，或为了评估员工的工作能力，必须进行处理；
- 在数据主体因身体或法律原因而无法表示同意的情况下，为保护数据主体或他人的切身利益，必须进行处理；
- 处理与数据主体公开的个人数据有关；和/或
- 对建立或辩护法律要求而言必须进行处理。

3.6 数据记录管理

Entrust 集中记录公司收集的个人数据类型以及收集这些数据的原因。 Entrust 只会出于集中记录所规定的特定目的，或数据保护法特别允许的任何其他目的处理个人数据。 Entrust 将在首次收集数据时，或在不可能的情况下尽快将这些目的告知数据主体。

Entrust 将仅在向数据主体告知的目的所需范围内处理个人数据。 这意味着 Entrust 不得要求或在其系统中记录超出所需的个人数据。 公司已采取适当的技术和组织措施，确保删除或销毁不再需要的个人数据。

本公司还采取合理措施，确保所持有的任何个人数据准确无误并保持最新状态。 Entrust 旨在在收集时以及之后定期检查任何个人数据的准确性。 公司将采取一切合理措施，在无不当延误的情况下，在任何情况下，以及在数据主体提出请求后的一个月内（或有特定原因导致一个月不可行的情况下，最多三个月内）删除、销毁或修改不准确或过期的数据。

有关记录管理和保留的更多信息，请访问全球记录管理政策和随附的记录保留时间表。

3.7 删除或销毁个人数据

当不再需要保留包含个人数据的纸质记录时，必须对其进行粉碎并安全处理。 *包含个人数据的纸质记录不得以任何其他方式处理。*

删除电子版个人数据时，应采取一切可行措施，使有关数据无法再使用。 如果不可能完全删除个人数据，必须采取合理措施以确保尽可能最大程度地删除数据。

IT 部门负责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携设备上的工作数据）。

3.8 信息安全

公司在处理个人数据时，会采取合理措施以确保数据安全，并保护数据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：

- 在可行且适当的情况下，加密个人数据；
- 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、可用性和恢复性；
- 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；以及
- 促进对确保数据安全的技术和组织措施的有效性的测试、评定和评估。

在评估相应的安全级别时，Entrust 会考虑与处理相关的风险，特别是意外或非法销毁、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 聘用第三方代表其处理个人数据，则此类第三方应根据书面指示进行处理并负有保密责任，有义务采取适当的技术和组织措施确保数据安全。 不得与 Entrust 或授权的第三方以外的任何人员分享个人数据。

如果办公桌和柜子内放有个人数据或任何类型的机密信息，请将它们锁好。 数据用户应确保个人显示器/屏幕不会向路人显示个人数据或机密信息，并确保在无人看管时注销计算机/平板电脑或将它们锁好。

3.9 报告个人数据事件

个人数据事件可能以多种方式发生，包括：

- 丢失包含个人数据的移动设备或硬拷贝文件（例如，不小心将设备丢在公共交通工具上）；
- 盗窃包含个人数据的移动设备或硬拷贝文件（例如，从车中或家中偷走）；
- 人为错误（例如，员工不小心向非计划收件人发送包含个人数据的电子邮件，或意外更改或删除个人数据）；
- 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）；

- 不可预见的情况，例如火灾或洪水；或
- 第三方通过欺骗手段从 Entrust 获取信息的情况。

可能发生个人数据事件的迹象包括以下方面：

- 异常登录和/或系统活动过多，特别是与活跃用户账户有关的活动；
- 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；以及
- 连接至或安装在 Entrust 系统中的硬件或软件键盘记录器。

意识到或出于任何理由怀疑已经发生或即将发生个人数据事件的同事必须立即通过电子邮件联系 Entrust 安全运营中心 SOC@entrust.com，以及合规主管 privacy@entrust.com。

3.10 个人数据事件响应计划

如果发生实际或即将发生个人数据事件，Entrust 会迅速采取行动以最大程度减少事件造成的影响，并在法律要求的情况下报告事件。 在大多数情况下，响应将涉及：

- 调查事件，以确定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）并发出相关通知。 如果有义务通知数据保护机构，则通常必须在公司（包括其任何员工）意识到该事件后的 72 小时内进行报告；以及
- 记录有关个人数据事件和应对措施的信息，包括解释通知或不通知决定的文档。

3.11 个人数据的存储和备份

Entrust 利用多个服务器位置来存储和备份个人数据。 关于 Entrust 与之合作并代表同事和客户处理个人数据的第三方所用的服务器位置，请查阅同事个人数据的相关数据保护影响评估，以及客户个人数据的外部子处理者页面和产品隐私声明。 这些文档全部位于内部的合规页面，或外部的法律与合规网站的“数据隐私”图标下。 有关公司数据服务器位置的最新列表，同事也可以直接联系 IT 部门。

3.12 国际数据传输和传输给第三方

根据《通用数据保护条例》，Entrust 可能会将个人数据传输给欧洲经济区（“EEA”）以外的国家/地区，这些国家/地区有足够的保护措施，或者 Entrust 已采取适当措施以确保数据得到保护。

Entrust 集团内的公司（即所有公司实体和子公司）必须签署集团内部数据传输协议，以确保在欧洲经济区以外但在 Entrust 集团内部传输个人数据时采取适当的保护措施。

Entrust 集团以外的为 Entrust 或代表 Entrust 处理个人数据的公司（Entrust 作为数据控制者或数据处理者），必须与 Entrust 签订数据处理协议，确保在欧洲经济区以外传输个人数据时采取

适当的保护措施。 该协议包含的内容旨在确保第三方采取适当的技术和组织措施遵守《通用数据保护条例》，同时确保数据主体权利得到保护。

Entrust 将个人数据传输至欧洲经济区以外的国家/地区的示例可能包括：

- 在 Entrust 告知数据主体与此类传输相关的任何潜在风险（例如，该国家/地区没有同等的保护措施）后，数据主体明确同意所提议的传输；
- 传输为履行数据主体为当事一方的合同，或在签订合同前应数据主体的要求采取措施所必需；
- 传输为在数据主体因身体或法律原因而无法表示同意的情况下，为保护数据主体或他人的切身利益所必需；或
- 传输对于建立或辩护法律要求而言所必需。

对于欧洲经济区以外的每次数据传输，Entrust 将遵守欧盟委员会制定的标准合同条款（2001/497/EC、2004/915/EC 和 2010/87/EU）。[1] 请注意，如果将个人数据传输至加拿大境外，还需要签署数据传输协议。

3.13 告知数据主体

Entrust 需要向数据主体提供有关其个人数据处理的信息。 公司的《网络隐私声明》（该声明公开发布在 www.entrust.com 上）、《求职者隐私声明》（该声明公开发布在 https://www.entrust.com/legal-compliance/data-privacy/job-applicant-privacy-statement 上）以及 Entrust 内联网发布的《员工隐私声明》中都包含这些信息。 此类声明提供以下信息：

- Entrust 处理的个人数据类型；
- 处理个人数据的目的和法律依据；
- 在处理过程中是否会向任何第三方披露个人数据；
- 个人数据是否会传输至欧洲经济区和加拿大以外区域，如果会，将采取哪些保护措施；
- 个人数据的处理时长，若无法确定，公司将用于确定处理期限的标准；
- 数据主体如何获取 Entrust 所持有的个人数据副本；
- 数据主体的权利，包括如何投诉；
- 如果为遵守法律或合同而必须处理个人数据，数据主体未能提供数据或反对处理可能造成的后果；以及
- 任何存在的自动决策流程及其详细信息（若适用）。

如果 Entrust 从第三方处获取有关数据主体的个人数据，公司还将向数据主体提供以下信息：

- 从第三方处获取的个人数据的类型；以及

[1] 自 2022 年 12 月 27 日起，将根据 2021 年 6 月 4 日 委员会实施决定 (EU) 2021/914 中关于欧洲议会和理事会指令 (EU) 2016/679 向第三方国家/地区传输个人数据的标准合同条款所概述的新标准合同条款传输数据。

- 数据的来源以及数据是否来自可公开访问的来源（例如，公众可访问的网站）。

3.14 隐私始于设计和数据保护影响评估

数据保护法要求 Entrust 在新产品开发阶段要考虑到数据保护。 为履行这一义务，Entrust 必须采取措施确保数据保护成为设计流程的一部分，并尽可能减少个人数据收集。

在某些情况下（即处理会对个人的权利和自由带来高风险时），Entrust 可能需要就个人数据的处理进行正式的数据保护影响评估 (DPIA)。 此类评估包括记录开展活动的目的、Entrust 将如何遵守数据保护法，以及公司将如何减轻个人隐私的潜在风险。 如果您认为可能需要进行数据保护影响评估，请通过 privacy@entrust.com 与合规主管联系。

3.15 数据主体权利

如果 Entrust 处理个人数据，根据数据保护法，数据主体可以有权：

- 要求提供与他们有关的个人数据的信息；
- 在 Entrust 确定数据实际上不准确或不完整的前提下，纠正有关他们的任何不准确的个人数据并完善不完整的个人数据；
- 反对 Entrust 处理他们的个人数据，若公司只为追求自身合法利益而要处理其个人数据。如果公司的合法利益超过数据主体的合法利益，或者如果 Entrust 为建立或辩护法律要求而需要这样做，即使反对，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 有继续处理的合法依据，公司可以拒绝此请求；
- 要求 Entrust 对其个人数据的处理仅限于存储。 只有在以下情况下才可要求这样做：个人数据的准确性受到质疑并且仍未经验证；Entrust 不再需要个人数据，但数据主体需要这些数据以建立或辩护法律要求；数据主体反对处理个人数据；以及 Entrust 正在决定其合法利益是否凌驾于数据主体的利益之上，或者处理是否非法。

Entrust 将根据适用的数据隐私法规逐个评估数据主体的权利，以确定如何满足数据主体的访问请求。 一般来说，Entrust 将利用数据主体在欧盟《通用数据保护条例》(GDPR) 下的权利作为满足访问请求的基准，并在对数据主体更有利的情况下应用适用数据隐私法规下的权利。 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。

3.16 数据主体访问权利

希望获取 Entrust 所持有的有关他们个人数据信息的数据主体，可以提交数据主体访问请求 (DSAR) 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），请立即将请求的详细信息转发至 privacy@entrust.com。 有关按司法管辖区划分的个人数据主体权利的更全面列表，请参见合规网站上的数据主体访问请求程序。

3.17 培训

Entrust 为其员工和临时工提供有关数据保护责任的培训。 入职之时以及入职后会定期开展此培训。

3.18 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见于此处。加拿大隐私专员办公室相关信息可见于此处。

3.19 数据保护官

如果您对 Entrust 的隐私信息管理系统存有任何疑问，请联系：

Entrust Corporation

收件人： 合规总监 Jenny Carmichael

1187 Park Place

Shakopee, MN 55379

privacy@entrust.com

Entrust Deutschland GmbH 指派的数据保护官是 Althammer & Kill GmbH & Co. 公司的 Niels Kill 先生 (kontakt-dsb@althammer-kill.de)。

4. 合规

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。

5. 异常

本政策不存在任何例外情况。

6. 所有权和审查

本政策为首席法务官和合规主管所有。 应该每年审查一次本政策。 对本文档的更改应符合信息安全管理系统 (ISMS) 文档和记录控制标准。

6.1 联系方式

对本政策有任何问题或有关个人数据处理的投诉，请直接联系合规主管 privacy@entrust.com。

6.2 文档属性和修订历史

文件属性	
属性	**说明**
流通范围	内部和外部使用
分类	公开
文件所有者	首席法律与合规官 Lisa Tibbits
计划下次审查时间	2022

文件批准		
批准人姓名	**标题**	**日期**
Lisa Tibbits	首席法律与合规官	2019 年 3 月 3 日
政策治理委员会	不适用	2021 年 8 月 3 日
政策治理委员会	不适用	2021 年 12 月 16 日

修订历史			
版本	**日期**	**变更描述**	**修订者**
1.0	2019 年 4 月 19 日	初始版本	企业高级律师 Anjali Doherty；合规总监 Jenny Carmichael
1.1	2020 年 4 月 19 日	年度更新	企业高级律师 Anjali Doherty；合规总监 Jenny Carmichael
1.2	2020 年 9 月 10 日	已更新为最新的政策模板	资深合规专家 Aileen Havel
1.3	2021 年 7 月 6 日	年度修订；增加有关访问特殊类别数据的章节	企业律师助理 Aileen Havel；资深合规保证专家 Lee Jones
1.4	2021 年 12 月 10 日	更新以符合 ISO 27701 控制和外部风险评估建议	合规总监 Jenny Carmichael