elastic

使用 Elastic 支持全球隐私法律的合规性

执行摘要

要在现代数字世界中成功运营，组织正在关注数据，特别是其在 AI 中的作用。为此，一系列隐私法律和法规的涌现正在重塑全球商业格局。紧跟这些监管动态不仅是为了降低和减轻风险；这还是一个关键且强大的市场差异化因素，遵守迅速变化的法律和监管隐私环境还能提升客户信任度、推动财务增长，并增强运营弹性。

本白皮书介绍了数据隐私法的基本概念，并展示了组织如何部署 Elastic 的强大平台，不仅满足适用的个人数据要求，还能以快速、高效且自信的方式将其付诸实践。我们将概述六项广泛适用于全球数据隐私法规的基础隐私原则，并将这些原则与 Elastic 的平台解决方案相匹配，帮助组织将数据隐私从合规义务转化为竞争优势。

请注意：本白皮书仅供参考，不构成法律建议。请咨询您自己的法律顾问以获取法律建议。

背景和全球隐私法入门

全球隐私法为收集个人数据的组织带来了日益复杂的挑战。个人数据被广泛认为是世界上最有价值的商品之一，遵守隐私法可以成为企业重要的业务驱动力，而不遵守隐私法可能会严重阻碍公司的发展。

随着组织收集越来越多的个人数据，找到一种可扩展的解决方案来管理和保护这些数据变得愈发重要，这对于在日益注重隐私的世界中展现责任担当并树立值得信赖的供应商形象变得愈发关键。

虽然各种隐私法之间存在差异，但许多隐私法都有一些共同的基本原则。

主要的隐私法包括：

- 欧盟的《通用数据保护条例》(“GDPR”) 及其英国类似法规
- 美国各州的隐私法，例如《加州消费者隐私法》(“CCPA”)
- 巴西通用数据保护法（“LGPD”）
- 加拿大《个人信息保护与电子文件法》(“PIPEDA”)
- 日本《个人信息保护法》（“APPI”）

Elastic 平台提供的灵活性和扩展使组织能够驾驭并管理这些多样且复杂的法律要求的合规性。

个人数据

“个人数据”这一概念仅限于明显标识符（如全名、电子邮件地址、政府标识符和电话号码）的时代已经一去不复返。如今，世界各地的隐私法对个人数据的定义十分宽泛，涵盖了任何能够与特定设备或个人相关联的信息。

一个很好的经验法则是，如果信息能与个人的唯一标识符相关联，那么隐私法很可能适用。随着智能手机、物联网设备和其他计算设备在日常生活中无处不在，各行业组织所收集的个人数据量急剧增加，这就对能够让组织自信地管理这些数据处理的产品和服务产生了迫切且不可否认的需求。

控制器和处理器

世界各地的隐私法通常会根据组织在处理个人数据时是作为“控制者”还是“处理者”，对其施加不同但往往相互重叠的义务。

- **控制者**（根据 CCPA，也称为“企业”）控制着处理个人数据的目的和方式。他们是能够独立决定收集哪些个人数据以及如何处理这些数据的实体。
- **处理器**（在《加州消费者隐私法》（CCPA）下也称为“服务提供商”）为上游控制器（或有时是另一个处理器）提供服务，并且只允许严格按照控制器的指示处理个人数据，以便为控制器提供服务。

虽然控制者和处理者的义务不同，但每个角色都需要了解所处理的个人数据类型，并能够以有针对性、可扩展且高效的方式找到个人数据，以确保合规性。

全球大多数隐私法还赋予个人对其数据行使某些权利，例如访问、删除和更正。在相对较短的响应时间内，使用像 Elastic 这样的平台来高效筛选非结构化和结构化数据集，不仅有助于简化合规性，还能降低监管调查和民事诉讼的风险。

基本隐私原则

全球的隐私法通常以基本隐私原则为基础。从总体来看，这些内容包括：

1

通知

隐私法规定，组织必须提供其隐私做法的准确且最新的通知。

2

隐私设计

隐私法规定，组织必须考虑其做法可能对隐私权和个人利益产生的影响，并在设计产品时遵守这些法律。

3

权利

隐私法赋予个人对其个人数据的某些权利，其中可能包括访问、删除和更正其数据的权利。

4

数据最小化

隐私法要求组织尽量减少数据（即仅收集和处理为业务目的所必需的个人数据），并规定保留期限和删除策略，以确保组织不会保留不必要的数据。

5

安全性

隐私法规定了保护个人数据的某些安全标准。

6

违规通知

隐私和安全法律对发生影响个人数据的安全事件或数据泄露的组织施加了一系列义务。

不合规的代价

不遵守隐私法律可能会导致高额罚款、律师费用和声誉受损。GDPR 和 CCPA 等框架下的监管处罚可能严重到足以对公司的盈利产生实质性影响，而民事诉讼当事人也可能对侵犯隐私的行为提出索赔，包括数据泄露后的集体诉讼。

根据 IBM Security 和 Ponemon Institute 的一份报告，2024 年的数据泄露的平均成本为 488 万美元，比前一年增长了 10%。AON 的《网络风险报告》发现，2024 年 56 起备受关注的网络事件导致受影响组织的股价平均下跌 27%。显然，这种声誉损害同样会不可逆转地影响组织的竞争优势。在这种情况下，合规性已不仅仅是一项开支，更是一项战略投资。

使用 Elastic 满足您的数据保护合规需求

Elastic 通过开放且灵活的企业解决方案，帮助组织以前所未有的速度找到重要的相关答案。要在全球范围内遵守隐私法，就必须了解您的整个数据生态系统：个人数据的存储位置、移动方式以及数据的其他处理方式。这正是 Elasticsearch 平台的优势所在，它简化并自动化这些流程，从而实现无缝合规。下面，我们将根据上述六项基本隐私原则概述 Elastic 的价值。

通知

Elastic 的数据映射功能使组织能够了解整个组织服务器及更广泛范围内个人数据的范围和类型。

通知是隐私法的核心基本原则。个人有权了解组织收集其个人数据的类型、收集目的以及向其他方披露其数据的情况。数据隐私法通常要求组织提供全面的隐私政策（例如 Elastic 自己的隐私声明），并在Elastic 信任中心解释这些概念。

为遵守这一通知原则，组织必须了解其收集的个人数据的范围。这需要开展强有力的数据映射工作，这是一个系统化的过程，用于识别和记录组织内的所有个人数据流。

如果没有可扩展性解决方案，组织往往只能依赖过时的电子表格、对数据清单调查的响应，以及与各个业务部门的随意访谈来识别所收集的个人数据以及这些数据在组织内部和外部的流动情况。

在最好的情况下，记录可能在某一时刻是准确的，但很快就会因数据驱动型经济对数据收集和处理的需求而受到影响。

Elastic 可以帮助组织获取关键见解，以改进其数据映射流程。如果组织不了解所收集的个人数据类型、数据位置及披露对象，组织就无法确认其是否遵守隐私法。通过将有关数据流的信息索引到 Elastic，其强大的全文本搜索功能能够快速识别依赖于个人数据的应用程序、表格、查询或报告。

使用 Elastic 简化数据映射还有助于组织遵守隐私法的合同义务，因为已识别的数据流将决定组织应与哪些其他方签订数据保护附录、数据传输机制或其他专门针对个人数据保护的协议。同样，当今的供应链可能会延伸到数百甚至数千个供应商和分包商。通过对数千份协议进行索引并立即执行全文本搜索的能力，也有助于生成供应商状态报告，更重要的是，能够实现积极主动的供应商管理计划。

隐私设计

组织可以使用 Elastic 来增强隐私设计，包括构建数据最小化原则。

如果组织正在考虑将 Elastic 用作个人数据的数据存储，那么 Elastic 的中央协调软件 Elastic Cloud Enterprise (“ECE”) 的功能可以让组织从一开始就步入正轨。通过设计保护数据的原则是指将个人数据视为一种宝贵的资产，通过限制访问、维护准确性、实施适当的数据安全控制以及限制保留期限来保护个人数据。

与传统的单一大型数据存储和大量复杂的重叠数据访问控制（允许不同的项目仅访问特定的数据）的数据架构不同，Elastic 允许用户为每个项目实例化新的 Elasticsearch 集群，并且仅在该集群中包含与该项目相关的数据。

这种分布式架构实现了个人数据的最小化——这是另一个核心隐私原则。例如，客户可以使用 Elastic 将数据分类到存储层级，利用 Elastic 支持的访问日志信息帮助企业识别未使用的数据，从而指导数据保留政策和实践。

Elastic 还能让组织了解何时以及如何执行数据隐私影响评估 (“DPIA”)。根据 GDPR 和类似的隐私法规，DPIA 是一项有时强制要求进行的评估，用于确保您以负责任的方式处理个人数据，并最大限度地减少对个人的潜在伤害。了解数据的存储位置、处理方式以及流向可简化 DPIA 的完成过程，而传统上，完成此类评估往往需要跨业务部门的多职能支持，以了解个人数据的使用情况。而 DPIA 既能体现基础合规性，又能使组织能够将个人数据的处理限制在全球隐私法律授权的范围内。

数据主体权利

组织可以使用 Elastic 来识别相关的个人数据，评估数据主体权利的适用性，并履行数据主体的请求。

全球隐私法让个人可以选择如何处理其个人数据。这通常包括访问、删除和更正个人数据的权利，以及反对某些类型的个人数据处理的权利。Elastic 的数据映射功能是组织处理数据主体请求的核心基础。

- **访问权限：**Elasticsearch 允许组织在数据存储中进行搜索，以识别整个组织中的个人数据，包括识别依赖于个人数据的表格、查询、报告或应用程序。组织还可以利用 Elastic 来支持终端用户搜索功能，以便终端用户能够搜索其用户数据。为终端用户提供强大的搜索功能可减少客户支持需求，因为终端用户可以使用自助工具来识别和导出其数据。如果自助工具无法满足需求，Elastic 允许组织快速搜索其自身的数据存储，以满足数据主体的访问请求。

- **删除：**组织使用 Elastic 识别个人数据后，可以进一步使用 Elastic 转换这些数据，包括为符合删除例外情况的数据添加保留标签、永久删除数据，以及使用隐私法可能允许的其他删除技术，包括对个人数据进行匿名化和某些类型的假名化处理。使用 Elastic 快速转换个人数据，且无需耗费高昂的工程成本，有助于组织保持合规性、避免监管审查，并在符合全球隐私法的前提下维护数据的可用性。

- **更正：**同样，隐私法通常允许个人请求更正其个人数据。Elastic 可以隔离有关个人的个人数据，使组织能够专注于处理请求——而不是查找数据。

- **限制：**一些隐私法（如 GDPR 及其英国类似法规）还包含反对权或请求限制处理个人数据的权利。组织可以使用 Elastic 的数据映射和数据分类功能，快速确定如何回应此类请求，并相应地限制访问和使用权限，从而节省宝贵时间，使合规团队能够在这些法律规定的较短时限内做出回应。

数据最小化

正如*"隐私设计"*部分中所述，Elastic 为企业业务提供数据最小化功能。数据最小化原则要求组织在收集、处理和限制保留个人数据时，仅保留实现组织授权处理目的所必需的信息。

例如，最大限度地减少个人数据处理以履行这一义务的方法之一是**假名化**（即用占位符值替换数据中的个人标识符）或**匿名化**（即完全移除数据中的个人标识符，从而无法再识别个人身份）。了解一家欧洲领先的航空公司如何使用 Elastic 摄取管道在存储敏感数据前对其进行模糊处理。通过使用 Logstash（Elastic 中可用的集成工具，可从众多来源摄取数据以促进此类数据的转换，包括匿名化和假名化），可以实现这样的结果，从而推进数据最小化目标并降低数据安全风险。

使用 Elastic 进行数据映射和审计，还能让组织更深入地分析其保留的个人数据的使用情况，从而更有效地调整数据保留期限和策略。

安全和漏洞通知

有关 Elastic 如何帮助组织保护个人数据安全并在发生数据泄露时迅速响应的更多信息，请参阅我们的《安全白皮书》。

结论

数据隐私不仅是一项法规要求，也是企业的当务之急。面对巨额罚款、业务中断、声誉受损和客户信任危机，组织需要一种可靠且可扩展的方式来映射、分类、管理、转换、分析和删除其数据。Elastic 简化了这一流程的每一个步骤，为组织提供满足合规要求和赢得客户信任所需的可扩展能力。

