全球个人数据保护政策

文件版本	1.2
日期	2020 年 9 月 10 日

目录

1 引言

作为企业和雇主，Entrust Corporation 及其子公司和附属公司（以下统称为“Entrust”或“公司”）需要收集、存储和处理与我们的员工、临时员工、客户、供应商以及接受我们的委托代表我们提供产品或服务的其他第三方有关的个人数据。

随着 2018 年 5 月 25 日欧洲《通用数据保护条例》（“GDPR”）以及其他适用的数据保护法律的出台，我们在如何收集、使用和存储个人数据方面需要遵守更严格的要求。

2 目的

此政策的目的在于帮助我们所有人遵守法律义务，使我们持有其个人数据的个人对我们有信心。 本政策适用于代表 Entrust 处理数据的所有 Entrust 员工、临时员工和第三方。 除非另有规定，本政策适用于 Entrust 运营和/或业务开展所在的所有国家/地区。

3 政策要求

3.1 定义

“数据控制者”指确定处理个人数据的目的和方式的实体。

“数据处理者”指代表控制者处理个人数据的实体。

“数据保护法律”指所有适用的数据保护和数据隐私法律和法规，包括但不限于欧盟《通用数据保护条例》(GDPR)、加拿大《个人信息保护和电子文件法》(PIPEDA) 和加利福尼亚州《消费者隐私法案》(CCPA)。

“数据主体”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”这一术语用于描述涉及为 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（包括数据处理者）行事的第三方。

“个人数据”与“个人可识别信息”、“个人信息”、“个人数据”或数据保护法律所定义的此类同等术语具有相同的含义。

“个人数据事件”与数据保护法律赋予的“安全事件”、“安全漏洞”或“个人数据泄露”具有相同的含义，并且应包括供应商认识到个人数据已被或可能被未经授权的人员以未经授权的方式访问、披露、更改、丢失、销毁或使用的任何情况。

“处理”指对个人数据进行的任何操作或一系列操作，无论是否通过自动方式进行，包括收集、记录、组织结构、存储、改写或更改、检索、咨询、使用、通过传输、传播进行披露或以其他方式公开方式提供、矫正或合并、限制、删除或销毁。 处理还包括向第三方转移或披露个人数据。

“特殊类别数据”是个人数据的一个子集，专门指与个人的种族或民族血统、性生活或性取向、政治观点、宗教或哲学信仰、工会会员、遗传数据、生物特征数据（眼睛颜色、发色、身高、体重）、病史或刑事定罪、犯罪或相关安全措施有关的信息。

3.2 我们的责任

根据具体情况，Entrust 可能会成为数据控制者或数据处理者。 作为数据控制者，Entrust 负责根据数据保护法律制定实践和政策。 同样重要的是，Entrust 能够证明始终遵守这些法律。 具体行动包括：

- 执行相关政策，使公司能够遵守数据保护法律，如本政策、有关文档保留和数据安全的政策以及 Entrust 隐私权声明；
- 向员工、临时员工和代表 Entrust 的第三方传达数据保护要求并进行相关培训；
- 调查未遵守 Entrust 数据保护政策的案例，并采取适当的补救措施和/或纪律处分；
- 调查、补救并在某些情况下通报个人数据事件；
- 需要进行新类型的数据处理活动时，开展数据处理影响评估；
- 定期对 Entrust 数据保护政策和程序进行内部审计；以及
- 从新产品设计之初便考虑数据保护。

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都必须：

- 以公正、合法、透明的方式进行处理；
- 只能出于特定、明确且合法的目的进行处理；
- 与 数据处理的必要合法目的相关，且仅限于该目的；
- 准确且保持最新，在合理可能的情况下，确保及时删除或纠正不准确的个人数据；
- 保存时间不得超过实现数据收集目的所需的时间；以及
- 处理方式必须确保适当的个人数据安全性，包括防止未经授权或非法处理、意外丢失、销毁或损坏。

3.4 处理个人资料的法律依据

公司只能在数据保护法律允许的情况下处理个人数据。 以下是 Entrust 处理个人数据的依据：

需要进行处理:

- 为履行数据主体为当事人的合同，或者为在订立合同前应数据主体的要求采取某些措施;
- 为遵守 Entrust 应遵守的法律义务；和/或
- 为实现 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这些利益之上。

除上述依据外，如果数据主体同意出于一个或多个特定目的处理其个人数据，Entrust 也可以处理个人数据，但前提是数据主体在知情的情况下具有针对性地自由给予该同意，并且明确表明了数据主体的意愿。 如果 Entrust 利用数据主体的同意作为处理的依据，则数据主体有权出于任何理由随时撤回该同意。

有时 Entrust 也可能需要处理员工或临时员工的特殊类别的个人数据（例如，安全雇用惯例要求的情况下）。 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 将确保满足以下条件（若适用）：

- 数据主体明确同意出于一个或多个特定目的处理其特殊类别的个人数据;
- 履行雇用法律、社会保障法律或社会保护法律或劳资谈判合同规定的义务而需要进行处理;
- 出于预防或职业医学的目的，或为评估员工的工作能力而需要进行处理;
- 为保护数据主体的切身利益，或者数据主体在实际或法律上无法给予同意的其他人员的切身利益而需要进行处理;
- 处理与数据主体公开的个人数据相关；和/或
- 发起或捍卫法律主张而需要进行处理。

3.5 数据记录管理

Entrust 保留有公司所收集的个人数据类型以及收集这些数据的原因的集中记录。Entrust 只会出于集中记录所规定的特定目的或数据保护法律特别许可的任何其他目的处理个人数据。Entrust 将在首次收集数据时（若不可行，则在首次收集后尽快）将这些目的告知数据主体。

Entrust 只会在提供给数据主体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必要的个人数据以外的数据。公司已采取适当的技术和组织措施，确保已删除或销毁不再需要的个人数据。

本公司还采取了合理措施，确保所持有的个人数据均准确且最新。Entrust 希望收集时以收集之后每隔一段时间检查任何个人数据的准确性。 公司将采取一切合理措施删除、销毁或修改不准确或过时的数据，不会无故拖延，并且在任何情况下均不迟于数据主体提出要求后的一个月内（或者如果有特殊原因无法在一个月内完成，则不迟于三个月）。

3.6 删除或销毁个人数据

当不再需要保留个人数据时，必须将包含个人数据的纸质记录粉碎并安全处理。 包含个人数据的纸质记录不得以任何其他方式处理。

在删除电子版个人数据时，应采取一切可能的措施，使有关数据再也无法使用。 如果无法彻底删除个人数据，则必须采取合理措施，确保尽最大可能删除数据。

IT 负责销毁或清除包含个人数据的电子设备（例如笔记本电脑、台式电脑、公司所有的移动设备和 BYOD 设备上的工作数据）。

3.7 信息安全

公司在处理个人数据时，会采取合理措施确保数据安全，并防止未经授权或非法处理、意外丢失、销毁或损坏。Entrust 采取的具体方式包括：

- 在可行的情况下采取适当方式加密个人数据；
- 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、可用性和恢复能力；
- 确保在发生物理或技术事件时，及时恢复个人数据的访问；以及
- 促进对技术和组织措施的有效性进行测试、评估和评价，以确保数据安全。

评估安全性的适当级别时，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所处理的个人数据的风险。

如果 Entrust 通过第三方代表其处理个人数据，则该方应根据书面指示进行处理、承担保密责任，并有义务采取适当的技术和组织措施，以确保数据安全。 个人数据不得与 Entrust 或授权第三方以外的任何人共享。

如果办公桌和橱柜中保管有任何类型的个人数据或机密信息，则应将其上锁。 数据用户应确保个人显示器/屏幕不会向旁人显示个人数据或机密信息，并且在计算机/平板电脑无人看管时，注销账号或锁定。

3.8 报告个人数据事件

个人数据事件可通过多种形式发生，包括：

- 包含个人数据的移动设备或硬拷贝文件丢失（例如，将设备意外遗留在公共交通工具上）；
- 包含个人数据的移动设备或硬拷贝文件失窃（例如，在车上或家中失窃）；
- 人为错误（例如，员工意外向非本意的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，打开包含勒索软件或其他恶意软件的未知第三方发送的电子邮件附件）；

- 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 办公室或系统的保护区域）；
- 不可预见的情况，如火灾或洪水；或
- 第三方通过欺骗手段从 Entrust 处获得信息。

可能发生个人数据事件的迹象包括：

- 异常的登录和/或过度的系统活动，特别是与活动用户账户有关的情况；
- 异常的远程访问活动；
- Entrust 的工作环境中存在可见或可访问的欺骗无线 (Wi-Fi) 网络；
- 设备故障；以及
- 连接到或安装在 Entrust 系统上的硬件或软件密钥记录器。

如有员工发现或有任何理由怀疑已发生或即将发生个人数据事件，则必须立即通过电子邮件 SOC@entrust.com 联系 Entrust 安全运营中心，并通过电子邮件 privacy@entrust.com 联系合规总监。

3.9 个人数据事件响应计划

如果实际发生或即将发生个人数据事件，Entrust 会迅速采取行动，将事件影响降到最低，并根据法律要求报告事件。在大部分情况下，响应措施包括：

- 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，阻止事件继续或再次发生，并减少对受影响数据主体的损害；
- 评估是否有义务通知其他方（如国家数据保护机构、受影响的数据主体），并予以通知。 如果有义务通知数据保护机构，通常必须在公司（包括其任何员工）意识到发生该事件后 72 小时内进行报告；以及
- 记录与个人数据事件有关的信息及所采取的响应措施，包括用于解释通知或不通知决定的文件。

3.10 国际数据传输和向第三方传输

根据 GDPR，如果欧洲经济区（“EEA”）以外的国家/地区具有足够的保护水平，或者如果 Entrust 已采取适当措施确保数据保护，则 Entrust 可向这些国家/地区传输个人数据。

Entrust 集团旗下公司（即所有公司实体和子公司）必须签订集团内数据传输协议，以确保 Entrust 集团内部在 EEA 以外的个人数据传输得到适当保护。

对于 Entrust 集团外部为 Entrust 或代表其处理个人数据的公司，如果 Entrust 为其承担了数据控制者或数据处理者的职责，则其必须与 Entrust 签订数据处理协议，以确保针对 EEA 以外的个人数据传输提供

适当的保护措施。该协议包含的条款旨在确保第三方采取了适当的技术和组织措施，以遵守 GDPR 并确保保护数据主体的权利。

Entrust 向 EEA 以外的国家/地区传输个人数据的情况可能包括：

- 数据主体在 Entrust 告知其与此类传输有关的任何潜在风险（例如，该国家/地区缺乏等效的保护措施）后，仍明确同意该拟议的传输；
- 为履行数据主体为当事人的合同，或者为在订立合同前应数据主体的要求采取某些措施而需要进行传输；
- 为保护数据主体的切身利益，或者数据主体在实际或法律上无法给予同意的其他人员的切身利益而需要进行传输；或
- 发起或捍卫法律主张而需要进行传输。

对于 EEA 以外的每次数据传输，Entrust 都将依据欧盟委员会制定的标准合同条款进行处理（2001/497/EC、2004/915/EC 和 2010/87/EU）。请注意，如果在加拿大以外传输个人数据，也需签订数据传输协议。

3.11 通知数据主体

Entrust 需要向数据主体提供与其个人数据处理有关的信息。 这些信息包含在公司隐私声明（在 www.entrust.com 上公开发布）和员工隐私声明（在 Entrust 内部网站上发布）中。 这两份声明提供以下信息：

- Entrust 处理的个人数据类型；
- 处理个人数据的目的和法律依据；
- 个人数据在处理过程中是否会向任何第三方披露；
- 个人数据是否会传输到 EEA 和加拿大以外地区，如果是，将采取哪些保护措施；
- 个人数据的处理期限是多久，如果尚无法确定，公司将采用何种标准来确定处理期限；
- 数据主体如何获取 Entrust 持有的其个人数据副本；
- 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对个人数据进行处理，则数据主体未能提供数据或拒绝处理数据可能产生的后果；以及
- 是否存在任何自动决策过程及其详细信息（如适用）。

如果 Entrust 从第三方接收与数据主体有关的个人数据，则公司还将向数据主体提供以下信息：

- 从第三方接收的个人数据类型；以及
- 数据来源以及数据是否来自公开可访问的来源（例如，公开可访问的网站）。

3.12 从设计着手保护隐私和数据保护影响评估

数据保护法律要求 Entrust 在新产品开发阶段便考虑到数据保护。 为履行这一义务，Entrust 必须采取措施以确保数据保护成为设计过程中的一部分，并尽可能减少个人数据的收集。

在某些情况下（即，处理个人数据会给个人权利和自由带来高风险时），Entrust 可能需要对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律以及公司将如何减轻对个人隐私带来的潜在风险。 如果您认为需要进行数据保护影响评估，请通过 privacy@entrust.com 联系合规总监。

3.13 数据主体权利

如果 Entrust 处理了数据主体的个人数据，根据数据保护法律，数据主体可能享有以下权利：

- 要求提供与持有的其个人数据有关的信息；
- 如果 Entrust 认定其个人数据实际上不准确或不完整，对与其有关的任何不准确的个人数据进行更正并补完不完整的个人数据；
- 拒绝 Entrust 出于公司自身的合法利益处理其个人数据。 如果公司的合法利益凌驾于数据主体的合法利益，或者如果 Entrust 需要通过处理个人数据来发起或捍卫法律主张，则即使数据主体拒绝，Entrust 依然可以继续处理个人数据；
- 要求 Entrust 销毁与数据主体有关的个人数据。 如果出于处理个人数据的目的仍需要使用个人数据，且 Entrust 具有合法理由继续处理个人数据，则公司有权拒绝该请求；
- 要求 Entrust 对其个人数据的处理限制在仅存储。 只有在个人数据的准确性受到质疑且未经核实的情况下；Entrust 不再需要该个人数据，但数据主体需要用以发起或捍卫法律主张的情况下；数据主体拒绝处理其个人数据的情况下；Entrust 正在确定其合法利益是否凌驾于数据主体利益或处理是否非法的情况下，方可提出该要求。

如果数据主体行使了上述权利，且 Entrust 已向第三方披露了相关个人数据，则公司应尽最大努力确保第三方也遵守数据主体的意愿。

3.14 数据主体访问请求

如果数据主体希望请求与 Entrust 持有的其个人数据有关的信息，可以通过 https://www.entrust.com/data-privacy-management 提交数据主体访问请求 (DSAR)。 如果员工直接收到该请求（无论是口头或书面形式），请立即将请求的详细信息转发至 privacy@entrust.com 。

3.15 培训

Entrust 为其员工和临时员工提供有关数据保护责任的培训。此类培训将在入职时和入职后定期进行。

3.16 数据保护官

Entrust 指定的 GDPR 代表是高级 公司法律顾问（英国）Anjali Doherty。Entrust Deutschland GmbH 指定的数据保护官是 Kill & Wolff GmbH 律师事务所。Entrust Corporation 没有指定的数据保护官。数据隐私合规计划由合规总监 Jenny Carmichael 负责监督，其办公地点位于美国明尼苏达州沙科皮的 Entrust 总部。

4 合规性

所有员工和临时员工均应遵守本政策。此外，所有业务部门必须确保已制定适当的当地标准和程序，以遵守本政策和其司法管辖区内适用的数据隐私法。违反本政策将受到严肃处理，并且可能导致纪律处分，情节严重者将遭到解雇。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 所有者和审查

此政策归首席法律和合规官所有。本政策应每年审查一次。本文件的更改应符合 ISMS 文件和记录控制标准。

6.1 联系方式

有关本政策的疑问或有关个人数据处理的投诉应通过 privacy@entrust.com 发送至合规总监。