Elastic 数据传输影响评估

阿拉伯联合酋长国

最后修订：2025 年 10 月

Elastic 数据传输和评估框架简介

Elastic 产品

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	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	以结果为导向的咨询、项目优化、通过 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、最终用户	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。

本评估针对向下方列出的适用国家/地区进行数据传输所涉及的法律与实操层面，提供了全面且详尽的审查。我们分析了相关的政府访问数据立法，评估了标准合同条款 (SCC) 的有效性，并详细介绍了 Elastic 在风险缓解方面采取的具体措施。

阿联酋数据传输影响评估

本节详细评估了向阿拉伯联合酋长国（UAE）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

阿联酋拥有一套正在不断发展完善的联邦数据保护框架，并辅以各自由贸易区的特定法律，同时在政府访问数据方面设有各项规定。

- **第 45/2021 号联邦法令《个人数据保护法》(PDPL)：**该法自 2022 年 1 月 2 日起生效，旨在通过制定收集、存储、使用和传输规则，保护阿联酋公民和居民的个人数据。它适用于在阿联酋境内运营的所有组织，包括外国公司。

- **2020 年 DIFC 第 5 号法案及 2021 年 ADGM 数据保护条例：**这些是分别适用于迪拜国际金融中心 (DIFC) 和阿布扎比全球市场 (ADGM) 自由区内的专门数据保护法律。

- **宪法保护：**阿联酋宪法保障通信自由及其保密性，并宣称住宅不可侵犯，这是隐私的基本准则。

- **同意例外 (PDPL)：**PDPL 允许在多种情况下无需明确同意即可处理数据，包括出于公共利益、数据可公开获取时、法律索赔/司法/安全程序、职业/预防医学、公共卫生、档案/统计研究、数据主体保护、招聘/社会保障义务、合同履行、遵守阿联酋法律或其他行政法规。

- **政府数据访问：**数据可提供给中央银行、其他监管机构（经中央银行批准），或根据阿联酋法院命令提供。安全和司法机构也被提及拥有访问权限。

- **数据导入者的范围：**所有在阿联酋运营的公司都必须遵守《个人数据保护法》。个人数据可能会被传输到阿联酋以外具有充分保护的司法管辖区，但截至 2025 年中期，尚无具体程序评估输入国数据保护框架的充分性。阿联酋还制定了数据本地化政策，其核心逻辑是认为本地化能够增强数据安全性，并能吸引信息通信技术领域的投资。

评估传输工具的有效性及法律挑战

由于阿联酋数据保护法尚处于萌芽阶段，且政府访问程序和透明度存在模糊性，标准合同条款的有效性目前仍难以全面评估。

有一项挑战源于阿联酋《个人数据保护法》中关于处理数据“无需征得同意”的例外条款既多又广。目前也尚不清楚是否所有的政府机构访问行为（例如安全部门的访问或出于“公共利益”的访问）都需要事先获得独立的司法授权。由于缺乏具体的流程来评估“数据输入国”保护框架的充分性，这意味着阿联酋本身尚未完全建立一套评估他国法律水平等效性的框架。

尽管存在上述挑战，近期颁布的《个人数据保护法》代表阿联酋向建立全面的联邦数据保护框架迈出了积极的一步。阿联酋数据局有权受理投诉并实施行政处罚。《个人数据保护法》还要求数据控制者和数据处理者实施技术和组织措施，包括加密和假名化处理。

Elastic 的特定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。

技术保障措施：

- **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：

- **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 维护内部政策，治理个人数据的使用和访问、数据泄露管理、数据主体访问请求、数据留存和访问控制。
- **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，并制定既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。