

安全管控





01	简介
02	监管浪潮来袭
03	面临压力的行业
04	五步计划
05	总结



O1

简介



协作是现代企业发展的动力。跨团队、跨地区和跨组织共享数据可以推动创新、提高团队工作效率并加速业务增长。然而，这种开放性往往与数据安全和合规性要求相冲突，给企业带来了复杂的挑战。

风险极高。仅在 2024 年，欧盟境内违反《通用数据保护条例》(GDPR) 的行为就导致了 277 起罚款，总额高达 11.9 亿欧元¹。Meta 因在没有充分保障措施的情况下将欧盟用户数据传输到美国而被处以 12 亿欧元罚款² 等备受关注的案例，凸显了不合规带来的财务和声誉风险。

这一挑战的核心在于数据主权，即控制数据存储位置、访问方式以及谁有权处理数据的能力。随着欧盟、美国和全球其他地区法规的不断演变，维护主权变得越来越重要。组织必须保护其数据免遭未经授权的访问，同时遵守日益复杂的地区法律。这对于 CIO、CISO 和合规官来说是一项重大挑战，他们往往会遇到来自内部对数据保护工作的阻力。

来源：1. <https://www.enforcementtracker.com/?insights> 2. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

借助 Google Workspace 中的安全管控，组织可以将数据隔离到特定区域，并自主选择在何处处理和存储数据（例如欧盟或美国），以满足严格的法规要求。通过精细化管理控制功能，它有助于确保您的数据免遭未经授权的访问，同时支持安全、无缝的协作。

本指南提供了一个实用的路线图，可帮助您保障数据安全并积极应对合规性挑战。从评估当前环境到实施高级控制措施，您将获得应对数据主权复杂性所需的洞见和工具。



为了在协作世界中实现数据主权，组织必须：

- 01 控制数据的存储和处理位置。
- 02 确保只有获得授权的相关方才能访问。



02

监管浪潮来袭



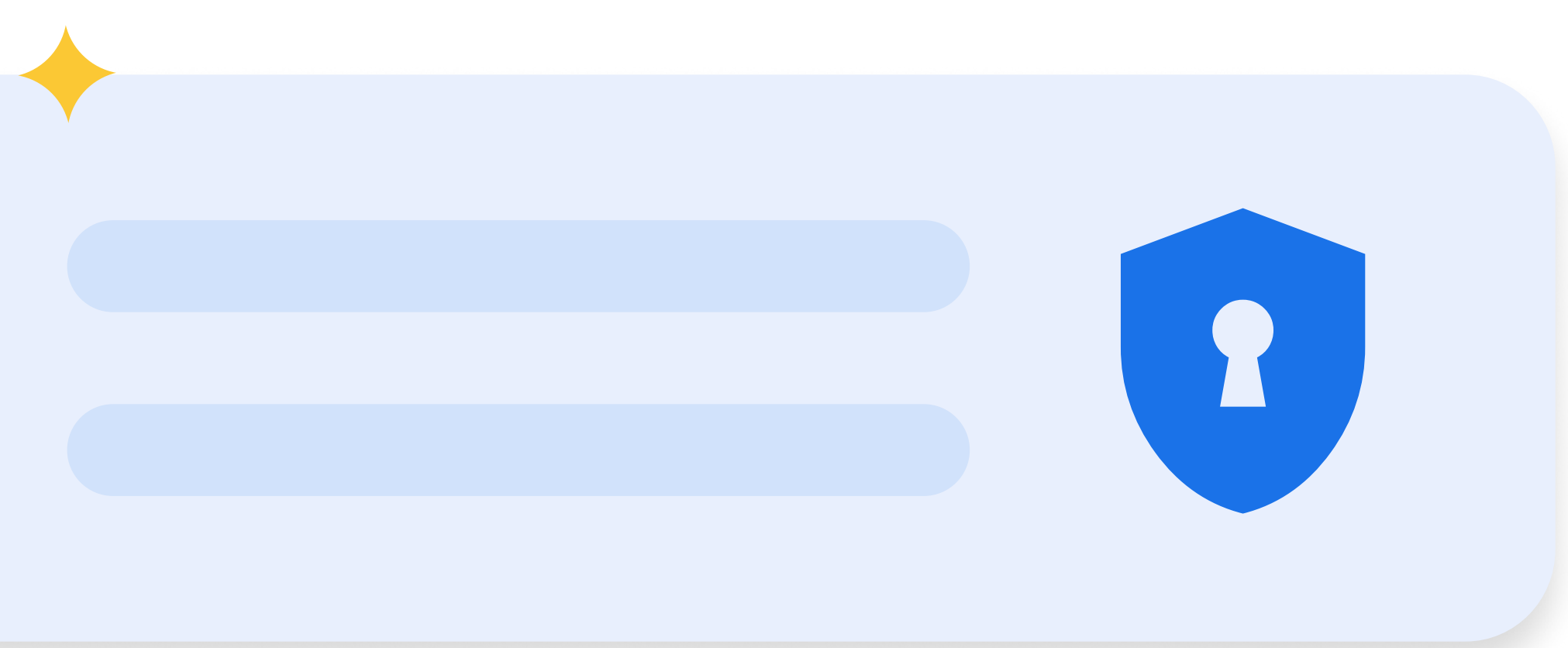
世界各国政府都在推出更严格的数据保护法律，以保障个人信息安全并确保敏感数据受本地管控。这些框架正在重塑企业管理信息的方式，为合规与创新创造新的机会，同时增加了不合规风险。





欧盟： GDPR 和《欧盟 AI 法案》

《通用数据保护条例》(GDPR) 为数据隐私保护设定了全球基准。它规定了对个人数据的存储、处理和传输方式的严格控制，尤其是在欧洲经济区 (EEA) 以外。组织必须实施适当的保障措施，例如标准合同条款或等效保护措施，以确保合规。GDPR 适用于向欧盟公民提供商品或服务或监控其行为的企业，无论这些企业位于何处。



《欧盟人工智能法案》(EU AI Act) 是全球首个 AI 法律框架，旨在监管风险并推动在欧洲可信地使用 AI。适用于在欧盟市场开发或部署 AI 的任何企业，无论这些企业位于何处。AI 系统分为四个风险级别：

不可接受的风险

凡是威胁安全和权利的 AI 应用均被禁止（例如社会评分、生物识别监控）。

高风险

在医疗保健、执法等关键领域应用的 AI 必须遵守严格的法规，包括风险评估和人工监督。

透明度风险

聊天机器人和生成式 AI 等 AI 系统必须明确披露 AI 生成的内容。

风险极小或无风险

低风险 AI（例如垃圾邮件过滤器、AI 赋能的游戏）不受限制。



美国： HIPAA、CCPA 和 CDPA

虽然美国没有统一的联邦数据隐私法，但行业和州级法规规定了重要义务：

HIPAA

适用于医疗服务提供方、保险公司及其业务伙伴，通过严格的隐私和安全措施保护患者信息。

CCPA（加利福尼亚州）

赋予消费者对其个人数据的权利，包括访问、删除或选择拒绝企业出售其个人数据的权利。适用于达到特定收入或数据门槛的企业。

CDPA（弗吉尼亚州）

与 CCPA 类似，该法律同样针对消费者隐私，但更强调数据最小化和透明度。

亚太地区： APPI 和 PIPA

- 01 日本《个人信息保护法》(APPI)：重点关注跨境数据传输，要求在处理日本公民的数据时获得同意或采用等效保护措施。
- 02 韩国《个人信息保护法》(PIPA)：实施严格要求，包括限制跨境传输，并对违规行为予以重罚。

南美洲： 巴西的《通用数据保护法》(LGPD)

巴西的《通用数据保护法》(LGPD) 与 GDPR 类似，要求在数据处理时严格征得同意，并对违规行为处以重罚。适用于处理与巴西公民相关数据的企业。



跨境复杂性

国际数据传输需要遵守多个合规框架。

不断变化的要求

随着 GDPR 和 LGPD 等法律不断演变，组织必须灵活调整以保持合规。

行业差异

法规之间常有重叠，但其适用性会因不同行业的特定风险和需求而有所不同。

各框架面临的普遍挑战

尽管存在地区差异，但企业普遍面临相同的挑战。

这些框架构成了数据主权的法律基础，但其影响在处理敏感数据的行业中最突出。请继续阅读，了解金融、医疗保健和科技等行业如何应对这些独特的挑战。



03

面临压力的行业

数据主权挑战对各行业的影响并不相同。对于处理高度敏感数据并受严格监管的行业，其影响尤为显著。

对于金融、医疗保健、政府和科技等行业，实现数据主权不仅仅是满足合规要求。其核心在于保护关键资产、与利益相关方建立信任，并确保在日益复杂的环境中实现顺畅且安全的运营。

 分享



金融： 在竞争激烈的环境中维护信任

由于客户数据的敏感性及其在全球经济中的作用，金融机构始终处于严格监管之下。《通用数据保护条例》(GDPR) 等法规要求对数据存储和访问进行精确管控，而开放银行计划则要求与第三方提供商安全地共享客户数据，以推动创新。



Shirley Franklin

主要注意事项：

跨境挑战

跨多个司法管辖区管理金融数据会引发风险，尤其是当数据在监管要求不同的区域之间流动时。

过时系统

许多银行依赖过时的基础设施，这使得实施高级加密或基于角色的访问等现代合规措施变得复杂。

声誉风险

在信任至关重要的行业中，一次数据泄露或合规失守就可能造成严重的财务和声誉损失。

通过实施精细化访问权限控制和本地化数据处理等解决方案，金融组织可以自信地满足合规标准，同时维护客户信任。



医疗保健： 在隐私保护与行业发展之间取得平衡

在医疗领域，保护患者隐私既是法律义务，也是道德责任。医疗行业需要在保护敏感医疗记录与开展挽救生命的科研合作之间保持微妙的平衡。

主要注意事项：

监管重叠

医疗服务提供方必须应对复杂的法规网络，从美国的 HIPAA 到欧盟的 GDPR，每个法规都有自己的数据存储、加密和访问标准。

跨境协作

研究机构通常需要进行国际数据共享，这使合规工作更加复杂。例如，全球临床试验中的匿名患者数据共享必须符合当地的数据主权法律。

运营中断

过时的系统和数据孤岛往往会导致效率低下，并在合规审计期间增加风险。

借助端到端加密和实时监督工具等强有力的数据保护措施，医疗机构既能满足合规要求，又能推动创新与合作。



政府： 确保公民信任和国家安全

政府机构管理着大量敏感的公民数据，从纳税记录到国家安全信息等。保护这些数据至关重要，这不仅是合规要求，更关乎公众信任和国家安全。



主要注意事项：

地缘政治风险

政府机构面临着独特的挑战，包括网络威胁和来自境外势力的压力，因此数据驻留和数据主权至关重要。

透明度与安全性

在开放性与严格数据控制之间取得平衡，对于维护公众信任至关重要。

区域法律

政府机构必须遵守相互重叠的法规，例如欧洲的 GDPR 以及要求数据本地化的地方性法规。

借助端到端加密和严格的访问权限控制等数据主权工具，公共部门组织可以保障其数据安全，同时不会影响透明度或运营效率。



科技： 在监管下推动创新

科技公司处在全球扩展与区域合规的交汇点，需处理海量跨境用户数据。对于这些组织而言，数据驻留不仅是合规性问题，对于保护知识产权和维护客户信任也至关重要。

“如果不对数据进行区域化处理，或者将数据交给其他技术提供商处理，空客公司、整个国家乃至整个欧洲都可能面临风险。这样的风险我们承担不起。”

Sebastien Aubineau，空客公司

主要注意事项：

全球覆盖，本地规则

Airbus 等公司强调了区域化数据处理的重要性，这有助于保护敏感信息并遵守主权法规。

可灵活伸缩的解决方案

科技公司必须实施既能支持全球拓展，又能确保合规的系统。

新兴风险

快速创新往往会导致不可预见的漏洞，从第三方应用集成到访问控制不足，都可能成为漏洞的来源。

借助精细化管理控制和先进安全措施，科技公司能够应对这些挑战，同时保持创新或增长动力。



04

五步计划



在通往数据主权的道路上，需要根据您的独特需求、行业和地点，采取系统化的方法。本指南概述了五个切实可行的步骤，可帮助您掌控数据环境、遵守法规并对组织的合规策略充满信心。

01

评估环境

了解数据的存储位置、哪些人可以访问，以及适用的法规。这是识别不足之处的第一步。

02

选择数据区域

实现数据存储和处理本地化，以符合监管要求，同时保持运营灵活性。

03

完善访问权限控制

调整权限，确保只有合适的人员才能访问合适的数
据，从而最大限度地降低数据暴露风险。

04

加强数据保护

通过加强安全措施和保护敏感数据，防范不断演变的网络威胁。

05

报告和监督

借助持续监控和报告功能，在不断变化的监管环境中保持合规并积极应对。



01

评估环境

每一段旅程都始于了解您所处的位置以及您想要到达的目的地。

要应对数据主权问题，首先要了解适用于您所在行业的外部法规以及数据环境的内部实际情况。这意味着要确保数据的存储、访问方式与合规要求相符，同时识别当前设置中的不足之处。



了解规则

GDPR、ISO 和 SOC 等全球框架为合规奠定了基础。但这些法规并非孤立存在，而是要求与组织的具体运营保持一致：

GDPR (欧洲)

要求数据严格驻留在欧洲经济区 (EEA) 内，除非有足够的保障措施，例如标准合同条款。对于有欧洲客户的组织，准确了解个人数据的存储和传输位置至关重要。

《欧盟 AI 法案》 (欧盟)

《欧盟人工智能法案》是欧盟制定的一项法规，旨在建立一个在欧盟境内通行的 AI 监管框架。它将 AI 系统和模型分为不同的类别，并针对每个类别规定了不同的要求。《欧盟人工智能法案》于 2024 年 8 月 2 日正式生效。

DORA (欧盟)

《数字运营弹性法案》制定了技术标准，以加强金融机构的 IT 安全。该框架由欧洲监管机构 (ESA) 制定并由欧盟委员会采纳，统一了金融部门和 ICT 第三方提供商的运营弹性规则。

SOC 合规性 (美国)

服务组织控制报告侧重于安全性、可用性和机密性等信任原则。要达到 AICPA 制定的这些标准，需要进行严格的内部审计并实现运营透明，尤其是对于美国境内的组织或与美国实体有业务往来的组织。

ISO 标准 (全球)

提供全球认可的信息安全管理框架，由国际标准化组织监管。对于在欧盟、美国和亚太地区等区域运营的跨国组织来说，这些标准对于建立一致的安全政策至关重要。



审计您的数据

下一步是内部工作：绘制数据环境图。您的数据位于何处？哪些人拥有访问权限？您目前的系统存在哪些不足？回答这些问题是制定合规策略的基础。

例如：

- 医疗服务提供方可能会发现，敏感的患者数据存储多个云服务中，加密级别各不相同。跨境数据共享以供研究进一步加剧了遵守《GDPR》（欧洲）和《HIPAA》（美国）的复杂性。
- 在这种情况下，数据审计可能会发现一些风险，例如未加密的记录或不明确的访问权限，这些风险必须加以解决，才能满足监管要求。

通过这些数据洞见与外部法规保持一致，组织可以弥合合规要求与运营现实之间的差距。





组建团队

数据主权不仅是一项技术挑战，也是一项协作挑战。组建合适的跨部门团队至关重要：

- **IT 领导者**可以规划技术基础设施，并解决加密或存储方面的不足。
- **法律团队**可以解读地区监管要求，确保合同反映合规要求。
- **业务部门**可以协助确定日常运营受到的实际影响，例如访问权限和工作流中断。

该团队应协同合作，确保您的内部流程符合 GDPR、SOC 或 ISO 等框架在各自区域的要求。

提前规划

随着法规和业务需求不断变化，组织现在采取这些措施，不仅可以满足合规要求，还可以构建支持未来增长的框架。

例如，采用 **Google Workspace 中的安全管控**等解决方案可以满足数据驻留和访问要求奠定基础，确保合规性并保持灵活性。





数据驻留和访问权限控制

02

数据驻留不仅关乎数据的存储位置，还关乎如何确保您能够控制数据的存储、访问和处理方式，同时兼顾性能、可伸缩性和合规性。

对于处理大量敏感数据的组织，Google Workspace 中的安全管控等工具可以简化合规流程，而不会中断运营。

“我们对区域内数据处理进行了广泛分析，整个过程非常顺利，避免了昂贵而复杂的第三方集成。此外，我们没有遇到任何故障或延迟，日常运营都非常顺利。”

Randstad 全球协作产品负责人
Roman Spantgar

本地数据驻留与灵活性

许多组织面临的挑战在于，如何在满足严格的数据驻留要求与保持运营敏捷性之间取得适当的平衡。例如，在全球范围内扩张的组织通常需要兼顾区域法规和性能需求。

这就形成了一个普遍的矛盾：组织如何在遵守法规的同时，避免构建会阻碍协作的孤立系统？Google Workspace 安全管控通过提供精细化灵活控制来解决这一问题，让您在保持云可伸缩性的同时，自定义数据的存储和处理位置。对于跨国企业，这意味着能够为各个团队、部门或区域设置数据驻留政策，同时不影响性能。

数据处理：超越存储

许多组织过于关注数据存储位置，却忽视了数据处理位置，而这在 GDPR 等框架中是一项关键合规因素。数据处理是指如何使用、分析或共享数据，通常需要比简单存储更严格的监督。安全管控不仅限于存储。通过实现存储和处理本地化，确保组织符合端到端数据主权要求。





应对未来监管变化

数据主权是一个不断变化的目标。政府不断完善现有法规并推出新法规，给企业带来了不确定性。依照当下规则设计的僵化系统可能难以适应未来变化。Google Workspace 中的安全管控让您能够灵活根据法规变化调整数据驻留政策。无论是跨区域迁移数据，还是完善访问控制，其目标都是确保您的主权合规态势始终能适应不断变化的监管环境。

应对美国医疗保健合规性要求

《健康保险流通与责任法案》(HIPAA) 等联邦法律为患者数据保护设定了全国性标准，但州法律增加了复杂性。加利福尼亚州的《CCPA》和弗吉尼亚州的《CDPA》等法规对数据隐私、消费者权益和保留期限设定了更严格的要求。本地化数据处理有助于医疗服务提供方从容应对这些重叠的法规要求。





03

完善访问权限控制

当数据安全存储后，下一步就是确保访问同样受到保护。通过应用最小权限原则，组织可以确保只有真正有需要的人员才能访问敏感信息。通过严格控制哪些人可以查看哪些内容，组织可以降低意外泄露、内部滥用和第三方漏洞的风险。

访问权限控制的重要性

在当今的环境中，不受限制的数据访问正带来日益增加的风险。内部权限过度会增加泄露和出错的风险，第三方访问可能会使合规性变得复杂，而 GDPR、HIPAA 等法规和其他框架要求对敏感信息的访问主体实施了更严格的监督。



如何优化访问权限

合适的工具可帮助组织实施更智能、更安全的访问政策：



零信任框架

采用“不信任任何人，验证一切”的方式，这样可确保所有用户、设备和连接都经过身份验证和授权，即使是内部用户也不例外。

访问透明度和审批

实施需要明确授权才能进行第三方访问的工作流。Google Workspace 中的访问权限审批等工具可确保支持团队仅在绝对必要时访问数据，同时提供全面的可见性和控制力。

基于角色的访问控制 (RBAC)

通过将权限与特定角色对齐，有助于最大限度地减少不必要的暴露。例如：

- 财务团队可以访问支付系统，但不能访问人力资源记录。
- 医疗保健提供方可以查看患者护理数据，但无法查看行政文件。
- 支持团队只有在获得明确批准后才能在规定时间内访问数据。

客户端加密

增加一层安全保障，确保企业自行管理加密密钥，防止云提供商访问敏感数据。



通过实施精细化访问控制，组织可以平衡安全性、合规性与协作式现代工作场所的需求。接下来，我们将探讨如何加强安全措施，进一步降低风险，确保您的组织能够应对不断演变的网络威胁。

 分享

限制访问权限不仅有助于保障安全，还能推动智能运营。

性能：

将数据存储靠近最终用户的位置可以缩短延迟时间、提高工作效率，并确保您的团队随时随地都能无缝协作。

合规：

将数据保留在区域内可以避免法律风险，并确保符合 GDPR、HIPAA 和其他不断变化的合规框架要求。

安全和数据泄露防护 (DLP)

04

在确保数据安全存储并优化访问控制后，下一个关键步骤就是保护组织免受不断演变的威胁。Google Workspace 中的安全管控提供高级客户端加密、精细化访问权限控制和强大的数据泄露防护 (DLP) 工具，确保您的数据在存储、传输和使用等各个阶段都安全无虞。





重要性

现代组织面临着日益复杂的安全挑战：

- **外部威胁：**钓鱼式攻击、恶意软件和未经授权的访问尝试变得越来越复杂。组织需要采取主动措施来保护敏感信息，防止被不法分子窃取。
- **内部风险：**权限过度、意外共享和人为错误依然是数据泄露的主要原因。收紧访问权限并嵌入技术保护措施有助于缓解这些漏洞。

员工日常使用的工具（如浏览器扩展程序、效率提升应用或第三方集成）可能会无意间引入漏洞。无论是未经验证的应用共享敏感数据、权限过度，还是恶意软件入侵，这些风险都会为您的安全状况增加一层无形的复杂性。

那么，如何保护关键数据，同时确保员工可以顺畅地使用所需的工具？

借助 Google Workspace 中的安全管控，组织可以在灵活性与安全性之间取得平衡：

- **精细化权限管理：**限制第三方工具的访问范围，确保敏感数据不被访问，并减少不必要的暴露。
- **客户端加密功能：**全方位保护数据，即使员工跨云服务协作也不例外。加密可确保未经授权的应用或服务无法访问敏感信息。
- **可见性和审批：**持续监控当前使用的工具，尽早发现潜在风险，并仅在确有必要时才批准外部访问。

通过嵌入这些控制措施，安全管控让组织能支持员工自由创新，同时将安全放在首位。工具应当提供助力，而不是成为隐患。

构建多层防御

安全管控还与零信任框架无缝集成，秉持“不信任任何人，验证一切”的理念，要求所有用户、设备和连接在访问敏感数据之前完成凭证验证。

无论是共享前加密文件，还是要求对第三方访问进行多层审批，这些技术控制都能确保安全机制始终保持主动。





数据泄露防护的重要性

数据泄露防护 (DLP) 政策在增强安全状况方面发挥着至关重要的作用。借助这些政策，您可以：

- **监控数据移动：**跟踪敏感数据在系统中的移动情况，识别并解决泄露或未经授权的共享问题。
- **设置自定义政策：**定义规则，自动阻止、提醒或标记违反合规性要求的共享数据行为。
- **保护敏感数据类别：**识别并保护特定数据类型，例如个人信息 (PII)、财务数据或知识产权。



安全通常被视为协作的障碍和额外负担。但实际上，它有助于企业自信地运营。借助安全管控的高级加密、主动式 DLP 政策和审批流程，组织可以在保护敏感数据和实现协作之间取得适当的平衡。

下一部分将探讨报告和监督如何帮助您在不断变化的监管环境中保持积极主动并遵守相关规定。



报告和监督：通过可见性增强信心

05

数据主权并不意味着控制措施落实到位就万事大吉，而是要证明这些措施确实发挥作用。报告和监督功能让组织能够监控、审计和调整其数据策略。通过持续监控加密、访问和存储，您可以确保不仅实现合规，还能长期保持合规。对于 Randstad 这样的组织，实时报告工具不仅可简化审计流程，还能确保顺畅的合规性。

“实施数据区域是我们在欧盟推进个人数据处理策略过程中具有变革性的一步。整个过程非常顺利，我们没有遇到任何运营问题”

Randstad 全球协作产品负责人 Roman Spantgar



报告就像是一个控制金字塔，这是一个分层系统，可在每一个层级建立信心：

客户端加密功能：

加密是安全的基础。但只有始终如一地实施加密，才能发挥其作用。报告工具可确认敏感数据从创建到存储全程保持端到端加密，审计记录则可验证加密密钥始终由您掌控。

情境感知访问权限：

数据访问不仅要加以控制，还应进行监控。实时报告可识别异常情况，例如异常访问位置、登录尝试失败或非工作时段的活动。这种可见性让您能够在风险演变为安全事件之前及时加以解决。

精细的访问权限控制：

监督工具可帮助您了解哪些用户何时出于何种原因访问了哪些数据。通过生成清晰的访问日志和报告，您可以识别权限过高的角色、监控临时访问（例如支持团队的临时访问），并遵守 GDPR 和 HIPAA 等框架。

本地数据存储：

对于受严格数据驻留要求约束的行业，透明度至关重要。报告工具可验证数据是否存储在指定位置（无论是在特定州还是地区），为 IT 团队和监管机构提供所需的证明。

数据区域：

想要拓展新市场？报告信息中心可清晰显示数据的存储、处理和访问位置，让组织能够根据法规变化或全球业务扩展情况来调整政策。

零信任架构：

零信任意味着从不进行假设，而是始终进行验证。报告工具会记录所有访问请求、设备和用户行为，确保数据政策得到严格落实，同时便于监控活动和检测可疑模式。



为什么可见性很重要

如果没有可靠的报告，合规工作就像是在猜谜。组织需要证明自身符合监管要求，同时保持足够的敏捷性来应对新兴威胁。

Google Workspace 中的安全管控可提供所需的监督工具，让您能够自信地监控、验证和调整数据策略。

- **简化审计：**生成符合 GDPR、HIPAA 和 SOC 2 等框架的合规报告。安全管控可简化 IT 团队和合规团队的报告流程，只需一键即可生成所有数据活动的详细可审计日志。
- **让一切尽在掌控：**实时信息中心可及早发现风险，透明的活动日志则可跟踪每项操作、审批或变更。团队可以获得所需的可见性，从而应对风险、证明治理成效并保持信任。

凭借实时数据洞见、可供审计的报告和透明的活动日志，安全管控不仅能帮助您满足合规要求，还能帮助您领先一步。借助监控、验证和调整工具，组织可以自信地展示对数据的掌控，同时降低盲点或新兴威胁带来的风险。

强大的报告功能让合规流程不再只是简单的打勾任务，而是成为一项战略优势。借助活动监控、控制验证和主动响应工具，组织可以从容应对不断变化的风险与法规，同时建立信任。





05

总结



Google Workspace 中的安全管控

通过将先进的合规工具与云的灵活性和可扩展性相结合，帮助组织以最小的投入，轻松实现数据主权。安全管控提供对数据存储、处理和访问的细粒度管控，同时帮助企业灵活应对不断变化的法规。无论是保护航空航天领域的知识产权，还是管理金融行业的敏感客户数据，安全管控都能让组织专注于协作、发展与创新。

[了解详情](#)