ACCCF / APPLIED KNOWLEDGE LIBRARY

02

VOLUME

Applied privacy, security and documented decisions

Spanish edition · 2026

Personal Data Protection and Compliance Evidence Manual

Inventory, rights, providers, incidents, preservation, and verifiable deletion

Protecting people through decisions that can be explained and verified, not through copied policies or folders of documents that no one puts into practice.

For privacy officers, legal, security, IT, human resources, and management teams, and providers that process personal information. It includes one workflow for small organizations and another for complex operations.

Editorial coordination: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.

Contents

Visible pagination corresponds to the PDF edition. Word may update this index when the document is opened; headings retain internal navigation.

Introduction: privacy is demonstrated in practice 3

Chapter 1. An inventory that supports decision-making 3

1.1 Describe processing without hiding it behind an acronym 3

1.2 Finding invisible copies 4

Chapter 2. Purpose, legal basis, and data minimization 5

2.1 Separate purposes that appear identical 5

2.2 The test for unnecessary data 5

2.3 Clear information and privacy notice 6

Chapter 3. Data subjects' rights without artificial barriers 6

3.1 Receipt, identity, and scope 6

3.2 Access without disclosing other people's data 7

3.3 When erasure does not mean destroying everything 7

Chapter 4. Verifiable security 7

4.1 Risk before the control catalog 7

4.2 Controls and evidence of operation 8

4.3 Pseudonymized does not mean anonymous 8

Chapter 5. Providers, cloud services, and transfers 9

5.1 The provider does not absorb responsibility 9

5.2 Data flow and transfer map 9

5.3 Controlled exit and technological dependence 10

Chapter 6. Breaches: contain, understand, and notify 10

6.1 Initial response without altering the scene 10

6.2 Deciding whether to notify and providing useful content 11

6.3 Harm, scope, and closure 11

Chapter 7. Retention, deletion, and portability 12

7.1 A schedule based on reasons, not whims 12

7.2 Portability that is actually usable 12

Chapter 8. Three end-to-end walkthroughs 13

8.1 Human resources: the shared folder 13

8.2 Health: the message sent to the wrong group 13

8.3 Analytics: the report that made individuals identifiable 13

Annex A. Functional equivalents in privacy 13

A.1 A table for selecting a legal basis, not translating legal provision numbers 14

Annex B. Templates ready to adapt 15

B.1 Record of processing activities 15

B.2 Data subject request form 15

B.3 Breach timeline 15

B.4 Provider assessment 16

B.5 Record of deletion or blocking 16

Annex C. Glossary and final checks 16

Introduction: privacy is demonstrated in practice

A privacy policy may be sound, yet the organization may still expose information it does not need every day. Compliance begins where the drafting ends: in the form that requests excessive data, the folder shared with external personnel, the provider that can download an entire database, the backup that no one knows how to restore, and the deletion that occurs only on screen. The useful question is not whether a document exists, but what happens to a specific individual and their information from collection until it is no longer needed.

This manual uses a simple workflow: data → purpose → legal basis → access → risk → evidence → final disposition. Every link must be explainable without resorting to generalities. If a record serves to document a sale, identify which fields that purpose requires, who administers them, how long they are retained, and what other information arrived with them. If a new purpose arises, renaming the folder is not enough: lawfulness, information provided to the data subject, and the scope of access must be reviewed.

Compliance evidence does not mean accumulating screenshots to create the appearance of work. It means preserving the version of a decision, the source that justified it, the person who authorized it, the control applied, and the result of verifying that control. The laws compared here are not used to copy another country's policy. They help identify the function the organization needs to document: minimization, security, transparency, rights, processor, incident, or transfer. The legal basis and time limits must always be checked against the territory, sector, and date of processing.

> **First decision**
> Before buying a tool or drafting another policy, choose a real process and trace it using fictitious data. If you cannot explain what information enters, why, who sees it, where it ends up, and how a right is exercised, that is your first concrete task.

Chapter 1. An inventory that supports decision-making

1.1 Describe processing without hiding it behind an acronym

A useful inventory does not begin with "customer database," because that label can combine sales, support, collections, marketing, and recruitment. It begins with an understandable activity: recording a purchase, handling a warranty claim, evaluating a job application, running payroll, answering an inquiry, or maintaining building security. For each activity, record the specific purpose, necessary fields, individuals covered, system, custodian, intake channel, and anticipated outcome.

Classification must reflect consequences, not merely nominal sensitivity. A name and telephone number may pose little risk in a contact directory but high risk when they reveal the location of a threatened person. An investigation file may combine identity, health, financial circumstances, communications, and unrelated third parties. The label "confidential" is not enough: define who may use the file, under what controls, for what decision, and for how long. Context can turn a combination of seemingly ordinary data into an intimate profile.

Inventory field	Operational question	Fictitious example
Activity	What specific task is being carried out?	Warranty service for equipment purchased online.

Inventory field	Operational question	Fictitious example
Minimum data	Which fields are required to complete it, and which are ancillary?	Order, contact details, delivery address, and diagnosis; no employment history.
Individuals	Data subjects, third parties, minors, or vulnerable groups?	Buyer, package recipient, and assigned technician.
Flow	Where does it come from, and to whom is it disclosed?	Store → support platform → courier; no public disclosure.
Custody and retention period	Who decides, and when is it no longer needed?	After-sales manager; retention period determined by operations and verifiable obligations.
Evidence	How are the decision and its implementation evidenced?	Notice version, roles, logs, contract, and deletion record.

1.2 Finding invisible copies

The inventory must include exports, attachments, scanned paper documents, personal folders, application logs, backups, and third-party services. The official database may be controlled while an Excel file circulates through messaging with no owner or deletion date. Calling that copy “temporary” does not mean it is no longer being processed. Document who created it, why it was needed, where it is stored, who can open it, and how it will be removed once it has served its purpose.

A good fact-finding interview does not merely ask which system the department uses. Ask a staff member to walk through an entire workday using fictitious information: how a request arrives, what they download, to whom they forward it, where they keep notes, what happens when an error occurs, and what they do before going on vacation. The real map emerges in the exceptions. Passwords must not be written in the inventory; record the control mechanism and its owner instead.

> **Final checks**
> No process should be closed with “and other data as necessary.” Specify the fields, source, destination, and reason. Mark unknowns for investigation; do not replace them with a reassuring checkbox.



Figure 1. From data to final disposition. Each decision leaves a source and a verification. Editorial reconstruction; it does not constitute actual evidence.

Chapter 2. Purpose, legal basis, and data minimization

2.1 Separate purposes that appear identical

Selling a product, sending advertising, and building a behavioral profile do not constitute a single purpose. The first may be necessary for a relationship; the others require their own analysis. When an organization combines purposes in a phrase such as “administrative and commercial purposes,” it becomes impossible to determine which data are actually necessary and which communications must be explained separately. The record must preserve that distinction so that individuals can refuse a use without unduly losing the essential service.

Consent is one possible legal basis, not a universal key. Other grounds may include a legal obligation, performance of a legal relationship, exercise of public functions, defense of rights, or another circumstance provided for in the relevant jurisdiction. Identify the specific rule before selecting a form. Requesting consent for everything can falsely shift responsibility to the individual and obscure an operation that already has another legal basis. If processing changes, review compatibility, information, and controls before carrying it out.

Mexican law includes principles of lawfulness, purpose, fairness, consent, quality, proportionality, information, and accountability; Colombian law develops legality, purpose, freedom, quality, transparency, restricted access, security, and confidentiality; Ecuadorian law requires proactive and demonstrable accountability. Similar principles help build a methodology, but each circumstance and exception must be read in the applicable law and sector-specific rules.[1][2][3]

2.2 The test for unnecessary data

Take a field and remove it from the fictitious example. If the activity can be completed without it, you must justify why it is requested. The criterion is not whether it might be useful in the future, but whether it is appropriate and necessary for the current purpose. A telephone number may suffice to provide notice of a delivery; a copy of identification is unnecessary if identity can be verified by a less intrusive means. For statistical analysis, it may not be necessary to retain the name alongside the result.

Situation	Data minimization decision	A record that prevents improvisation
Support for a purchase	Order and contact channel, not the customer’s complete file.	Approved fields and a screenshot of the current form.
Identity verification	Choose the least invasive method that provides the required security.	Alternatives assessed, risk and approval.
Aggregate report	Remove identifiers and review combinations that could enable reidentification.	Small-group testing and suppression applied.
Third-party request	Separate the requester’s data from other individuals’ data.	Delivered version and pre-delivery content review.
New purpose	Stop until compatibility and legal basis have been reviewed.	Request, analysis, and dated authorization.

[1]Mexico. Federal Law on the Protection of Personal Data Held by Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and handling of rights requests. The current federal authority is the Secretaría Anticorrupción y Buen Gobierno. Official online source

[2]Colombia. Statutory Law 1581 of 2012, Articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of controllers and processors, and transfers to third countries. Official online source

[3]Ecuador. Organic Law on the Protection of Personal Data, Official Registry Supplement 459 of 26-05-2021. Articles 10, 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

2.3 Clear information and privacy notice

The privacy notice must enable individuals to identify who decides, the purposes for which their data are used, with whom the data are shared, how to exercise their rights, and where to raise a question. A lengthy text is no substitute for a timely explanation. Retain the version actually presented and its context: page, date, flow, language, and changes. If the site changes, do not delete the previous version from the compliance record.

In Argentina, individuals must be informed in advance of the purpose, recipients or categories of recipients, controller, and possibility of exercising rights. In Colombia, clear and express information must be provided when authorization is requested, and proof of compliance must be retained. These examples show why evidence must combine text and context: a current URL does not establish what an individual saw years earlier.[4][5]

> **Fictitious case: the promotion that requested a dossier**
>
> A retailer requests official identification, marital status, and home address to issue a digital coupon. The analysis results in a version that requests an email address, separate consent for advertising, and no copy of identification. Document which data are no longer collected and what the organization does with copies already received. Improving the form does not authorize forgetting the past.

Chapter 3. Data subjects' rights without artificial barriers

3.1 Receipt, identity, and scope

The rights channel requires a record containing the date, apparent requester, request type, scope, person responsible, applicable deadline, and status. Identity must be verified proportionately: demanding an excessive file for every request can create a barrier and cause further exposure. Review what information the organization already holds to authenticate the request, the risk of disclosure to another person, and the verification alternatives offered by the channel.

Next, define what the individual is actually requesting: to know whether processing occurs, obtain a copy, correct data, object to advertising, erase, block, withdraw consent, port data, or lodge a complaint. Do not turn every request into total erasure or respond "inadmissible" without explaining the reason and review procedure. If the response contains third parties, prepare a disclosure that protects their rights without purporting to erase facts from the original file.

Stage	What is documented	Error avoided
Receipt	Channel, date, and time zone; verbatim content and acknowledgment of receipt.	Measuring the deadline from when someone decides to check the email.
Identity	Chosen method, risk, and data used, with no secrets in the form.	Creating an unnecessary new copy of identification.
Locating data	Systems, backups, processors, and search criteria.	Responding solely from the primary database.
Decision	Legal basis, exceptions, review, and data provided.	Disclosing third-party information or refusing without giving reasons.

[4] Argentina. Law 25.326, updated text. Articles 4–6, 9–10, 14–16, and 25: quality, information, security, confidentiality, data subjects' rights, and provision of processing services on behalf of third parties. Official online source

[5] Colombia. Statutory Law 1581 of 2012, Articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of controllers and processors, and transfers to third countries. Official online source

Stage	What is documented	Error avoided
Closure	Date, channel, evidence of delivery, and actions taken in systems.	Marking the request as resolved without implementing the change.

3.2 Access without disclosing other people's data

An export may contain data about employees, customers, relatives, or participants in a conversation. The right of access does not automatically authorize their disclosure. Review fields, identifiers, content, attachments, and metadata; use a disclosure copy separate from the preserved original. The review must not alter meaning or conceal information that does belong to the requester.

In Argentina, information must be clear and comprehensive and must not reveal third-party data even when linked to the data subject. Rectification, updating, and erasure have their own rules and deadlines, as well as exceptions where there is a retention obligation or third-party rights are involved. Do not copy that deadline to another country: record the legal regime applicable to the case.[6]

3.3 When erasure does not mean destroying everything

A deletion request may coexist with a retention obligation or the defense of a right. The response must distinguish which processing ceases, which record is blocked, which copy is retained with restricted access, and on what legal basis. Actions must be implemented in the systems and with processors, not merely stated in the response. If a database is retained for defense purposes, its use must be limited to that purpose and subsequent access controlled.

> **Fictitious example**
> An individual asks for all their information to be deleted after closing their account. The organization retains the necessary tax documentation, blocks their marketing profile, deletes segmentation attributes, and documents the systems in which it implemented each measure. The response explains what was deleted, blocked, and retained, without claiming that everything disappeared.

Chapter 4. Verifiable security

4.1 Risk before the control catalog

The analysis starts with individuals and potential harm, not a list of products. Identify who could gain access, what error is plausible, which copy is most exposed, and the consequences of alteration, loss, unavailability, or disclosure. Then select controls for access, encryption, logging, segregation, backup, training, and review. An expensive control may be disproportionate for a public directory and insufficient for a clinical file.

Ecuador requires analysis of risks, threats, and vulnerabilities, taking into account the processing, individuals, and categories and volume of data. The European Union requires technical and organizational measures appropriate to the risk, with data protection by design and by default. Recording

[6] Argentina. Law 25.326, updated text. Articles 4–6, 9–10, 14–16, and 25: quality, information, security, confidentiality, data subjects' rights, and provision of processing services on behalf of third parties. Official online source

this assessment is more useful than stating "we have the highest standards," because it explains why each measure was selected and what residual risk the organization accepted.[78]

4.2 Controls and evidence of operation

Control	Test with fictitious information	Evidence retained
Least privilege	A support user cannot open payroll records or download the entire database.	Role, authorization, attempt result, and access review.
Encryption and keys	A copy is encrypted and only an authorized role can recover it.	Configuration, responsible persons, recovery, and no keys recorded in the test report.
Logs	A test action generates an event with user, date, time zone, and object.	Native export, data dictionary, retention, and review.
Backup	A fictitious dataset is restored in an isolated environment.	Date, duration, incidents, hash, and file-opening validation.
Staff offboarding	Access is revoked and verified as no longer functional.	Termination date, systems reviewed, and person responsible.
Anonymization	Attempt to identify records through combinations and extreme values.	Method, residual risk, testing, and release approval.

Evidence must demonstrate operation, not merely existence. A screenshot of an encrypted console does not prove that every copy is protected; a password policy does not prove that privileges are reviewed; a folder named "backup" does not establish recoverability. Design tests with fictitious data to avoid causing a breach while assessing another. If unexpected access does work, preserve the event and correct the issue before publishing the report.

4.3 Pseudonymized does not mean anonymous

Replacing names with reference numbers reduces direct exposure, but identity can be inferred again by combining date, address, job title, hobbies, or a unique transaction. Pseudonymization retains the possibility of association through additional information; anonymization requires a reidentification analysis in the actual context of disclosure. The file must separate the working version from the public version and protect the lookup table with distinct controls.

Before sharing a dataset, review small groups, unique values, attachments, coordinates, sequences, and metadata. A testimonial without a name may still identify someone through their town and job title. In that case, generalize or suppress the information, or do not publish it. Do not claim perfect anonymity: document the method, assumptions, residual risk, and review if the context changes.

> **Practical rule**
> Do not assess the effectiveness of anonymization by asking "Do I see a name?" Ask what other sources someone could reasonably combine and which individual would be identified by an uncommon characteristic.

[7] Ecuador. Organic Law on the Protection of Personal Data, Official Registry Supplement 459 of 26-05-2021. Articles 10, 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

[8] European Union. Regulation (EU) 2016/679, Articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of security breaches. Spain also requires review of applicable national and sector-specific legislation. Official online source

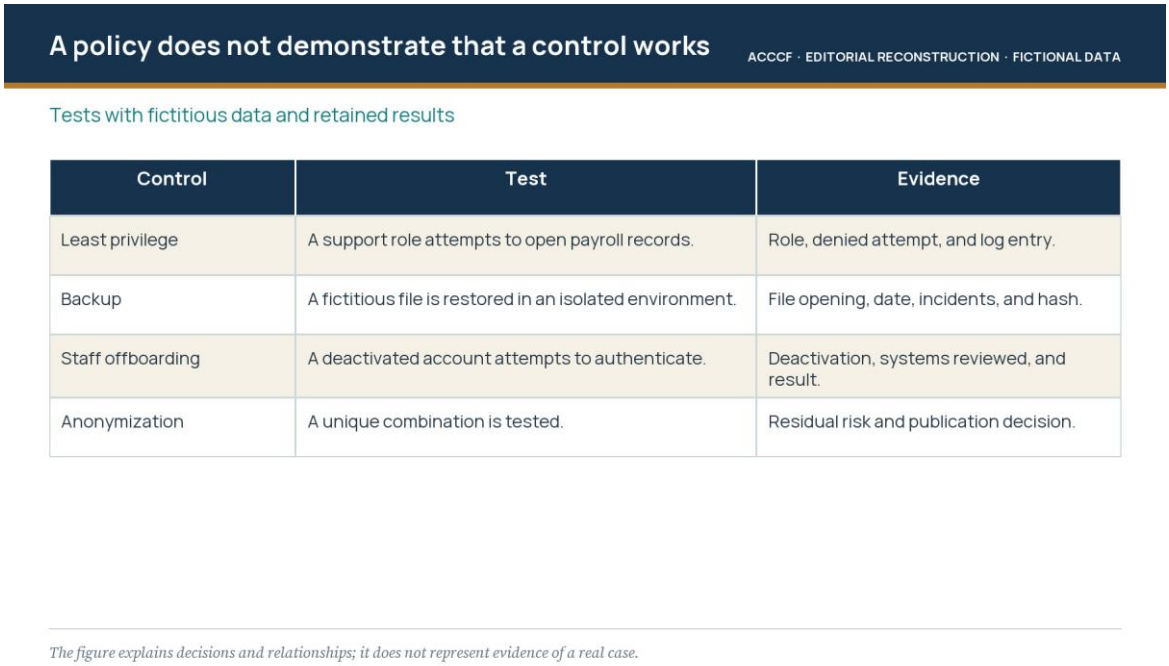


Figure 2. A policy does not demonstrate that a control works. Tests with fictitious data and retained results. Editorial reconstruction; it does not constitute actual evidence.

Chapter 5. Providers, cloud services, and transfers

5.1 The provider does not absorb responsibility

When a provider processes data on the organization's behalf, define instructions, purpose, authorized personnel, location, subcontractors, confidentiality, security measures, incident support, assistance with rights requests, return, deletion, and evidence available for review. Signing a contract is not enough: you must know which button can download the database, who can restore it, and where the access logs are.

In Argentina, a provider of computer-based services on behalf of third parties may not use the data for a purpose other than that of the contract or transfer them for storage; upon completion of the service, the statutory regime for destruction or authorized retention applies. Colombia distinguishes between controller and processor and assigns specific duties to each. The contractual classification must reflect what each party actually decides, not the service's commercial name.[9][10]

5.2 Data flow and transfer map

A cloud service may be administered in one country, store data in another, provide support from a third, and maintain backups in several. The map records these routes, the entity that makes decisions, processors, subprocessors, the reason for each access, and the safeguard or mechanism required by law. "The server is in the cloud" describes neither location nor risk. An international transfer requires more than copying a clause: scope, exceptions, recipient, and controls must be verified.

Question for the provider	Expected documented response	Red flag
Who can access it?	Roles, location, authentication, logging, and review.	"Global support" with no named personnel or conditions.

[9]Argentina. Law 25.326, updated text. Articles 4–6, 9–10, 14–16, and 25: quality, information, security, confidentiality, data subjects' rights, and provision of processing services on behalf of third parties. Official online source

[10]Colombia. Statutory Law 1581 of 2012, Articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of controllers and processors, and transfers to third countries. Official online source

Question for the provider	Expected documented response	Red flag
Which subprocessors are involved?	Identity, role, location, and change procedure.	Undisclosed list or changes without notice.
How do you assist with rights requests?	Search, correction, blocking, export, and deadlines.	Offers only PDF, with no search or filters.
How do you report incidents?	Channel, contact, timeline, evidence and updates.	Verbal notification with no record.
How does the relationship end?	Export, readability, deletion, backups, and documented confirmation.	Account closure without data recovery.

5.3 Controlled exit and technological dependence

Before contracting, test the exit process with fictitious data. Download an export, open it in an independent tool, and check whether it preserves fields, time zone, relationships, and data dictionary. If the platform only supports printing, declare the lock-in risk. Exit also covers deletion from production, test copies, backups, and logs; some components may be retained for legal or security reasons, but their scope must be defined.

> **Fictitious case**
> An organization changes survey providers. The export contains responses but no form identifiers or time zone. It requests a new delivery with a data dictionary, retains both as separate objects, and records the limitation of the first. Finally, it deletes the account and obtains confirmation of the actual scope of that action.

Chapter 6. Breaches: contain, understand, and notify

6.1 Initial response without altering the scene

The first objective is to protect individuals and limit harm without destroying information that explains the incident. Record when it was detected, who reported it, which systems appear affected, what data may be involved, and what actions have already occurred. Change passwords through a secure channel, but preserve relevant access events first. Restoration must not be used to erase evidence or to claim prematurely that the incident is over.

NIST SP 800-61 Rev. 3 organizes response around preparation, detection, response, recovery, and continuous improvement. This prevents a narrow interpretation: an incident does not exist only when the “server is shut down”; scope, communication, effects on individuals, and subsequent changes must also be understood. In a data breach, also preserve a record of which fields were exposed, with what precision, and which copies a third party may have obtained.[11][12]

Phase	Documented action	Reflexive actions to avoid
Detection	Record the signal, source, time, person responsible, and initial scope.	Declaring a root cause based on the first suspicion.
Containment	Choose a proportionate measure and document prior evidence.	Resetting devices or deleting accounts without exporting logs.

[11] NIST SP 800-61 Rev. 3 (April 2025). Incident response recommendations integrated into CSF 2.0: preparation, detection, response, recovery, and improvement. It supersedes Revision 2. Official online source

[12] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodological guidance, not legislation or a guarantee of admissibility. Official online source

Phase	Documented action	Reflexive actions to avoid
Assessment	Identify data, data subjects, access, use, and plausible consequences.	Confusing the number of rows with the number of individuals.
Notification	Apply local requirements for the notifying party, threshold, recipient, content, and deadline.	Copying 72-hour or 48-hour deadlines to every country and sector.
Recovery	Verify controls, monitoring, support for affected individuals, and changes.	Closing with a new folder and no lessons learned.

6.2 Deciding whether to notify and providing useful content

Notification depends on applicable law, the type of organization, the nature and severity of the incident, and the individuals affected. In Mexico, the law in force in 2026 requires that significant breaches be reported immediately to affected individuals so that they can defend their rights. In Peru, the Regulation approved in 2024 introduces timely incident reporting to the authority and communication to affected individuals according to exposure; the official source specifies 48 hours in principle, unless there are justified reasons. In the European Union, Articles 33 and 34 distinguish notification to the authority from communication to the data subject according to risk. These rules are not interchangeable.[13][14][15]

A useful notice explains what happened to the extent known, which categories of data may be affected, what is being done, what reasonable steps individuals can take, and where to obtain information. Do not include secrets or speculation about the attacker. If the facts change, update the notice and retain its history. Concealing an incident to protect reputation can multiply the harm it was intended to avoid.

6.3 Harm, scope, and closure

The assessment considers the possibility of use, credential confidentiality, ease of contact, individuals' vulnerability, whether the access was public, and physical, financial, or discriminatory effects. "It was only names" can be serious if they are linked to a sensitive care facility. Collect evidence without downloading the leaked data again from a public link or distributing it to the entire team.

> **Genuine closure**
> An incident does not end when the system is restored. It ends when individuals have been informed as appropriate, controls verified, access reviewed, evidence preserved, and the process modified to prevent the same sequence. If anything remains unknown, the report must retain it as a limitation.

[13] Mexico. Federal Law on the Protection of Personal Data Held by Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and handling of rights requests. The current federal authority is the Secretaría Anticorrupción y Buen Gobierno. Official online source

[14] Peru. Law 29733 and its Regulation approved by DS 016-2024-JUS. Principles of purpose, proportionality, security, and confidentiality; the new Regulation addresses incidents, preventive assessment, and the progressive functions of the data officer. Official online source

[15] European Union. Regulation (EU) 2016/679, Articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of security breaches. Spain also requires review of applicable national and sector-specific legislation. Official online source



Figure 3. Breach: contain without erasing the explanation. The timeline guides response and notification. Editorial reconstruction; it does not constitute actual evidence.

Chapter 7. Retention, deletion, and portability

7.1 A schedule based on reasons, not whims

Retention is determined by purpose, legal obligation, contract, defense of rights, and operational need. There is no universal retention period for "personal data." Distinguish the period of ordinary use from restricted blocking and evidentiary retention. Review the schedule when the purpose changes. Keeping everything just in case increases exposure and makes it harder to respond accurately to a request.

Deletion must cover systems, exports, users, providers, and available copies. Backups may follow a different technical cycle: document whether they are deleted, overwritten, or kept inaccessible until expiration. If restoration could reintroduce deleted data, the procedure must explain how to delete it again. Do not issue a confirmation that claims more than technically occurred.

7.2 Portability that is actually usable

Providing data does not mean printing it. Where a right to portability or a migration need exists, review scope, structured format, machine readability, interoperability, fields, dates, and links between tables. Test the export with a fictitious recipient without exposing third-party information or secrets. EML can preserve delivery context, and hashes allow the transmitted and received files to be compared; neither certifies by itself that the content is complete.[16][17]

Action	Useful evidence	Declared limitation
Delete profile	Identifier, system, date, operator, and verification of absence.	Pending technical copies and expiration date.
Block for retention	Reason, restricted access and residual purpose.	Do not use for advertising or ordinary analytics.

[16]RFC Editor. RFC 5322, Internet Message Format: message structure, headers, and body. It is a technical reference for preserving and understanding email, not automatic proof of human identity. Official online source

[17]Ecuador. Organic Law on the Protection of Personal Data, Official Registry Supplement 459 of 26-05-2021. Articles 10, 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

Action	Useful evidence	Declared limitation
Export	Native format, data dictionary, filters, rows, time zone, and hash.	Query coverage and excluded data.
Return to processor	Inventory, channel, recipient, and download verification.	Remaining copies under the processor's control.
Restore backup	Test in an isolated environment and maintain a list of deletions to reapply.	Do not claim deletion if the cycle has not yet ended.

Proper confirmation

"The profile was deleted from the marketing system and its absence was verified on 10 November 2026. The encrypted backup follows the documented cycle until expiration; if restored, the deletion is reapplied." This is more rigorous than "all information was destroyed."

Chapter 8. Three end-to-end walkthroughs

8.1 Human resources: the shared folder

A fictitious company stores résumés in a folder accessible to everyone. The walkthrough identifies data about relatives, references, documents, and assessments with no retention period. It decides to separate active files, rejected files, and files retained for justified reasons; restrict roles; remove public links; log access; and delete exports. An individual requests access and receives their data without information about the evaluators that should not be disclosed. The change is tested with a test account, not by browsing a real file out of curiosity.

8.2 Health: the message sent to the wrong group

A fictitious clinic sends a table containing names and diagnoses to an external group. The group is asked to stop distributing and delete it without forwarding it to the entire team; recipients, content, and the possibility of copying are recorded. Access, contacts, and the recipient-selection procedure are reviewed. The notification assessment considers sensitivity and consequences, not merely the number of rows. The final changes include recipient verification, export controls, and a practical exercise.

8.3 Analytics: the report that made individuals identifiable

A team publishes a pseudonymized dataset containing region, date, and an exceptional purchase. A reader can link it to a previous post and identify the customer. Distribution is halted, small groups reviewed, and unique values suppressed. The new version retains statistical utility without direct identifiers and states its limitations. The case is a reminder that flawed anonymization can constitute a new breach caused by the attempt to report itself.

Shared method

All three cases follow the same sequence: locate data and copies, restrict access and distribution, understand the consequences, decide on communication, implement controls, and preserve evidence. The individuals and technology change; the discipline does not.

Annex A. Functional equivalents in privacy

Sources reviewed as of 10 November 2026. The functions compared do not imply identical scope, legal basis, time limits, or effect. Articles are cited to locate the legal regime, not to resolve a case automatically.

For Chile, the delayed entry into force of the new regime is expressly noted to avoid presenting it as applicable before that time.

Jurisdiction	Functions identified	Operational precaution
Mexico	LFPDPPP: principles, security, confidentiality, rights, and notification of significant breaches.	New 2025 law and current federal authority; check sector-specific rules and reforms.
Peru	Law 29733 and Regulation DS 016-2024-JUS: principles, security, incidents, prevention, and progressive roles.	The Regulation has its own transition provisions and details; do not copy European deadlines.
Chile	Law 21.719 amends Law 19.628: principles, rights, security, accountability, and the Agency.	New regime with delayed entry into force on 01-12-2026; check the law applicable at the relevant date.
Argentina	Law 25.326: quality, consent, information, security, rights and services on behalf of third parties.	Do not reduce rights to a generic form or disclose third-party data.
Colombia	Law 1581: principles, categories, rights, information, controllers, processors, and transfers.	Review exclusions, special rules and specific duties of each role.
Ecuador	LOPDP: principles, security, risk, protection by design and by default, incidents, and rights.	Access for response purposes does not authorize unlimited processing or perpetual retention.
Spain / EU	RGPD (GDPR): principles, design, processors, security, and breaches; national and sector-specific supplements.	Distinguish the risk threshold for notifying the authority from the high-risk threshold for communicating with data subjects; review the LOPDGDD and sector-specific rules.

Table sources:[18][19][20][21][22][23][24]

A.1 A table for selecting a legal basis, not translating legal provision numbers

For each case, first state the required function: collect data, change the purpose, engage a processor, transfer data outside the territory, respond to a rights request, report an incident, or erase data. Then consult the applicable instrument, identifying the article, subject matter, covered entity, date, and exceptions. A rule that applies only to the public, financial, or health sector must not be treated as universal. If an exception has not been verified, do not invent an answer.

The electronic-document rules of the seven legal systems help preserve evidence of decisions: recognition, attribution, integrity, originality, accessibility, and retention. However, a signature, seal, or hash does not

[18] Mexico. Federal Law on the Protection of Personal Data Held by Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and handling of rights requests. The current federal authority is the Secretaría Anticorrupción y Buen Gobierno. Official online source

[19] Peru. Law 29733 and its Regulation approved by DS 016-2024-JUS. Principles of purpose, proportionality, security, and confidentiality; the new Regulation addresses incidents, preventive assessment, and the progressive functions of the data officer. Official online source

[20] Chile. Law 21.719, which amends Law 19.628 on personal data protection. The version containing the new regime has a delayed effective date of 01-12-2026; before that date, the law then applicable must be reviewed, and future obligations must not be treated as currently in force. Official online source

[21] Argentina. Law 25.326, updated text. Articles 4–6, 9–10, 14–16, and 25: quality, information, security, confidentiality, data subjects' rights, and provision of processing services on behalf of third parties. Official online source

[22] Colombia. Statutory Law 1581 of 2012, Articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of controllers and processors, and transfers to third countries. Official online source

[23] Ecuador. Organic Law on the Protection of Personal Data, Official Registry Supplement 459 of 26-05-2021. Articles 10, 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

[24] European Union. Regulation (EU) 2016/679, Articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of security breaches. Spain also requires review of applicable national and sector-specific legislation. Official online source

make unlawful processing lawful or prove that an individual understood a notice. Privacy, record integrity, and the truthfulness of content must be assessed separately.[25][26][27][28][29][30][31]

Annex B. Templates ready to adapt

B.1 Record of processing activities

Field	Minimum content	Acceptance check
Activity and controller	Specific task, process owner, and deputy.	Another person can identify who makes the decisions.
Purpose and legal basis	Specific purpose, legal basis, and any exception.	Does not use “management” as a complete answer.
Data and individuals	Fields, sensitivity, third parties, and groups requiring priority attention.	The need for each field is explained.
Data flow and processors	Intake, systems, access, transfers, and destination.	Includes exports and backups.
Retention and rights	Retention period, blocking, deletion, and contact channel.	No “indefinite” period without a reason.
Risk and controls	Plausible harm, measures, testing, and residual risk.	Evidence of operation exists.

B.2 Data subject request form

Fictitious template for internal records

```
ID: PRIV-DEMO-2026-001
Receipt: [date, time, time zone, channel]
Verbatim request: [access, rectification, erasure, objection, other]
Identity: [proportionate method; do not include documents in this form]
Scope: [period, systems, individuals, and exclusions]
Applicable deadline: [law, article, start date, and expiry date]
Search: [systems, filters, processors, and backups]
Decision: [legal basis, review, third-party data]
Actions completed: [system, date, operator, verification]
Delivery: [format, channel, recipient, date, and verification]
Outstanding issues and limitations: [what was not resolved and why]
```

B.3 Breach timeline

Event	Required record	Associated decision
Initial signal	Source, verbatim value, time zone, person responsible, and evidence.	Open a case file and preserve evidence.

[25] Mexico. Commercial Code, Articles 89–94 and 1205: neutrality, attribution, written form, originality, integrity, accessibility, and admission of data messages. Official compilation. Official online source

[26] Colombia. Law 527 of 1999, Articles 5–13, 16–25, and 28: data messages, written form, originals, integrity, admissibility, retention, dispatch, receipt, and digital signatures. Official online source

[27] Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages, Law 67, Articles 2, 6–8, and 10–16: equivalence, written form, originals, retention, origin, dispatch, receipt, and electronic signatures. Official online source

[28] Regulation (EU) No 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination of electronic signatures and documents based on their format, advanced electronic signatures, and legal effects of qualified electronic signatures. Official online source

[29] Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, burden of proof when an electronic signature is challenged, and limited presumptions. Official online source

[30] Chile. Law 19.799 on electronic documents and electronic signatures, Articles 1–5: equivalence, written form, simple/advanced electronic signatures, date, and evidentiary value. Official online source

[31] Peru. IOFE Regulation, DS 052-2008-PCM, Articles 3 and 4: requirement for and admission of digitally signed electronic documents. Official online source

Event	Required record	Associated decision
Containment	Measure, authority, scope, effect, and prior evidence.	Limit harm without erasing context.
Scope	Data, individuals, access, copies, use, and uncertainties.	Assess risk based on facts.
Communications	Recipient, content, channel, time and version.	Comply with the local regime without disclosing more than necessary.
Recovery	Restoration, access, monitoring, and testing.	Check that the control works.
Improvement	Cause, process change, person responsible, and validation.	Prevent recurrence, not merely closure.

B.4 Provider assessment

Checklist before enabling real data

```
1. Each party’s role and the contractual purpose.
2. Minimum data, location, authorized personnel, and subprocessors.
3. Authentication, least privilege, logs, encryption, and keys.
4. Verifiable security evidence, not merely marketing claims.
5. Incident channel, content, and proof of communication.
6. Support for rights requests, searches, and native exports.
7. Transfers, safeguards, and changes of location.
8. Exit: format, data dictionary, accessibility, and file-opening test.
9. Deletion, backups, and confirmation stating its limitations.
10. Periodic review and internal owner.
```

B.5 Record of deletion or blocking

Fictitious example

```
Subject: EXP-DEMO-2026-001
Scope: marketing profile and campaign export
Action: erasure of the active profile and blocking of the required supporting document
Systems: [name, version, location, and person responsible]
Execution: [date, time zone, operator, and method]
Verification: [query, absence, access, and result]
Backup: [cycle, access, and reapplication if restored]
Processors: [notification and response]
Residual retention: [legal basis, purpose, and period]
Limitation: [what cannot be asserted]
Review: [person, date and linked evidence]
```

Annex C. Glossary and final checks

Term	Practical use in this manual
Controller	The party that decides on the legal basis and processing within the applicable regime.
Processor	The party that processes on the controller’s behalf, subject to instructions and its own duties.
Pseudonymization	Association remains possible with additional information; requires separation and controls.
Anonymization	No reasonable possibility of association in the context; requires testing and review.
Blocking	Restriction of processing without erasing the data, for a justified reason.
Portability	Structured and interoperable delivery within the permitted scope.
Breach	An incident affecting personal data security; its severity must be assessed.

Term	Practical use in this manual
Compliance evidence	A record that enables review of the decision, implementation, and result, not merely the intention.

Before closing a process	Required answer
What data and copies exist?	Inventory including files, backups, and providers.
Why is every field necessary?	Documented purpose, legal basis, and data minimization.
Who can access the data, and what evidence supports this?	Roles, logs, and testing with fictitious data.
How does an individual exercise their rights?	Channel, search, decision, delivery, and implementation.
What happens during an incident or exit?	Verified timeline, communications, export, and deletion.
What remains unknown?	Explicit limitation, person responsible, and next check.

Closure

Protecting data means reducing the likelihood that an organizational decision will harm an individual. Evidence exists to review and correct that care, not to turn it into an administrative façade.