ACCCF / 应用知识库

02

卷

应用隐私、安全与记录在案的决策

西班牙语版 · 2026

个人数据保护与合规证据手册

清单、权利、供应商、事件、保存与可验证的删除

通过可解释、可核验的决策保护个人，而非依靠照搬的政策或无人落实的文件汇编。

本手册面向隐私负责人、法律、安全、技术、人力资源及管理团队，以及处理个人信息的供应商。手册为小型组织和复杂运营分别提供工作路径。

编辑统筹：Jocsan Laguna · 美国网络安全与计算机取证委员会

通用技术指南和开放教育材料。不构成法律意见、专家鉴定意见，也不构成未经授权访问系统的操作指导。示例和数据均为虚构；图示为编辑重构。

目录

可见页码对应 PDF 版本。Word 打开文档时可能会更新此索引；标题保留内部导航。

前言：隐私保护须体现于实际运营 4

第1章 支持决策的数据清单 4

1.1 描述处理活动，不以缩写加以掩盖 4

1.2 找出隐蔽的副本 5

第2章 目的、法律依据与最小化 6

2.1 区分看似相同的处理目的 6

2.2 检验数据是否多余 7

2.3 提供清晰易懂的信息与告知 7

第3章 保障个人权利，不设置人为障碍 8

3.1 接收、身份与适用范围 8

3.2 提供访问，同时避免泄露他人信息 8

3.3 删除并不意味着销毁一切 9

第4章 可验证的安全性 9

4.1 风险优先于控制措施目录 9

4.2 控制措施及其运行证据 10

4.3 假名化不等于匿名化 10

第5章 供应商、云与数据传输 11

5.1 使用供应商并不转移责任 11

5.2 数据流转与传输图 11

5.3 受控退出与技术依赖 12

第6章 数据泄露：遏制、研判与通知 12

6.1 初步行动：勿清除现场痕迹 12

6.2 通知决策与实用内容 13

6.3 损害、影响范围与结案 14

第7章 数据留存、删除与可携带性 14

7.1 留存期限应有依据，而非随心所欲 14

7.2 真正可用的数据可携带性 15

第8章 三个完整流程 15

8.1 人力资源：共享文件夹 15

8.2 医疗：误发到群组的消息 15

8.3 数据分析：导致个人可被识别的报告 16

附录A 隐私保护的功能等效对照 16

A.1 用于选择法律依据的表格，而非换算数字的表格 17

附录B 便于调整的现成模板 18

B.1 处理活动记录 18

B.2 数据主体申请表 18

B.3 数据泄露事件时间线 18

B.4 供应商评估 19

B.5 删除或屏蔽证明 19

附录C 术语表与输出控制 19

前言：隐私保护须体现于实际运营

隐私政策本身可能正确，但组织仍可能每天暴露并不需要的信息。合规始于文案写完之处：索取过多数据的表单、与外部人员共享的文件夹、可以下载整个数据库的供应商、无人知晓如何恢复的备份，以及只在屏幕上发生的删除。真正有用的问题不是是否存在一份文件，而是某个具体个人的信息从收集到不再需要期间究竟经历了什么。

本手册采用一个简单的工作单元：数据 → 目的 → 法律依据 → 访问 → 风险 → 证据 → 最终去向。每个环节都必须能作出具体回答，而不是泛泛而谈。如果一份记录用于证明某项销售，就要明确该目的需要哪些字段、由谁管理、保留多长时间，以及还一并收集了哪些其他信息。如果出现新的目的，仅更改文件夹名称并不够：必须重新审查合法性、向数据主体提供的信息以及访问范围。

合规证据也不是堆积截图来营造开展工作的假象。它要求保留决策的版本、支持该决策的依据来源、批准人、实施的控制措施以及验证结果。比较不同法律，不是为了照搬他国政策，而是为了找出组织需要记录的功能：最小化、安全、透明度、权利、受托处理方、事件或传输。法律依据和期限始终应结合处理所在地域、所属行业和处理日期进行审查。

> **第一项决策**
> 在购买工具或再写一份政策之前，先选择一个真实流程，用虚构数据完整走一遍。如果你无法说明哪些信息进入、为何进入、谁能查看、最终流向何处以及如何行使权利，那么这就是第一项具体工作。

第1章 支持决策的数据清单

1.1 描述处理活动，不以缩写加以掩盖

有用的数据清单不应从“客户数据库”开始，因为这一标签可能混杂销售、支持、收款、营销和人员招聘。它应从一项清晰易懂的活动开始：登记购买、处理保修、评估求职申请、发放工资、答复咨询或维护楼宇安全。对每项活动，都要记录具体目的、必要字段、涉及的人员、系统、保管人、输入渠道和预期输出去向。

分类应反映实际后果，而不只是名义上的敏感性。姓名和电话在联系名录中可能风险较低，但如果会暴露受威胁者的位置，则可能风险很高。调查案卷可能同时包含身份、健康、经济状况、通信以及无关第三方的信息。“机密”标签并不足够：必须明确谁可以使用、采取哪些控制、用于何种决策以及使用多久。具体情境可能使一组看似普通的数据组合成私密画像。

清单字段	操作问题	虚构示例
活动	具体执行什么任务？	处理在线购买设备的保修事宜。
最少必要数据	哪些字段是完成该任务所必需的，哪些是附加的？	订单、联系方式、送货地址和诊断信息；不需要工作经历。
涉及人员	涉及数据主体、第三方、未成年人还是弱势群体？	购买者、包裹收件人和指定技术人员。
数据流转	数据从何而来，又会传输给谁？	商店 → 支持平台 → 快递服务商；不对外公开。
保管与期限	由谁决定，何时不再需要？	售后负责人；期限由运营需要和可证明的义务确定。
证据	如何证明决策及其执行？	告知文本版本、角色、日志、合同和删除记录。

1.2 找出隐蔽的副本

清单必须涵盖导出文件、附件、扫描纸质文件、个人文件夹、应用程序日志、备份副本和第三方服务。官方数据库可能已受到控制，而一个 Excel 文件却通过即时通讯工具流传，既没有负责人，也没有删除日期。副本即使名为“临时”，也仍属于数据处理。应记录由谁创建、为何必要、存放何处、谁能打开，以及其用途结束后如何清除。

一次良好的信息收集访谈，不应只询问部门使用什么系统。应请一名人员用虚构信息展示完整的工作流程：请求如何到达、下载什么、转发给谁、在哪里保存备注、发生错误时如何处理，以及休假时如何交接。真实的流转图往往显现在例外情形中。密码不得写入清单；只记录访问控制机制及其负责人。

> **输出控制**
>
> 任何流程都不能以“以及其他必要数据”收尾。必须明确字段、来源、去向和理由。未知事项应标记为待调查，而不是用一个让人安心的复选框代替。



图1 从数据到最终去向。每项决策都留下依据来源和核验记录。编辑重构；不构成真实证据。

第2章 目的、法律依据与最小化

2.1 区分看似相同的处理目的

销售产品、发送广告和建立行为画像并不是同一个目的。第一项可能是维持双方关系所必需；其他目的则需要分别分析。组织如果把多个目的混在“行政和商业目的”之类的一句话中，就无法判断哪些数据确有必要，也无法确定哪些通信需要单独说明。记录中必须保留这种区分，使个人可以拒绝某项用途，而不会不当失去基本服务。

同意只是可能的法律依据之一，并非万能钥匙。还可能存在法律义务、履行某种关系、行使公共职能、维护权利或所辖法域规定的其他情形。应先确定具体规则，再选择表单。凡事都要求同意，可能会错误地把责任转嫁给个人，也会使本来已有其他依据的处理活动变得混乱。如果处理活动发生变化，应在实施前重新审查兼容性、告知内容和控制措施。

墨西哥规定了合法性、目的性、诚信、同意、质量、比例性、告知和责任原则；哥伦比亚确立了合法性、目的性、自由、质量、透明度、访问受限、安全和保密原则；厄瓜多尔则要求主动且可证明的问

责。这些原则的相似之处有助于建立方法，但每种情形和例外都必须结合适用的法律规范和行业规定来解读。[1][2][3]

2.2 检验数据是否多余

选取一个字段，在虚构示例中将其删除。如果缺少该字段仍能完成活动，就需要说明为何还要收集。判断标准不是它日后是否可能有用，而是它对当前目的是否适当且必要。通知送货可能只需电话号码；如果可以用侵扰更小的方式核验身份，就无需留存身份证件副本。进行统计分析时，或许也无须将姓名与结果一起保存。

情况	最小化决策	防止随意处置的记录
购买售后支持	订单和联系渠道，而非完整的客户档案。	经批准的字段和现行表单的截图。
身份验证	选择既能达到所需安全水平又侵扰最小的方法。	已评估的替代方案、风险和批准记录。
汇总报告	移除标识符，并检查可能导致重新识别的数据组合。	小群组测试及已应用的数据抑制。
第三方查询	将申请人的数据与其他人的数据分开。	交付版本及交付前的内容审查。
新处理目的	暂停处理，直至审查兼容性和法律依据。	请求、分析记录和注明日期的授权。

2.3 提供清晰易懂的信息与告知

隐私告知应让个人清楚了解由谁决定、为何使用其数据、与谁共享、如何行使权利以及在哪里提出疑问。冗长的文本不能代替及时的说明。应保留实际展示的版本及其背景信息：页面、日期、流程、语言和变更。网站更新后，也不得从合规记录中删除旧版本。

在阿根廷，须事先告知处理目的、接收方或接收方类别、责任方以及行使权利的可能性。在哥伦比亚，请求授权时负有清晰、明确的告知义务，并须保存履行该义务的证据。这些例子说明，证据为何必须同时涵盖文本和背景：当前 URL 无法证明个人多年前看到了什么。[4][5]

[1]墨西哥。《联邦私人持有个人数据保护法》，文本发布于 20-03-2025，修订于 14-11-2025。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和权利请求受理。现行联邦主管机关为反腐败与善治部。 官方在线来源

[2]哥伦比亚。2012 年第 1581 号法律，第 4、8、12、17–18 和 26 条：原则、权利、告知、控制方和受托处理方的义务，以及向第三国传输。 官方在线来源

[3]厄瓜多尔。《个人数据保护基本法》，26-05-2021《官方公报》第 459 号增刊。第 10、37–44 条：原则、安全措施、设计保护、风险和事件处理。 官方在线来源

[4]阿根廷。第 25.326 号法律，更新文本。第 4–6、9–10、14–16 和 25 条：数据质量、告知、安全、保密、数据主体权利，以及代表第三方提供数据处理服务。 官方在线来源

[5]哥伦比亚。2012 年第 1581 号法律，第 4、8、12、17–18 和 26 条：原则、权利、告知、控制方和受托处理方的义务，以及向第三国传输。 官方在线来源

虚构案例：索取个人档案的促销活动

一家商家要求提供官方身份证件、婚姻状况和住址，才能发放电子优惠券。分析后形成的版本只要求提供电子邮箱，单独征得广告营销同意，不再留存身份证件副本。应记录停止收集哪些数据，以及组织如何处理已经收到的副本。改进表单并不意味着可以抹去过去。

第3章 保障个人权利，不设置人为障碍

3.1 接收、身份与适用范围

权利请求渠道需要记录日期、请求人所称身份、请求类型、范围、负责人、适用期限和状态。身份核验应当适度：对任何请求都要求过多材料，可能形成障碍并造成新的信息暴露。应审查组织已掌握哪些信息可用于验证请求真实性、误交他人会造成何种风险，以及该渠道提供哪些替代核验方式。

随后要明确个人真正提出的是什么请求：了解是否存在处理、获取副本、更正数据、反对广告、删除、屏蔽、撤回同意、移植数据或提出投诉。不能把所有请求都变成彻底删除，也不能不作理由和复核途径说明就答复“不予受理”。如果答复中包含第三方信息，应在保护其权利的前提下准备交付版本，但不得声称原始案卷中的事实也随之删除。

阶段	记录内容	可避免的错误
接收	渠道、日期和时区、原文内容及收件确认。	从有人决定查看邮件时才开始计算期限。
身份	所选方法、风险和使用的数据；请求表中不记录秘密信息。	制作不必要的新身份证件副本。
定位	系统、备份、受托处理方和检索条件。	仅依据主数据库作答。
决策	法律依据、排除项、复核情况和交付的数据。	发送第三方信息，或无理由拒绝。
结案	日期、渠道、交付证据及系统中执行的操作。	未实际执行变更就标记为已解决。

3.2 提供访问，同时避免泄露他人信息

导出文件可能包含员工、客户、亲属或对话参与者的数据。访问权并不自动授权披露这些数据。应检查字段、标识符、内容、附件和元数据；交付版本应与保留的原始版本分开。审查不得改变原意，也不得隐去确属请求人的信息。

在阿根廷，所提供的信息必须清晰、充分，即使第三方数据与当事人相关，也不得予以披露。更正、更新或删除有各自的规则和期限；存在保存义务或第三方权利时，还适用例外规定。不得将该期限照搬到其他国家：应记录案件适用的法律制度。[6]

3.3 删除并不意味着销毁一切

删除请求可以与保存义务或权利抗辩并存。答复应区分哪些处理停止、哪些记录被屏蔽、哪些副本受到限制保留，以及各自的法律依据。必须在系统和受托处理方处实际执行措施，而不能只写在答复文本中。如果为抗辩而保留某个数据库，应将其用途限定于该目的，并控制后续访问。

> **虚构示例**
>
> 一个人在注销账户后要求删除其全部信息。组织保留必要的税务凭证，屏蔽其营销画像，删除细分属性，并记录实施各项措施的系统清单。答复应说明已删除、已屏蔽和已保留的内容，不得声称所有信息均已消失。

第4章 可验证的安全性

4.1 风险优先于控制措施目录

分析应从个人和潜在损害出发，而不是从产品清单出发。应识别谁可能访问、可能出现什么错误、哪份副本暴露程度最高，以及数据遭到篡改、丢失、无法使用或泄露会造成什么后果。然后再选择访问控制、加密、日志记录、隔离、备份、培训和审查等措施。对于公开名录，昂贵的控制可能并不相称；对于临床档案，却又可能远远不够。

厄瓜多尔要求结合处理活动、个人以及数据类别和数量，分析风险、威胁和脆弱性。欧盟要求采取与风险相适应的技术和组织措施，并实行设计即保护和默认保护。保留该项评估记录，比声称“我们采用最高标准”更有用，因为它可以解释为何选择各项措施，以及组织接受了哪些剩余风险。[7][8]

[6]阿根廷。第 25.326 号法律，更新文本。第 4–6、9–10、14–16 和 25 条：数据质量、告知、安全、保密、数据主体权利，以及代表第三方提供数据处理服务。 官方在线来源

[7]厄瓜多尔。《个人数据保护基本法》，26-05-2021《官方公报》第 459 号增刊。第 10、37–44 条：原则、安全措施、设计保护、风险和事件处理。 官方在线来源

[8]欧盟。（UE）2016/679 号条例，第 5、25、28 和 32–34 条：原则、设计保护、受托处理方、安全及数据安全泄露的通知/告知。西班牙还要求审查适用的国家和行业法律。 官方在线来源

4.2 控制措施及其运行证据

控制措施	使用虚构信息测试	留存的证据
最小权限	支持岗位用户不得访问工资薪酬数据或下载整个数据库。	角色、授权、尝试访问的结果和访问权限审查。
加密与密钥	对一份副本加密，只有获授权的角色才能恢复该副本。	配置、负责人、恢复情况，以及密钥未记入记录。
日志记录	一项测试操作会生成包含用户、日期、时区和对象的事件。	原生导出文件、数据字典、留存情况和审查记录。
备份	在隔离环境中恢复一组虚构数据。	日期、耗时、异常情况、哈希值和打开验证。
员工离职	撤销访问权限，并验证其已无法继续操作。	离职日期、已检查的系统和负责人。
匿名化	尝试通过数据组合和极端值识别记录。	方法、剩余风险、测试结果和发布批准。

证据必须证明控制措施确实运行，而不只是存在。一张控制台已加密的截图，不能证明所有副本均受到保护；一项密码政策，不能证明权限得到审查；一个名为“备份”的文件夹，也不能证明可以恢复。测试应使用虚构数据，以免在评估一起数据泄露事件时又造成另一起。如果意外访问确实成功，应保留该事件记录并先纠正问题，再发布报告。

4.3 假名化不等于匿名化

用编号替代姓名可以减少直接暴露，但将日期、住址、职位、爱好或某次特殊操作组合起来，仍可能重新识别个人。假名化仍可通过附加信息建立关联；匿名化则要求结合实际披露环境分析重新识别风险。案卷必须将工作版本与公开版本分开，并采用不同的控制措施保护对应关系表。

共享数据集之前，应检查小群组、唯一值、附件、坐标、序列和元数据。即使没有姓名，一段证言仍可能因村镇和职务而识别出个人。此时应进行泛化、抑制或不予公开。不得宣称匿名性完美无缺：应记录方法、假设、剩余风险，并在情境变化时重新审查。

> **实用规则**
>
> 不要只问“我能看到姓名吗？”来判断匿名化是否有效。还要问：他人可以合理地将哪些其他来源组合起来，又有哪些个人会因某项少见特征而被识别。



图2 政策不能证明控制措施有效运行。使用虚构数据测试并留存结果。编辑重构；不构成真实证据。

第5章 供应商、云与数据传输

5.1 使用供应商并不转移责任

供应商代表组织处理数据时，应明确处理指令、目的、获授权人员、地点、分包商、保密要求、安全措施、事件支持、权利请求协助、返还、删除以及可供审查的证据。仅签署合同并不足够：必须知道哪个按钮可以下载数据库、谁可以恢复数据库，以及访问日志保存在哪里。

在阿根廷，代表第三方提供计算机化服务的一方，不得将数据用于合同约定之外的目的，也不得转让数据以供保存；服务履行完毕后，应适用法律规定的数据销毁或经授权保存制度。在哥伦比亚，控制方与受托处理方有所区分，双方均承担特定义务。合同中的角色分类必须符合各方实际决定的事项，而不是服务的商业名称。[9][10]

5.2 数据流转与传输图

云服务的管理可能在一个国家，存储在另一个国家，支持服务在第三个国家，备份则分布在多个国家。流转图应记录这些路径、作出决策的实体、受托处理方、次级受托处理方、每次访问的理由，以及法律

[9]阿根廷。第 25.326 号法律，更新文本。第 4–6、9–10、14–16 和 25 条：数据质量、告知、安全、保密、数据主体权利，以及代表第三方提供数据处理服务。 官方在线来源

[10]哥伦比亚。2012 年第 1581 号法律，第 4、8、12、17–18 和 26 条：原则、权利、告知、控制方和受托处理方的义务，以及向第三国传输。 官方在线来源

要求的保障或机制。“服务器在云端”并未说明位置或风险。跨境传输不能仅靠复制一条条款：必须核实适用范围、例外、接收方和控制措施。

向供应商提问	应提供的书面答复	警示信号
谁可以访问?	角色、地点、身份验证、日志记录和审查。	仅称“全球支持”，却不说明人员和条件。
有哪些次级受托处理方参与?	身份、职能、地点和变更机制。	名单保密或变更时不通知。
如何协助处理权利请求?	查询、更正、屏蔽、导出和期限。	仅提供 PDF，无法搜索或筛选。
如何提供事件通报?	渠道、联系人、时间线、证据和更新情况。	口头通知但未留存记录。
关系如何终止?	导出、可读性、删除、备份和证明文件。	注销账户后无法恢复信息。

5.3 受控退出与技术依赖

签约前，应使用虚构数据测试退出流程。下载导出文件，用独立工具打开，并检查是否保留字段、时区、关联关系和数据字典。如果平台只能打印，应明确记录技术依赖风险。退出还包括生产环境、测试副本、备份和日志中的数据删除；某些组件可能因义务或安全原因需要保留，但必须明确其范围。

> **虚构案例**
> 一家组织更换问卷调查供应商。导出文件包含答复，却没有表单标识符或时区。组织要求供应商重新交付包含数据字典的文件，将两次交付作为不同对象分别保留，并记录第一次交付的局限。最后注销账户，并取得证明文件，说明该操作的实际覆盖范围。

第6章 数据泄露：遏制、研判与通知

6.1 初步行动：勿清除现场痕迹

首要目标是保护个人、限制损害，同时不破坏能够解释事件的信息。应记录发现时间、报告人、可能受影响的系统、可能涉及的数据以及已经采取的措施。通过安全渠道更改密码，但应先保存相关访问事件。不得借恢复系统来清除证据，也不得过早宣称一切已经结束。

NIST SP 800-61 Rev. 3 将准备、检测、响应、恢复和持续改进整合为响应体系。这避免了狭隘的理解：事件响应不能只做“关闭服务器”这一步；还必须了解影响范围、沟通、对个人的影响和后续改进。对于数据泄露事件，还应保存暴露了哪些字段、精确程度如何，以及第三方可能取得了哪些副本。[11][12]

时点	已记录的行动	避免的本能反应
检测	记录信号、来源、时间、负责人和初步影响范围。	因最初的怀疑就宣布根本原因。
遏制	选择适度的措施，并记录处置前的证据。	未导出日志就重置设备或删除账户。
评估	识别数据、数据主体、访问情况、使用情况和可能后果。	把行数误当作人数。
通知	确定适用的义务主体、门槛、接收方、内容和当地期限。	在所有国家和行业照搬 72 小时或 48 小时的规定。
恢复	验证控制措施、监测、对受影响者的支持和变更。	仅以新建文件夹结案，却不总结任何教训。

6.2 通知决策与实用内容

是否通知取决于适用法律、组织类型、事件性质和严重程度以及受影响个人。墨西哥 2026 年现行法律要求立即将重大数据泄露告知受影响者，使其能够维护自身权利。秘鲁 2024 年通过的条例规定，应及时向主管机关报告事件，并根据暴露情况告知受影响者；官方来源指出，原则上期限为 48 小时，有正当理由的除外。在欧盟，第 33 条和第 34 条根据风险区分向主管机关的通知与向数据主体的告知。这些规则不能相互套用。[13][14][15]

有用的通知应在已知事实范围内说明发生了什么、哪些类别的数据可能受到影响、正在采取哪些措施、个人可以采取哪些合理措施，以及从何处获取信息。不得包含秘密信息或关于攻击者的推测。事实发生变化时，应更新通知并保留历史版本。为保护声誉而隐瞒事件，可能会使原本希望避免的损害成倍增加。

[11] NIST SP 800-61 Rev. 3（2025 年 4 月）。CSF 2.0 中的综合事件响应建议：准备、检测、响应、恢复和改进。取代第 2 修订版。 官方在线来源

[12] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 方法指南，并非法律，也不保证证据可采性。 官方在线来源

[13] 墨西哥。《联邦私人持有个人数据保护法》，文本发布于 20-03-2025，修订于 14-11-2025。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和权利请求受理。现行联邦主管机关为反腐败与善治部。 官方在线来源

[14] 秘鲁。第 29733 号法律及其经 DS 016-2024-JUS 批准的条例。目的、比例、安全和保密原则；新条例规定了事件、预防性评估和数据官的渐进职能。 官方在线来源

[15] 欧盟。（UE）2016/679 号条例，第 5、25、28 和 32–34 条：原则、设计保护、受托处理方、安全及数据安全泄露的通知/告知。西班牙还要求审查适用的国家和行业法律。 官方在线来源

6.3 损害、影响范围与结案

评估应考虑数据被使用的可能性、凭据的保密性、联系相关个人的难易程度、个人的脆弱性、访问行为的公开程度，以及身体、经济或歧视性影响。“只是姓名”也可能很严重，因为这些姓名可能与某个敏感服务机构相关联。收集证据时，不得再从公开链接下载泄露数据，也不得将其分发给整个团队。

> **真正结案**
>
> 系统恢复并不意味着事件结束。只有按需告知相关个人、验证控制措施、审查访问情况、保存证据，并修改流程以避免同样的事件序列再次发生，事件才算结束。如果仍有未知事项，报告应将其保留为结论的局限。



图3 数据泄露：遏制事态，但不清除解释事件所需的信息。时间线用于指导响应和通知。编辑重构；不构成真实证据。

第7章 数据留存、删除与可携带性

7.1 留存期限应有依据，而非随心所欲

留存期限应根据处理目的、法律义务、合同、权利抗辩和运营需要确定。“个人数据”并不存在统一的留存年限。应区分正常使用期限、受限屏蔽期和举证保存期。目的发生变化时，应重新审查期限表。“以防万一”而保留一切会增加暴露风险，也会使准确答复请求更加困难。

删除应涵盖系统、导出文件、用户端、供应商及所有可用副本。备份可能有不同的技术周期：应记录备份会被删除、覆盖，还是保持不可访问直至到期。如果恢复备份可能重新引入已删除的数据，程序中必须包括如何再次删除。证明文件不得超出技术实际发生的情况。

7.2 真正可用的数据可携带性

交付数据不等于把数据打印出来。存在数据可携带权或迁移需要时，应审查范围、结构化格式、机器可读性、互操作性、字段、日期和表间关联。使用虚构接收方测试导出，不得暴露第三方信息或秘密。EML 可以保留交付背景，哈希值可用于比对传输文件与接收文件；但二者各自都不能证明内容完整。[16][17]

行动	有用的证据	已声明的局限
删除个人资料	标识符、系统、日期、操作员及不存在验证。	待处理的技术副本及到期日期。
因保存需要而屏蔽	理由、受限访问和剩余用途。	不得用于广告或常规分析。
导出	原生格式、数据字典、筛选条件、行数、时区和哈希值。	查询覆盖范围及排除的数据。
返还给受托处理方	清单、渠道、接收方和下载验证。	仍由受托处理方控制的副本。
恢复备份	在隔离环境中测试，以及重新执行删除操作的清单。	如果周期尚未结束，不得声称已经删除。

> **正确的证明表述**
>
> “营销系统中的个人资料已于 2026 年 11 月 10 日删除，并经核验确认不存在。加密备份按已记录的周期保留至到期；如果恢复备份，将重新执行删除。”这比“所有信息均已销毁”更为严谨。

第8章 三个完整流程

8.1 人力资源：共享文件夹

一家虚构公司将简历保存在人人均可访问的文件夹中。检查发现，其中有亲属信息、推荐人信息、证件材料和没有期限的评估记录。公司决定将处理中、已拒绝和经说明理由保留的案卷分开；限制角色权限；移除公开链接；记录访问情况；并在导出文件中执行删除。一名个人请求访问并获得了自己的数据，其中不包含不应交付的评估人员信息。变更通过测试账户验证，而不是出于好奇查看真实案卷。

8.2 医疗：误发到群组的消息

一家虚构诊所将包含姓名和诊断信息的表格发送到一个外部群组。诊所要求停止传播并删除，且不得将其转发给整个团队；同时记录接收方、内容和复制可能性。随后审查访问权限、联系人和接收方选择程

[16] RFC Editor. RFC 5322, Internet Message Format：消息结构、邮件头和正文。这是保存和理解电子邮件的技术参考，并不能自动证明人的身份。 官方在线来源

[17] 厄瓜多尔。《个人数据保护基本法》，26-05-2021《官方公报》第 459 号增刊。第 10、37–44 条：原则、安全措施、设计保护、风险和事件处理。 官方在线来源

序。是否通知的评估应考虑敏感性和后果，而不只是行数。最终整改包括接收方复核、导出控制和实际演练。

8.3 数据分析：导致个人可被识别的报告

一个团队发布了一个经过假名化处理的数据集，其中包含地区、日期和一次异常购买。读者可以将其与先前发布的信息关联，从而识别客户。团队停止传播，检查小群组并抑制特殊值。新版本不含直接标识符，保留统计用途，并声明其局限。该案例提醒我们，匿名化不当可能使发布信息的本意反而造成新的数据泄露。

> **共同方法**
>
> 三个案例都按相同顺序处理：定位数据和副本、限制访问和传播、了解后果、决定是否沟通、实施控制并保存证据。变化的是人员和技术，不变的是工作规范。

附录A 隐私保护的功能等效对照

文献审查截至 2026 年 11 月 10 日。所比较的功能并不意味着适用范围、法律依据、期限或效力完全相同。引用条文是为了定位相关法律制度，而不是自动解决具体案卷。对于智利，明确注明新制度延后生效，以免将其误作提前适用。

法域	对应功能	操作注意事项
墨西哥	LFPDPPP：原则、安全、保密、权利及重大数据泄露告知。	2025 年新法及现行联邦主管机关；审查行业规定和修法情况。
秘鲁	第 29733 号法律和 DS 016-2024-JUS 号条例：原则、安全、事件、预防和渐进式角色。	该条例有过渡安排和自身具体规定；不得照搬欧洲期限。
智利	第 21.719 号法律修订第 19.628 号法律：原则、权利、安全、责任和监管局。	新制度延后至 01-12-2026 生效；应核查相应日期适用的法律。
阿根廷	第 25.326 号法律：数据质量、同意、告知、安全、权利和代表第三方提供的服务。	不得将权利简化为通用表单，也不得披露第三方数据。
哥伦比亚	第 1581 号法律：原则、类别、权利、告知、控制方、受托处理方和传输。	审查排除事项、特别规则和各角色的具体义务。
厄瓜多尔	LOPDP：原则、安全、风险、设计与默认保护、事件和权利。	为答复请求而访问数据，不授权无限期处理或永久保存。

法域	对应功能	操作注意事项
西班牙 / 欧盟	RGPD：原则、设计保护、受托处理方、安全和数据泄露；辅以国家和行业规定。	区分向主管机关通知所依据的风险与向数据主体告知所依据的高风险；审查 LOPDGDD 和行业规定。

表格来源： 18192021222324

A.1 用于选择法律依据的表格，而非换算数字的表格

处理具体案件时，先写明所需功能：收集数据、变更目的、聘请受托处理方、向境外传输、响应权利请求、通知事件或删除数据。然后查阅适用法律文件，明确条文、事项、主体、日期和例外。如果某项规则仅适用于公共、金融或医疗行业，就不能将其当作普遍规则。未核实某项例外时，不得编造答案。

七个法律体系的电子文件规则有助于保存决策证据：法律认可、归属、完整性、原件、可访问性和保存。但签名、印章或哈希值既不能使非法处理合法化，也不能证明个人理解了告知内容。隐私、记录完整性和内容真实性应分别评估。 25262728293031

[18]墨西哥。《联邦私人持有个人数据保护法》，文本发布于 20-03-2025，修订于 14-11-2025。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和权利请求受理。现行联邦主管机关为反腐败与善治部。 官方在线来源

[19]秘鲁。第 29733 号法律及其经 DS 016-2024-JUS 批准的条例。目的、比例、安全和保密原则；新条例规定了事件、预防性评估和数据官的渐进职能。 官方在线来源

[20]智利。第 21.719 号法律，修订关于个人数据保护的第 19.628 号法律。包含新制度的版本延后至 01-12-2026 生效；在该日期之前，应核查当时适用的法律，不得将未来义务提前当作现行义务。 官方在线来源

[21]阿根廷。第 25.326 号法律，更新文本。第 4–6、9–10、14–16 和 25 条：数据质量、告知、安全、保密、数据主体权利，以及代表第三方提供数据处理服务。 官方在线来源

[22]哥伦比亚。2012 年第 1581 号法律，第 4、8、12、17–18 和 26 条：原则、权利、告知、控制方和受托处理方的义务，以及向第三国传输。 官方在线来源

[23]厄瓜多尔。《个人数据保护基本法》，26-05-2021《官方公报》第 459 号增刊。第 10、37–44 条：原则、安全措施、设计保护、风险和事件处理。 官方在线来源

[24]欧盟。（UE）2016/679 号条例，第 5、25、28 和 32–34 条：原则、设计保护、受托处理方、安全及数据安全泄露的通知/告知。西班牙还要求审查适用的国家和行业法律。 官方在线来源

[25]墨西哥。《商法典》，第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文的可采性。官方汇编。 官方在线来源

[26]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。 官方在线来源

[27]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。 官方在线来源

[28]《（UE）910/2014 号 eIDAS 条例》，第 25–26 和 46 条：不得因电子签名和文件的格式而加以歧视，高级电子签名及合格电子签名的效力。 官方在线来源

[29]阿根廷。第 25.506 号《数字签名法》，第 1 和 5–9 条：数字文件、援引遭否认的电子签名时的举证责任，以及有限范围的推定。 官方在线来源

[30]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级电子签名、日期和证据效力。 官方在线来源

[31]秘鲁。IOFE 条例，DS 052-2008-PCM，第 3 和 4 条：经数字签名的电子文件的要求与认可。 官方在线来源

附录B 便于调整的现成模板

B.1 处理活动记录

字段	最低内容要求	验收控制
活动与负责人	具体任务、流程负责人和代理人。	其他人能够据此找到决策人。
目的与法律依据	具体目的、依据及例外（如有）。	不得仅用“管理”作为完整答复。
数据与人员	字段、敏感性、第三方和需要优先关注的群体。	每个字段均有必要性说明。
流转与受托处理方	输入、系统、访问、传输和最终去向。	包括导出文件和备份。
留存与权利	期限、屏蔽、删除和受理渠道。	不得无理由地写“无限期”。
风险与控制措施	可能的损害、措施、测试和剩余风险。	具有控制措施运行的证据。

B.2 数据主体申请表

内部记录用虚构模板

```
ID: PRIV-DEMO-2026-001
接收：[日期、时间、时区、渠道]
请求原文：[访问、更正、删除、反对、其他]
身份：[适度的方法；本表不附证件材料]
范围：[期间、系统、人员和排除项]
适用期限：[规范、条文、起算和届满]
检索：[系统、筛选条件、受托处理方和备份]
决策：[法律依据、复核、第三方数据]
已执行措施：[系统、日期、操作员、核验]
交付：[格式、渠道、接收方、日期和验证]
待办事项与局限：[哪些事项未解决及其原因]
```

B.3 数据泄露事件时间线

事件	必须记录的内容	相关决策
初始信号	来源、原始值、时区、负责人和证据。	建立案卷并保全证据。
遏制	措施、授权、范围、效果和处置前证据。	限制损害，同时保留背景信息。
范围	数据、人员、访问、副本、使用情况和疑点。	依据事实划分风险等级。
沟通	接收方、内容、渠道、时间和版本。	遵守当地制度，不作超出必要的披露。
恢复	恢复、访问、监测和测试。	验证控制措施有效运行。

事件	必须记录的内容	相关决策
改进	原因、流程变更、负责人和验证。	防止再次发生，而不只是结案。

B.4 供应商评估

启用真实数据前的核查清单

1. 各方的角色和合同目的。
2. 最少必要数据、地点、获授权人员和次级受托处理方。
3. 身份验证、最小权限、日志记录、加密和密钥。
4. 可验证的安全证据，而不只是商业声明。
5. 事件报告渠道、内容和沟通证明。
6. 权利请求协助、检索和原生导出。
7. 数据传输、保障措施和地点变更。
8. 退出：格式、数据字典、可访问性和打开测试。
9. 删除、备份和注明局限的证明文件。
10. 定期审查和内部负责人。

B.5 删除或屏蔽证明

虚构示例

对象：EXP-DEMO-2026-001
范围：营销个人资料和营销活动导出文件
措施：删除在用个人资料，屏蔽须留存的凭证
系统：[名称、版本、地点和负责人]
执行：[日期、时区、操作员和方法]
核验：[查询、缺失情况、访问情况和结果]
备份：[周期、访问权限，以及恢复时重新执行删除]
受托处理方：[通知和答复]
剩余保存：[法律依据、目的和期限]
局限：[不能断言的事项]
复核：[人员、日期和关联证据]

附录C 术语表与输出控制

术语	在本手册中的实际用法
控制方	在适用制度下决定处理法律依据和处理活动的一方。
受托处理方	代表控制方处理数据的一方，须遵循指示并承担自身义务。
假名化	可借助附加信息建立关联；需要分离信息和实施控制。
匿名化	在特定情境下，经合理判断无法建立关联；需要测试和复核。
屏蔽	因有正当理由而限制处理，但不删除对象。
可携带性	在允许的范围内提供结构化、可互操作的数据交付。
数据泄露	影响个人数据安全的事件；其严重程度需要评估。

术语	在本手册中的实际用法
合规证据	可用于审查决策、执行和结果的记录，而不只是意图。

结束流程之前	必须给出的答复
存在哪些数据和副本？	清单涵盖文件、备份和供应商。
为什么每个字段都必不可少？	目的、法律依据和最小化均有记录。
谁可以访问，有何证据？	角色、日志记录和虚构数据测试。
个人如何行使权利？	渠道、检索、决策、交付和执行。
发生事件或退出时怎么办？	时间线、沟通、导出和删除均经核验。
哪些事项仍不清楚？	明确的局限、负责人和下一次核验。

结语

保护数据，就是降低组织决策对个人造成伤害的可能性。证据的作用是让这种保护得到审查和纠正，而不是把它变成行政管理上的表面文章。