Elastic 数据传输影响评估

墨西哥

最后修订：2025 年 10 月

Elastic 数据传输与评估框架介绍

Elastic 产品与服务

Elastic 提供一整套 Elasticsearch、Observability 和 Security 产品及相关功能，旨在帮助客户获得实时见解并实现强大的数据管理能力。

当客户在 Elastic Cloud 部署 Elastic 产品和功能，或使用 Elastic 的支持服务和/或咨询服务（以下简称“Elastic 产品与服务”）时，Elastic 可能会作为处理者代表客户处理个人数据（以下简称“客户个人数据”），这些服务的个人数据处理范围各不相同。

Elastic Cloud 提供了一个托管平台，供客户在 Amazon Web Services、Microsoft Azure 和 Google Cloud 上部署 Elastic 的搜索、Observability 和 Security 解决方案。您可以从众多全球选项中选择您偏好的数据托管区域，包括欧洲经济区 (EEA) 内的众多地点。默认情况下，备份存储在与您的部署相同的区域。尽管您可以控制数据驻留的位置，但为了提供平台管理、技术运维及客户支持等必要服务，Elastic 的内部人员及分包处理方可能仍需从 EEA 境外对您的数据进行有限访问。

支持服务为 Elastic 产品的用户提供全方位的协助，涵盖从初始数据摄取到扩展部署和获得有意义的见解等各个方面。在涉及客户个人数据时，Elastic 在提供支持服务期间的处理活动受到严格限制。支持专员主要与 Elastic Cloud 的管理层交互，从而最大限度地减少对存储在索引中的客户数据内容的直接访问。如果遇到特殊问题，需要直接访问客户内容或客户数据索引（其中可能包括涉及的个人数据，例如用于分析堆转储），则需事先获得客户批准。这些流程受严格控制，可供审计，且遵守公认的合规标准。

咨询服务提供以结果为导向的指导，帮助组织优化 Elastic Stack 的使用，缩短项目周期，并实现具体的业务目标。这些服务在全球范围内提供，包含灵活的虚拟交付选项。与支持服务相似，提供咨询服务的过程可能涉及处理必要的客户个人数据，以协助完成约定的咨询服务交付。

Elastic 的个人数据处理

在向客户提供服务的过程中，Elastic 扮演着数据处理者的角色。所处理的客户个人数据的最终性质和类别由 Elastic 客户自行决定和控制。Elastic 不会主动监测客户导入其产品/服务中的具体数据。

以下表格总结了 Elastic 各项产品与服务对客户个人数据的处理情况。

Elastic 产品与服务	*主要处理目的*	*处理的个人数据的性质*	*数据主体类别*	*托管/处理地点控制*
Elastic Cloud	实时见解、搜索、可观测性、安全性、分析、平台管理、技术运维	客户个人数据（内容由客户确定，不受 Elastic 监测）、用于平台管理的有限运营数据（例如使用日志、在线标识符、电子通信、网络活动数据）。	客户管理员、终端用户、客户的客户/合作伙伴的员工	客户可选择偏好的数据托管区域（可选择 EEA 选项），并在同一区域进行备份。某些处理活动（平台管理、技术运维、支持）可能涉及从 EEA 外部进行有限访问。
支持服务	提供全面协助、故障排除和技术指导	对客户个人数据的访问权限受到高度限制（主要限于管理层面的交互）。只有在客户批准后，才能直接访问客户内容（例如堆转储）。	客户管理员、终端用户	可能涉及 Elastic 和子处理者从 EEA 以外的地点进行访问。
咨询服务	结果导向咨询、项目简化，利用 Elastic Stack 实现业务成果	为协助提供服务所需的客户个人数据。	客户管理员、终端用户	可能涉及 Elastic 和子处理者从 EEA 以外的地点进行访问。

国际数据传输的法律依据：标准合同条款 (SCC)

Elastic 的国际数据传输框架稳固建立在标准合同条款 (SCC) 的使用之上。这一机制既适用于直接传输（即数据从客户流向 Elastic），也适用于后续传输（即数据从 Elastic 流向其内部和外部子处理者），以直接符合欧盟法院 (CJEU) 在“Schrems II”裁决中提出的要求。2020 年 7 月 16 日发布的“Schrems II”裁决宣布《欧盟-美国隐私盾协议》无效，但同时重申了 SCC 作为个人数据从欧洲经济区 (EEA) 传输至第三国的合法工具的有效性。不过，欧盟法院的裁决还要求数据导入方和导出方对数据传输进行详细的逐案评估，并在必要时实施额外保障措施，以确保个人数据保持“实质等同”于 EEA 内保障的保护水平。

本评估对以下所列适用国家/地区的数据传输相关法律及实践层面进行了全面审查。我们分析了相关政府数据访问立法，评估了标准合同条款 (SCC) 的有效性，并详细介绍了 Elastic 为降低风险所采取的具体措施。

墨西哥数据传输影响评估

本节详细评估了向墨西哥进行数据传输的法律与实操环境，分析了适用的政府访问数据立法、标准合同条款 (SCC) 的有效性，以及 Elastic 采取的具体风险缓解措施。

适用的政府访问法律法规及监控范围

墨西哥的数据保护框架的特点是拥有一部与国际标准紧密接轨的全面法律，且没有针对大规模监视的明确立法。

- **《保护私有主体持有的个人数据联邦法》(FDPL)：**这是墨西哥自 2010 年起生效的全面数据保护法律。它以欧盟第 95/46/EC 号指令为蓝本，拥有与《通用数据保护条例》相似的原则，包括知情同意、目的限制和比例原则。

- **墨西哥宪法：**宪法确立了个人数据保护的基本权利，包括访问、更正、取消和对处理提出异议的权利。

- **国家数据保护局：**自 2025 年 3 月 21 日起，反腐败与良政部负责监督并强制执行数据保护法律的合规情况。

- **数据披露法（大规模监视之外）：**在刑事法律、选举法、数据保护、合规、金融和银行等领域，政府当局和法院可以要求访问个人数据，以此作为诉讼或调查的一部分。访问请求必须“有充分依据和理由”，并由已启动的程序支持，且仅以侵入性最小的方式获取必要数据。如果是出于公共利益、司法行政或司法程序的需要或法律要求，《保护私有主体持有的个人数据联邦法》允许在未经同意的情况下传输数据。

- **大规模监视法：**墨西哥没有关于大规模监视的法律或实践。
- **数据导入者的范围：**Elastic 子公司在墨西哥进行的处理活动受当地隐私法律法规的约束。

传输工具有效性评估与法律挑战

由于墨西哥拥有强大的法律框架，并且明确没有大规模监视法律，因此标准合同条款在墨西哥的有效性被评估为高度有效，这使其成为了一个风险较低的司法管辖区。墨西哥的法律框架与《通用数据保护条例》的原则高度一致。《保护私有主体持有的个人数据联邦法》内容全面，保障基本权利，维护法治，其执行目前由反腐败与良政部监督。墨西哥是《108 号公约》的缔约国，并积极寻求欧盟的充分性认定，这表明了其致力于达成高数据保护标准的决心。明确没有大规模监视立法是一个重要的利好因素，直接解决了 Schrems II 裁决的主要关切。

此外，个人有权对侵犯其权利的当局提起“宪法保护令”诉讼，这是一项受宪法保障的有效补救措施。公司还可以在法庭上对访问请求提出挑战。重要的是，公共机构访问个人数据事先会告知公司，公司一般*不*受限制，可以将访问请求告知任何人。

墨西哥的法律框架——尤其是《保护私有主体持有的个人数据联邦法》以及明确没有大规模监视法——使其成为了数据传输的低风险司法管辖区。

Elastic 的具体保障措施和数据保护缓解措施

Elastic 对数据隐私和安全的承诺建立在一套全面且分层的技术、组织和合同保障之上。这些措施的目的是在 Elastic 产品的整个生命周期内保护个人数据，并遵守 SCC 的原则，以符合 GDPR、UK GDPR 和 Swiss FDPA 的要求。

技术保障：

- **数据驻留：**Elastic Cloud 为客户提供了灵活性，客户可以从 AWS、GCP 和 Azure 的众多全球选项中选择偏好的数据托管区域，包括 EEA 内的众多位置。这样一来，客户就可以满足特定的数据驻留要求，备份会自动存储在选定的区域。
- **传输中加密和静态加密：**客户数据在传输过程中采用 TLS 1.2 进行加密，在静态存储时采用至少 AES-256 位加密算法。此外，Elastic 还维护着强大的加密密钥管理程序。
- **定期系统更新和补丁：**为了最大限度地降低漏洞风险，Elasticsearch 实例基于最新的操作系统内核进行部署，并持续应用补丁以修复常见漏洞与披露 (CVE)。
- **使用业界领先的服务提供商：**Elastic 的服务托管在由主要云服务提供商管理的数据中心，这些提供商以其最先进的技术和组织安全措施而著称，旨在保护托管数据。
- **访问控制：**Elastic 实施严格的逻辑和管理控制，将数据访问权限严格限制在授权用户范围内。这包括多因素身份验证、强密码标准以及使用 VPN 进行管理访问。严格遵守最小权限原则，确保员工仅获得其岗位所需的访问权限，并定期审查访问权限。集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，详细记录所有对客户数据及其所在系统的访问。对于支持服务，对客户个人数据的访问受到高度限制，客服专员主要与管理层互动，访问内容需要获得客户授权。
- **事件检测与响应：**Elastic 维护并持续更新先进的检测规则，用于识别可疑活动和未经授权的访问，包括文件完整性监测和账号接管指标。这些检测已集成到自动化工作流中，可以向威胁检测与响应团队发出警报，并触发即时调查。

组织保障措施：

- **信息安全管理系统 (ISMS)：**Elastic 已正式采用通过 ISO 27001、ISO 27017 和 ISO 27018 认证的 ISMS 系统。该系统是所有信息安全政策、标准和指南的基础，确保采取全面的技术和组织措施来保护数据。
- **隐私与安全设计：**这些原则贯穿于 Elastic 产品从概念设计到部署的整个过程，确保数据保护成为产品开发的基础环节。
- **公共机构索取客户信息原则：**Elastic 制定了明确的原则和程序，用于管理公共机构索取客户信息的请求。这些程序包括对请求提出挑战、通知相关方以及寻求豁免通知禁令。Elastic 从未为我们的产品创建过后门或万能钥匙，也从未允许任何政府机构不受限制或直接地访问我们的服务器。
- **供应链管理：** Elastic 对所有服务提供商进行全面的跨职能尽职调查流程，涉及安全、隐私和合规

团队。这包括审查拟共享数据的类型和风险等级，评估供应商的安全政策、措施及第三方审计情况，以及进行隐私影响评估。

- **其他内部政策：**Elastic 维持着多项内部政策，以规范个人数据的利用与访问、数据泄露管理、数据主体访问请求、数据保留以及访问控制。
- **合规框架：** Elastic Cloud 符合广泛的行业框架要求，包括 SOC 2 Type II、CSA CCM 4.0、PCI-DSS、HIPAA、Cyber Essentials+、云服务提供商 NIS2 指令、TISAX 和 FedRAMP Moderate。
- **定期测试：**定期进行网络和应用程序漏洞及渗透测试，并制定程序来记录和解决任何发现的漏洞。
- **员工培训：**所有员工在入职时及之后每年都必须完成信息安全、数据保护和隐私方面的培训。

合同保障：

- **数据处理附录 (DPA)：**Elastic 在合同层面承诺根据我们的数据保护附录实施强有力的数据保护和隐私保障措施，附录包括 SCC 及其瑞士和英国版，同时包括我们的信息安全附录。我们会定期审查和更新我们的数据处理附录，以确保其始终符合适用的数据隐私要求及最佳实践。
- **客户指令：**客户个人数据处理仅在客户指令下严格执行。
- **保密原则：**所有获授权处理客户个人数据的人员都必须遵守严格的保密协议、政策和程序。
- **控制：**客户仍可随时检索、更正或删除上传到 Elastic Cloud 的任何客户个人数据。
- **披露请求通知：**根据合同，Elastic 承诺在收到客户数据披露请求时通知客户，除非法律禁止这样做。
- **子处理方义务：**我们对子处理方的信息完全透明，他们必须遵守同样严格的标准和组织要求。我们对子处理方的行为和不作为承担与自行提供服务相同的责任。