ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

02

BAND

Angewandter Datenschutz, Sicherheit und dokumentierte Entscheidungen

Spanische Ausgabe · 2026

Handbuch zum Schutz personenbezogener Daten und zur Nachweisführung der Einhaltung

Inventar, Rechte, Anbieter, Vorfälle, Aufbewahrung und überprüfbare Löschung

Menschen durch Entscheidungen schützen, die erläutert und überprüft werden können – nicht durch kopierte Richtlinien oder Ordner voller Dokumente, die niemand in der Praxis anwendet.

Für Datenschutzverantwortliche, Rechts-, Sicherheits-, Technologie- und Personalteams, Geschäftsleitungen und Anbieter, die personenbezogene Daten verarbeiten. Enthält einen Arbeitsweg für kleine Organisationen und einen für komplexe Abläufe.

Redaktionelle Koordination: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

Allgemeine technische Anleitung und offenes Bildungsmaterial. Diese Unterlagen ersetzen keine Rechtsberatung oder forensische Begutachtung und enthalten keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Verzeichnis beim Öffnen aktualisieren; die interne Navigation der Überschriften bleibt erhalten.

Einleitung: Datenschutz muss sich in der Praxis nachweisen lassen 3
Kapitel 1. Ein Inventar als Grundlage für Entscheidungen 3
1.1 Die Verarbeitung beschreiben, ohne sie hinter einer Abkürzung zu verbergen 3
1.2 Unsichtbare Kopien aufspüren 4
Kapitel 2. Zweck, Rechtsgrundlage und Datenminimierung 5
2.1 Scheinbar gleiche Zwecke voneinander abgrenzen 5
2.2 Der Test: Welche Daten sind überflüssig? 6
2.3 Verständliche Informationen und Datenschutzhinweise 6
Kapitel 3. Rechte betroffener Personen ohne künstliche Hürden 7
3.1 Eingang, Identität und Umfang 7
3.2 Auskunft ohne Preisgabe von Daten anderer Personen 8
3.3 Wenn Löschung nicht bedeutet, alles zu vernichten 8
Kapitel 4. Nachweisbare Sicherheit 8
4.1 Risikobetrachtung vor Kontrollkatalog 8
4.2 Kontrollen und Nachweise ihrer Funktionsweise 9
4.3 Pseudonymisierung bedeutet nicht Anonymität 9
Kapitel 5. Anbieter, Cloud und Datenübermittlungen 10
5.1 Der Anbieter entlastet nicht von der Verantwortung 10
5.2 Datenfluss- und Übermittlungsübersicht 10
5.3 Kontrollierter Ausstieg und technologische Abhängigkeit 11
Kapitel 6. Datenschutzverletzungen: eindämmen, verstehen und melden 11
6.1 Erste Maßnahmen, ohne die Beweislage zu verändern 11
6.2 Entscheidung über die Meldung und aussagekräftige Inhalte 12
6.3 Schaden, Umfang und Abschluss 13
Kapitel 7. Aufbewahrung, Löschung und Datenübertragbarkeit 13
7.1 Ein Zeitplan mit Begründungen statt Willkür 13
7.2 Datenübertragbarkeit, die tatsächlich nutzbar ist 14
Kapitel 8. Drei vollständige Beispielabläufe 14
8.1 Personalwesen: der freigegebene Ordner 14
8.2 Gesundheitswesen: die Nachricht an die falsche Gruppe 15
8.3 Analytik: der Bericht, der Personen wieder identifizierbar machte 15
Anhang A. Funktionale Entsprechungen im Datenschutz 15
A.1 Die Tabelle dient der Wahl der Rechtsgrundlage, nicht der Übertragung von Artikelnummern 16
Anhang B. Vorlagen zur Anpassung 17
B.1 Verzeichnis von Verarbeitungstätigkeiten 17
B.2 Antragsformular für betroffene Personen 17
B.3 Chronologie einer Datenschutzverletzung 17
B.4 Anbieterbewertung 18
B.5 Nachweis der Löschung oder Sperrung 18
Anhang C. Glossar und Abschlusskontrolle 18

Einleitung: Datenschutz muss sich in der Praxis nachweisen lassen

Eine Datenschutzrichtlinie kann korrekt sein, während eine Organisation dennoch täglich Informationen offenlegt, die sie nicht benötigt. Die praktische Einhaltung beginnt dort, wo das Formulieren aufhört: bei einem Formular, das unnötige Daten abfragt, einem für externe Mitarbeiter freigegebenen Ordner, einem Anbieter, der eine vollständige Datenbank herunterladen kann, einer Sicherungskopie, deren Wiederherstellung niemand beherrscht, und einer Löschung, die nur auf dem Bildschirm stattfindet. Entscheidend ist nicht, ob ein Dokument vorhanden ist, sondern was mit den Daten einer bestimmten Person geschieht, von ihrer Erhebung an, bis sie nicht mehr benötigt werden.

Dieses Handbuch arbeitet mit einer einfachen Einheit: Datenelement → Zweck → Rechtsgrundlage → Zugriff → Risiko → Nachweis → endgültiger Verbleib. Für jedes Glied dieser Kette müssen konkrete Antworten vorliegen, keine Allgemeinplätze. Wenn ein Datensatz einen Verkauf belegen soll, muss festgelegt werden, welche Felder für diesen Zweck erforderlich sind, wer sie verwaltet, wie lange sie aufbewahrt werden und welche weiteren Informationen zusammen mit ihnen erfasst wurden. Kommt ein neuer Zweck hinzu, genügt es nicht, den Ordner umzubenennen: Rechtmäßigkeit, Information der betroffenen Person und Umfang des Zugriffs müssen überprüft werden.

Auch ein Nachweis der Einhaltung besteht nicht darin, Bildschirmfotos zu sammeln, um Arbeit vorzutäuschen. Aufzubewahren sind vielmehr die Version einer Entscheidung, die Quelle ihrer Begründung, die Person, die sie genehmigt hat, die angewandte Kontrolle und das Ergebnis ihrer Überprüfung. Die verglichenen Rechtsvorschriften dienen nicht dazu, eine Richtlinie aus einem anderen Land zu kopieren. Sie helfen, die Funktion zu bestimmen, die die Organisation dokumentieren muss: Datenminimierung, Sicherheit, Transparenz, Rechte, Auftragsverarbeiter, Vorfall oder Datenübermittlung. Rechtsgrundlage und Fristen müssen stets für das Gebiet, den Sektor und den Zeitpunkt der Verarbeitung geprüft werden.

> **Erste Entscheidung**
> Bevor Sie ein Werkzeug kaufen oder eine weitere Richtlinie verfassen, wählen Sie einen realen Prozess aus und durchlaufen Sie ihn mit fiktiven Daten. Können Sie nicht erklären, welche Informationen eingehen, weshalb dies geschieht, wer sie einsehen kann, wo sie verbleiben und wie ein Recht ausgeübt wird, haben Sie Ihre erste konkrete Arbeitsaufgabe gefunden.

Kapitel 1. Ein Inventar als Grundlage für Entscheidungen

1.1 Die Verarbeitung beschreiben, ohne sie hinter einer Abkürzung zu verbergen

Ein brauchbares Inventar beginnt nicht mit „Kundendatenbank“, denn diese Bezeichnung kann Vertrieb, Support, Forderungseinzug, Marketing und Personalauswahl vermischen. Ausgangspunkt ist eine verständliche Tätigkeit: einen Kauf erfassen, eine Garantie abwickeln, eine Bewerbung prüfen, Gehälter auszahlen, eine Anfrage beantworten oder die Sicherheit eines Gebäudes gewährleisten. Für jede Tätigkeit werden der konkrete Zweck, die erforderlichen Felder, die betroffenen Personen, das System, die zuständige Stelle, der Eingangskanal und der vorgesehene Verbleib festgehalten.

Die Klassifizierung muss die möglichen Folgen abbilden, nicht nur die Bezeichnung der Sensibilität. Name und Telefonnummer können in einem Kontaktverzeichnis ein geringes Risiko darstellen, aber ein

hohes, wenn sie den Aufenthaltsort einer bedrohten Person verraten. Die Akte einer Untersuchung kann Identität, Gesundheit, wirtschaftliche Situation, Kommunikation und Daten unbeteiligter Dritter zusammenführen. Die Kennzeichnung „vertraulich“ genügt nicht: Festzulegen ist, wer die Daten verwenden darf, mit welchen Kontrollen, für welche Entscheidung und wie lange. Der Kontext kann eine Kombination scheinbar gewöhnlicher Daten zu einem intimen Profil machen.

Feld des Inventars	Operative Frage	Ein fiktives Beispiel
Aktivität	Welche konkrete Aufgabe wird ausgeführt?	Abwicklung der Garantie für ein online gekauftes Gerät.
Mindestdaten	Welche Felder sind für ihre Erfüllung erforderlich und welche sind nur ergänzend?	Bestellung, Kontaktdaten, Lieferadresse und Diagnose; kein beruflicher Werdegang.
Personen	Betroffene Personen, Dritte, Minderjährige oder besonders schutzbedürftige Gruppen?	Käufer, Paketempfänger und zugewiesener Techniker.
Datenfluss	Woher stammen die Daten und an wen werden sie weitergegeben?	Shop → Supportplattform → Paketdienst; keine öffentliche Verbreitung.
Verwahrung und Aufbewahrungsfrist	Wer entscheidet darüber und wann werden die Daten nicht mehr benötigt?	Verantwortliche Stelle für den After-Sales-Service; die Frist richtet sich nach dem Vorgang und nachweisbaren Pflichten.
Nachweis	Wie werden die Entscheidung und ihre Umsetzung nachgewiesen?	Version des Datenschutzhinweises, Rollen, Protokolle, Vertrag und Löschaufzeichnung.

1.2 Unsichtbare Kopien aufspüren

Das Inventar muss Exporte, E-Mail-Anhänge, eingescannte Papierdokumente, persönliche Ordner, Anwendungsprotokolle, Sicherungskopien und Dienste Dritter erfassen. Die offizielle Datenbank kann kontrolliert sein, während eine Excel-Datei ohne Eigentümer und Löschdatum per Messenger kursiert. Dass eine solche Kopie als „vorübergehend“ bezeichnet wird, ändert nichts daran, dass sie einer Verarbeitung unterliegt. Dokumentiert wird, wer sie erstellt hat, warum sie erforderlich war, wo sie verblieben ist, wer sie öffnen kann und wie sie nach Erfüllung ihres Zwecks entfernt wird.

Bei einer guten Bestandsaufnahme wird nicht nur gefragt, welches System ein Bereich nutzt. Eine Person soll einen vollständigen Arbeitstag mit fiktiven Informationen nachstellen: wie eine Anfrage eingeht, was sie herunterlädt, an wen sie etwas weiterleitet, wo sie Notizen speichert, was bei einem Fehler geschieht und was sie vor ihrem Urlaub tut. Der tatsächliche Datenfluss zeigt sich in den Ausnahmen. Passwörter werden nicht im Inventar festgehalten; erfasst werden der Kontrollmechanismus und die dafür verantwortliche Person.

> **Abschlusskontrolle**
> Kein Prozess darf mit der Formulierung „und andere erforderliche Daten“ abgeschlossen werden. Felder, Quelle, Empfänger und Zweck sind anzugeben. Unbekanntes wird zur Prüfung gekennzeichnet und nicht durch ein beruhigendes Kontrollkästchen ersetzt.



Abbildung 1. Vom Datenelement bis zum endgültigen Verbleib. Jede Entscheidung hinterlässt eine Quelle und eine Überprüfung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Nachweis dar.

Kapitel 2. Zweck, Rechtsgrundlage und Datenminimierung

2.1 Scheinbar gleiche Zwecke voneinander abgrenzen

Der Verkauf eines Produkts, der Versand von Werbung und die Erstellung eines Verhaltensprofils sind nicht ein und derselbe Zweck. Der Verkauf kann für eine Vertragsbeziehung erforderlich sein; die beiden anderen Zwecke erfordern jeweils eine eigene Prüfung. Wenn eine Organisation Zwecke in einer Formulierung wie „zu administrativen und kommerziellen Zwecken“ vermischt, lässt sich nicht mehr bestimmen, welche Daten wirklich erforderlich sind und welche Kommunikation gesondert erläutert werden muss. Diese Trennung muss im Verzeichnis erhalten bleiben, damit eine Person einer Nutzung widersprechen kann, ohne dadurch ungerechtfertigt die wesentliche Dienstleistung zu verlieren.

Die Einwilligung ist eine mögliche Rechtsgrundlage, aber kein Universalschlüssel. Es kann auch eine rechtliche Verpflichtung, die Durchführung einer Vertragsbeziehung, die Wahrnehmung öffentlicher Aufgaben, die Geltendmachung von Rechten oder ein anderer in der jeweiligen Rechtsordnung vorgesehener Tatbestand vorliegen. Die konkrete Vorschrift ist vor der Auswahl eines Formulars zu bestimmen. Eine pauschale Einholung von Einwilligungen kann die Verantwortung fälschlich auf die betroffene Person verlagern und einen Vorgang unübersichtlich machen, für den bereits eine andere Rechtsgrundlage besteht. Ändert sich die Verarbeitung, sind vor ihrer Durchführung die Vereinbarkeit, die Informationen und die Kontrollen zu überprüfen.

In Mexiko gelten die Grundsätze der Rechtmäßigkeit, Zweckbindung, Treue, Einwilligung, Datenqualität, Verhältnismäßigkeit, Information und Rechenschaftspflicht; Kolumbien konkretisiert Rechtmäßigkeit, Zweckbindung, Freiheit, Datenqualität, Transparenz, beschränkten Zugang, Sicherheit und Vertraulichkeit; Ecuador verlangt eine aktive und nachweisbare Rechenschaftspflicht. Die Ähnlichkeit

dieser Grundsätze erleichtert die Entwicklung einer Methode, doch jeder Tatbestand und jede Ausnahme muss anhand der einschlägigen Rechts- und Sektorvorschriften geprüft werden.[123]

2.2 Der Test: Welche Daten sind überflüssig?

Nehmen Sie ein Feld aus dem fiktiven Beispiel heraus. Lässt sich die Tätigkeit auch ohne dieses Feld ausführen, müssen Sie begründen, warum es abgefragt wird. Maßgeblich ist nicht, ob es künftig interessant sein könnte, sondern ob es für den aktuellen Zweck geeignet und erforderlich ist. Für einen Lieferhinweis kann eine Telefonnummer genügen; eine Kopie des Ausweises ist nicht erforderlich, wenn die Identität mit einem weniger eingriffsintensiven Mittel überprüft werden kann. Für eine statistische Auswertung muss der Name möglicherweise nicht zusammen mit dem Ergebnis aufbewahrt werden.

Situation	Entscheidung zur Datenminimierung	Aufzeichnung, die Improvisation vermeidet
Support zu einem Kauf	Bestellung und Kontaktkanal, keine vollständige Kundenakte.	Genehmigte Felder und Bildschirmfoto des aktuellen Formulars.
Identitätsprüfung	Wählen Sie die am wenigsten eingriffsintensive Methode, die das erforderliche Sicherheitsniveau gewährleistet.	Bewertete Alternativen, Risiko und Genehmigung.
Aggregierter Bericht	Identifikatoren entfernen und Kombinationen auf Reidentifizierbarkeit prüfen.	Prüfung von Kleingruppen und angewandte Suppression.
Anfrage Dritter	Daten der antragstellenden Person von Daten anderer Personen trennen.	Übermittelte Version und vorherige inhaltliche Prüfung.
Neuer Zweck	Bis zur Prüfung von Vereinbarkeit und Rechtsgrundlage aussetzen.	Antrag, Analyse und datierte Genehmigung.

2.3 Verständliche Informationen und Datenschutzhinweise

Der Datenschutzhinweis muss für die betroffene Person erkennbar machen, wer über die Verarbeitung entscheidet, zu welchen Zwecken ihre Daten verwendet werden, mit wem sie geteilt werden, wie sie ihre Rechte ausüben kann und an wen sie sich mit Fragen wenden kann. Ein langer Text ersetzt keine rechtzeitige Erklärung. Aufzubewahren sind die tatsächlich angezeigte Fassung und ihr Kontext: Seite, Datum, Ablauf, Sprache und Änderungen. Bei einer Änderung der Website darf die frühere Fassung nicht aus den Compliance-Aufzeichnungen gelöscht werden.

In Argentinien müssen vorab der Zweck, die Empfänger oder Empfängerkategorien, der Verantwortliche und die Möglichkeit der Rechtsausübung angegeben werden. In Kolumbien bestehen bei der Einholung der Einwilligung eine Pflicht zu klarer und ausdrücklicher Information sowie eine Pflicht zur Aufbewahrung des Nachweises ihrer Erfüllung. Diese Beispiele zeigen, warum der Nachweis Text und

[1]Mexiko. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, veröffentlichter Text vom 20-03-2025 und Reform vom 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Datenschutzverletzungen und Bearbeitung von Anträgen auf Rechtsausübung. Derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno. Offizielle Online-Quelle

[2]Kolumbien. Ley Estatutaria 1581 de 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Informationen, Pflichten der Verantwortlichen und Auftragsverarbeiter sowie Datenübermittlungen in Drittländer. Offizielle Online-Quelle

[3]Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Verarbeitung bei Vorfällen. Offizielle Online-Quelle

Kontext verbinden muss: Eine aktuelle URL belegt nicht, was die betroffene Person Jahre zuvor gesehen hat.[45]

> **Fiktiver Fall: die Werbeaktion, die eine ganze Akte verlangte**
> Ein Händler verlangt einen amtlichen Ausweis, den Familienstand und die Anschrift, um einen digitalen Gutschein auszustellen. Am Ende der Prüfung steht eine Fassung, die die E-Mail-Adresse und eine gesonderte Einwilligung in Werbung abfragt, aber keine Ausweiskopie. Dokumentiert wird, welche Daten nicht mehr erhoben werden und wie die Organisation mit den bereits erhaltenen Kopien verfährt. Die Verbesserung des Formulars erlaubt es nicht, die Vergangenheit zu ignorieren.

Kapitel 3. Rechte betroffener Personen ohne künstliche Hürden

3.1 Eingang, Identität und Umfang

Der Kanal für die Ausübung von Rechten benötigt eine Registrierung mit Angaben zu Datum, mutmaßlicher antragstellender Person, Art und Umfang der Anfrage, zuständiger Person, geltender Frist und Status. Die Identitätsprüfung muss verhältnismäßig sein: Die pauschale Forderung nach einer umfangreichen Akte kann ein Hindernis schaffen und zusätzliche Daten offenlegen. Zu prüfen ist, über welche Informationen die Organisation bereits zur Authentifizierung der Anfrage verfügt, welches Risiko eine Übermittlung an eine andere Person hätte und welche alternativen Prüfmöglichkeiten der Kanal bietet.

Anschließend ist abzugrenzen, was die Person tatsächlich verlangt: zu erfahren, ob eine Verarbeitung stattfindet, eine Kopie zu erhalten, Daten zu berichtigen, Werbung zu widersprechen, Daten löschen oder sperren zu lassen, eine Einwilligung zu widerrufen, Daten zu übertragen oder eine Beschwerde vorzubringen. Nicht jede Anfrage darf in eine vollständige Löschung umgedeutet oder mit „unzulässig“ beantwortet werden, ohne Grund und Überprüfungsmöglichkeit zu erläutern. Enthält die Antwort Daten Dritter, ist eine Fassung bereitzustellen, die deren Rechte wahrt, ohne eine Tilgung von Tatsachen in der Originalakte vorzutäuschen.

Verfahrensschritt	Was dokumentiert wird	Zu vermeidender Fehler
Eingang	Kanal, Datum und Zeitzone, wörtlicher Inhalt und Empfangsbestätigung.	Die Frist erst ab dem Zeitpunkt berechnen, an dem jemand beschließt, die E-Mail zu prüfen.
Identität	Gewählte Methode, Risiko und verwendete Daten; keine Geheimnisse im Formular.	Eine unnötige neue Ausweiskopie anfertigen.
Datensuche	Systeme, Sicherungskopien, Auftragsverarbeiter und Suchkriterien.	Antwort ausschließlich auf Grundlage der Hauptdatenbank erteilen.
Entscheidung	Rechtsgrundlage, Ausnahmen, Prüfung und übermittelte Daten.	Daten Dritter übermitteln oder ohne Begründung ablehnen.
Abschluss	Datum, Kanal, Zustellnachweis und durchgeführte Systemmaßnahmen.	Als erledigt markieren, ohne die Änderung umzusetzen.

[4] Argentinien. Ley 25.326, aktualisierter Text. Artikel 4–6, 9–10, 14–16 und 25: Datenqualität, Information, Sicherheit, Vertraulichkeit, Rechte betroffener Personen und Erbringung von Verarbeitungsdienstleistungen im Auftrag Dritter. Offizielle Online-Quelle

[5] Kolumbien. Ley Estatutaria 1581 de 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Informationen, Pflichten der Verantwortlichen und Auftragsverarbeiter sowie Datenübermittlungen in Drittländer. Offizielle Online-Quelle

3.2 Auskunft ohne Preisgabe von Daten anderer Personen

Ein Export kann Daten von Beschäftigten, Kunden, Angehörigen oder Gesprächsteilnehmern enthalten. Das Auskunftsrecht berechtigt nicht automatisch zu ihrer Offenlegung. Felder, Identifikatoren, Inhalte, Anhänge und Metadaten sind zu prüfen; für die Übermittlung wird eine von dem unverändert aufbewahrten Original getrennte Fassung verwendet. Die Prüfung darf weder die Bedeutung verändern noch Informationen vorenthalten, die der antragstellenden Person selbst zustehen.

In Argentinien müssen die Informationen klar und umfassend sein und dürfen keine Daten Dritter offenlegen, selbst wenn diese mit der betroffenen Person verbunden sind. Für Berichtigung, Aktualisierung oder Löschung gelten eigene Regeln und Fristen sowie Ausnahmen bei Aufbewahrungspflichten oder Rechten Dritter. Diese Fristen werden nicht auf andere Länder übertragen; das für den Fall geltende Rechtsregime wird dokumentiert.[6]

3.3 Wenn Löschung nicht bedeutet, alles zu vernichten

Ein Löschverlangen kann neben einer Aufbewahrungspflicht oder der Verteidigung eines Rechts bestehen. In der Antwort sind die einzustellende Verarbeitung, der zu sperrende Datensatz, die mit eingeschränktem Zugriff aufzubewahrende Kopie und die jeweilige Rechtsgrundlage zu unterscheiden. Die Maßnahmen sind in den Systemen und bei den Auftragsverarbeitern umzusetzen, nicht nur im Antwortschreiben zu beschreiben. Wird eine Datenbank zur Rechtsverteidigung aufbewahrt, ist ihre Nutzung auf diesen Zweck zu beschränken und der spätere Zugriff zu kontrollieren.

> **Ein fiktives Beispiel**
> Eine Person verlangt nach Schließung ihres Kontos die Löschung aller ihrer Daten. Die Organisation bewahrt den erforderlichen Steuerbeleg auf, sperrt ihr Marketingprofil, löscht Segmentierungsattribute und dokumentiert die Systeme, in denen die einzelnen Maßnahmen ausgeführt wurden. Die Antwort erläutert, was gelöscht, gesperrt und aufbewahrt wurde, ohne zu behaupten, alles sei verschwunden.

Kapitel 4. Nachweisbare Sicherheit

4.1 Risikobetrachtung vor Kontrollkatalog

Die Analyse geht von den betroffenen Personen und den möglichen Schäden aus, nicht von einer Produktliste. Zu bestimmen ist, wer Zugriff erlangen könnte, welche Fehler plausibel sind, welche Kopie am stärksten gefährdet ist und welche Folgen Veränderung, Verlust, Nichtverfügbarkeit oder Offenlegung hätten. Anschließend werden Kontrollen für Zugriff, Verschlüsselung, Protokollierung, Trennung, Datensicherung, Schulung und Überprüfung ausgewählt. Eine kostspielige Kontrolle kann für ein öffentliches Verzeichnis unverhältnismäßig und für eine Patientenakte unzureichend sein.

Ecuador verlangt eine Analyse von Risiken, Bedrohungen und Schwachstellen unter Berücksichtigung der Verarbeitung, der betroffenen Personen sowie der Kategorien und des Umfangs der Daten. Die Europäische Union verlangt risikoangemessene technische und organisatorische Maßnahmen sowie Datenschutz durch Technikgestaltung und Voreinstellungen. Die Dokumentation dieser Bewertung ist

[6] Argentinien. Ley 25.326, aktualisierter Text. Artikel 4–6, 9–10, 14–16 und 25: Datenqualität, Information, Sicherheit, Vertraulichkeit, Rechte betroffener Personen und Erbringung von Verarbeitungsdienstleistungen im Auftrag Dritter. Offizielle Online-Quelle

aussagekräftiger als die Behauptung „wir erfüllen die höchsten Standards“, weil sie erläutert, warum jede Maßnahme gewählt wurde und welches Restrisiko die Organisation akzeptiert hat.[78]

4.2 Kontrollen und Nachweise ihrer Funktionsweise

Kontrolle	Test mit fiktiven Informationen	Aufbewahrte Nachweise
Prinzip der minimalen Berechtigungen	Ein Supportmitarbeiter darf weder Gehaltsabrechnungen öffnen noch die gesamte Datenbank herunterladen.	Rolle, Berechtigung, Ergebnis des Zugriffsversuchs und Zugriffsüberprüfung.
Verschlüsselung und Schlüssel	Eine Kopie wird verschlüsselt und kann nur von einer berechtigten Rolle wiederhergestellt werden.	Konfiguration, Verantwortlichkeiten, Wiederherstellung und Fehlen von Schlüsseln im Protokoll.
Protokolle	Eine Testaktion erzeugt ein Ereignis mit Benutzer, Datum, Zeitzone und Objekt.	Nativer Export, Datenwörterbuch, Aufbewahrung und Überprüfung.
Datensicherung	Ein fiktiver Datensatz wird in einer isolierten Umgebung wiederhergestellt.	Datum, Dauer, aufgetretene Probleme, Hashwert und Öffnungstest.
Austritt von Personal	Der Zugriff wird zurückgezogen und überprüft, dass er nicht mehr funktioniert.	Austrittsdatum, geprüfte Systeme und Verantwortlicher.
Anonymisierung	Es wird versucht, Datensätze anhand von Kombinationen und Extremwerten zu identifizieren.	Methode, Restrisiko, Test und Genehmigung der Verbreitung.

Nachweise müssen die Funktionsweise belegen, nicht lediglich das Vorhandensein. Ein Bildschirmfoto einer verschlüsselten Konsole beweist nicht, dass alle Kopien geschützt sind; eine Passwortrichtlinie belegt nicht, dass Berechtigungen überprüft werden; ein Ordner mit der Bezeichnung „Datensicherung“ belegt keine Wiederherstellbarkeit. Der Test wird mit fiktiven Daten so konzipiert, dass nicht bei der Bewertung einer Datenschutzverletzung eine neue verursacht wird. Funktioniert ein unerwarteter Zugriff tatsächlich, wird das Ereignis aufbewahrt und der Fehler vor Veröffentlichung des Berichts behoben.

4.3 Pseudonymisierung bedeutet nicht Anonymität

Die Ersetzung von Namen durch Fallnummern verringert die direkte Offenlegung, doch die Identität kann durch die Kombination von Datum, Anschrift, Position, Hobbys oder einem einmaligen Vorgang wieder erkennbar werden. Bei der Pseudonymisierung bleibt eine Zuordnung mithilfe zusätzlicher Informationen möglich; die Anonymisierung erfordert eine Analyse des Reidentifizierungsrisikos im tatsächlichen Verbreitungskontext. In der Dokumentation sind die Arbeitsfassung und die öffentliche Fassung zu trennen; die Zuordnungstabelle ist mit eigenen Kontrollen zu schützen.

Bevor Sie einen Datensatz weitergeben, prüfen Sie kleine Gruppen, einmalige Werte, Anhänge, Koordinaten, Sequenzen und Metadaten. Auch ein Bericht ohne Namen kann eine Person über den Ortsnamen und ihre Position identifizierbar machen. In diesem Fall werden Angaben verallgemeinert, entfernt oder nicht veröffentlicht. Versprechen Sie keine vollkommene Anonymität: Dokumentieren Sie Methode, Annahmen, Restrisiko und eine erneute Prüfung für den Fall, dass sich der Kontext ändert.

[7] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Verarbeitung bei Vorfällen. Offizielle Online-Quelle

[8] Europäische Union. Reglamento (UE) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit sowie Meldung/Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten. Für Spanien sind außerdem die einschlägigen nationalen und sektoralen Rechtsvorschriften zu prüfen. Offizielle Online-Quelle

Praktische Regel

Beurteilen Sie die Wirksamkeit einer Anonymisierung nicht mit der Frage „Sehe ich einen Namen?“. Fragen Sie, welche anderen Quellen jemand vernünftigerweise kombinieren könnte und welche Person durch ein seltenes Merkmal identifizierbar würde.



Tests mit fiktiven Daten und aufbewahrte Ergebnisse

Kontrolle	Test	Nachweis
Minimale Berechtigungen	Eine Supportrolle versucht, Gehaltsabrechnungen zu öffnen.	Rolle, verweigerter Zugriffsversuch und Protokolleintrag.
Datensicherung	Eine fiktive Datei wird in einer isolierten Umgebung wiederhergestellt.	Öffnungstest, Datum, aufgetretene Probleme und Hashwert.
Austritt von Personal	Ein deaktiviertes Konto versucht, sich zu authentifizieren.	Deaktivierung, geprüfte Systeme und Ergebnis.
Anonymisierung	Eine einzigartige Kombination wird getestet.	Restrisiko und Entscheidung über die Veröffentlichung.

Die Abbildung erläutert Entscheidungen und Zusammenhänge; sie stellt keine Beweise aus einem echten Fall dar.

Abbildung 2. Eine Richtlinie beweist nicht, dass eine Kontrolle funktioniert. Tests mit fiktiven Daten und aufbewahrte Ergebnisse. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Nachweis dar.

Kapitel 5. Anbieter, Cloud und Datenübermittlungen

5.1 Der Anbieter entlastet nicht von der Verantwortung

Verarbeitet ein Anbieter Daten im Auftrag der Organisation, sind Weisungen, Zweck, befugtes Personal, Standort, Subunternehmer, Vertraulichkeit, Sicherheitsmaßnahmen, Unterstützung bei Vorfällen und bei der Wahrnehmung von Rechten, Rückgabe, Löschung und die für Prüfungen verfügbaren Nachweise festzulegen. Ein Vertrag allein genügt nicht: Es muss bekannt sein, welche Schaltfläche den Download der Datenbank ermöglicht, wer sie wiederherstellen darf und wo sich die Zugriffsprotokolle befinden.

In Argentinien darf ein Dienstleister, der IT-Dienstleistungen im Auftrag Dritter erbringt, die Daten weder für einen anderen als den vertraglich vereinbarten Zweck verwenden noch zur Aufbewahrung an Dritte übertragen; nach Erfüllung der Leistung gilt das gesetzliche Regime für Vernichtung oder zulässige Aufbewahrung. In Kolumbien wird zwischen Verantwortlichem und Auftragsverarbeiter unterschieden und beiden werden besondere Pflichten zugewiesen. Die vertragliche Einordnung muss den tatsächlichen Entscheidungsbefugnissen der Parteien entsprechen, nicht der kommerziellen Bezeichnung des Dienstes.[9][10]

5.2 Datenfluss- und Übermittlungsübersicht

Eine Cloud kann die Verwaltung in einem Land, die Speicherung in einem zweiten, den Support in einem dritten und Sicherungskopien in mehreren Ländern umfassen. Die Übersicht erfasst diese Wege, die

[9] Argentinien. Ley 25.326, aktualisierter Text. Artikel 4–6, 9–10, 14–16 und 25: Datenqualität, Information, Sicherheit, Vertraulichkeit, Rechte betroffener Personen und Erbringung von Verarbeitungsdienstleistungen im Auftrag Dritter. Offizielle Online-Quelle

[10] Kolumbien. Ley Estatutaria 1581 de 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Informationen, Pflichten der Verantwortlichen und Auftragsverarbeiter sowie Datenübermittlungen in Drittländer. Offizielle Online-Quelle

entscheidende Stelle, Auftragsverarbeiter und weitere Unterauftragsverarbeiter, den Grund jedes Zugriffs sowie die Garantie oder den Mechanismus, den die Rechtsvorschriften verlangen. „Der Server befindet sich in der Cloud“ beschreibt weder Standort noch Risiko. Eine internationale Datenübermittlung beschränkt sich nicht auf das Kopieren einer Vertragsklausel: Geltungsbereich, Ausnahmen, Empfänger und Kontrollen sind zu überprüfen.

Frage an den Anbieter	Erwartete dokumentierte Antwort	Warnsignal
Wer kann zugreifen?	Rollen, Standort, Authentifizierung, Protokollierung und Überprüfung.	„Globaler Support“ ohne Angaben zu Personen oder Bedingungen.
Welche Unterauftragsverarbeiter sind beteiligt?	Identität, Funktion, Standort und Verfahren für Änderungen.	Geheime Liste oder Änderungen ohne Vorankündigung.
Wie unterstützt der Anbieter die Rechtsausübung?	Auskunft, Berichtigung, Sperrung, Export und Fristen.	Nur PDF ohne Such- oder Filterfunktionen.
Wie übermittelt der Anbieter Informationen zu Vorfällen?	Kanal, Kontakt, Chronologie, Nachweise und Aktualisierungen.	Mündliche Mitteilung ohne Dokumentation.
Wie endet die Beziehung?	Export, Lesbarkeit, Löschung, Sicherungskopien und Nachweis.	Kontoschließung ohne Wiederherstellbarkeit der Daten.

5.3 Kontrollierter Ausstieg und technologische Abhängigkeit

Vor der Beauftragung wird der Ausstieg mit fiktiven Daten getestet. Ein Export wird heruntergeladen, mit einem unabhängigen Werkzeug geöffnet und darauf geprüft, ob Felder, Zeitzone, Beziehungen und Datenwörterbuch erhalten bleiben. Erlaubt die Plattform lediglich den Druck, wird das Abhängigkeitsrisiko ausgewiesen. Zum Ausstieg gehören außerdem die Löschung in der Produktivumgebung sowie die Entfernung von Testkopien, Sicherungskopien und Protokollen; einzelne Bestandteile dürfen aus rechtlichen oder Sicherheitsgründen aufbewahrt werden, ihr Umfang muss jedoch abgegrenzt werden.

> **Fiktiver Fall**
> Eine Organisation wechselt den Anbieter für Umfragen. Der Export enthält Antworten, aber weder Formular-IDs noch Zeitzone. Es wird eine neue Lieferung mit Datenwörterbuch angefordert; beide Exporte werden als getrennte Objekte aufbewahrt und die Einschränkung des ersten wird dokumentiert. Abschließend wird das Konto gelöscht und ein Nachweis über den tatsächlichen Umfang dieser Maßnahme eingeholt.

Kapitel 6. Datenschutzverletzungen: eindämmen, verstehen und melden

6.1 Erste Maßnahmen, ohne die Beweislage zu verändern

Das vorrangige Ziel ist, Menschen zu schützen und den Schaden zu begrenzen, ohne Informationen zu vernichten, die den Vorfall erklären. Dokumentiert werden der Zeitpunkt der Entdeckung, die meldende Person, die offenbar betroffenen Systeme, die möglicherweise betroffenen Daten und die bereits erfolgten Maßnahmen. Passwörter werden über einen sicheren Kanal geändert; zuvor werden die relevanten Zugriffsereignisse gesichert. Die Wiederherstellung darf weder zur Vernichtung von Beweisen dienen noch als Grundlage für die voreilige Aussage, der Vorfall sei abgeschlossen.

NIST SP 800-61 Rev. 3 gliedert die Reaktion in Vorbereitung, Erkennung, Reaktion, Wiederherstellung und kontinuierliche Verbesserung. Dadurch wird eine zu enge Sichtweise vermieden: Ein Vorfall beschränkt sich nicht auf den Moment, in dem „der Server abgeschaltet wird“; Umfang, Kommunikation, Auswirkungen auf Menschen und spätere Änderungen müssen ebenfalls berücksichtigt werden. Bei einer Datenschutzverletzung ist außerdem zu dokumentieren, welche Felder mit welcher Genauigkeit offengelegt wurden und welche Kopien ein Dritter erlangt haben konnte.[1112]

Zeitpunkt	Dokumentierte Maßnahme	Nicht unüberlegt handeln
Erkennung	Signal, Quelle, Uhrzeit, Verantwortlichen und erste Einschätzung des Umfangs erfassen.	Die Grundursache allein aufgrund des ersten Verdachts festlegen.
Eindämmung	Eine verhältnismäßige Maßnahme wählen und zuvor vorhandene Beweise dokumentieren.	Geräte zurücksetzen oder Konten löschen, ohne Protokolle zu exportieren.
Bewertung	Daten, betroffene Personen, Zugriffe, Nutzung und plausible Folgen bestimmen.	Die Zahl der Zeilen mit der Zahl der betroffenen Personen verwechseln.
Meldung	Meldepflichtigen, Meldeschwelle, Empfänger, Inhalt und lokale Frist bestimmen.	Fristen von 72 oder 48 Stunden ungeprüft auf alle Länder und Branchen übertragen.
Wiederherstellung	Kontrollen, Überwachung, Unterstützung der Betroffenen und Änderungen überprüfen.	Den Vorgang mit einem neuen Ordner abschließen, ohne daraus zu lernen.

6.2 Entscheidung über die Meldung und aussagekräftige Inhalte

Die Meldung richtet sich nach dem geltenden Recht, der Art der Organisation, Art und Schwere des Vorfalls sowie den betroffenen Personen. In Mexiko verlangt das im Jahr 2026 geltende Gesetz, erhebliche Datenschutzverletzungen den Betroffenen unverzüglich mitzuteilen, damit sie ihre Rechte wahren können. In Peru führt die 2024 erlassene Verordnung eine zeitnahe Meldung von Vorfällen an die Behörde und eine Mitteilung an Betroffene je nach Exposition ein; die offizielle Quelle nennt grundsätzlich 48 Stunden, es sei denn, begründete Umstände sprechen dagegen. In der Europäischen Union unterscheiden die Artikel 33 und 34 zwischen der Meldung an die Aufsichtsbehörde und der Benachrichtigung der betroffenen Person je nach Risiko. Diese Regeln sind nicht austauschbar.[131415]

Ein nützlicher Hinweis erläutert nach dem aktuellen Kenntnisstand, was geschehen ist, welche Datenkategorien betroffen sein könnten, welche Maßnahmen ergriffen werden, was die betroffene Person sinnvollerweise tun kann und wo sie Informationen erhält. Er enthält weder Geheimnisse noch spekulative Aussagen über den Angreifer. Ändern sich die Erkenntnisse, wird der Hinweis aktualisiert und der Verlauf aufbewahrt. Ein Vorfall, der aus Rücksicht auf den Ruf verschwiegen wird, kann den Schaden vervielfachen, der eigentlich vermieden werden sollte.

[11]NIST SP 800-61 Rev. 3 (April 2025). In CSF 2.0 integrierte Empfehlungen für die Reaktion auf Vorfälle: Vorbereitung, Erkennung, Reaktion, Wiederherstellung und Verbesserung. Ersetzt Revision 2. Offizielle Online-Quelle

[12]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die gerichtliche Zulässigkeit. Offizielle Online-Quelle

[13]Mexiko. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, veröffentlichter Text vom 20-03-2025 und Reform vom 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Datenschutzverletzungen und Bearbeitung von Anträgen auf Rechtsausübung. Derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno. Offizielle Online-Quelle

[14]Peru. Ley 29733 und die zugehörige, durch DS 016-2024-JUS genehmigte Verordnung. Grundsätze der Zweckbindung, Verhältnismäßigkeit, Sicherheit und Vertraulichkeit; die neue Verordnung konkretisiert Vorfälle, vorbeugende Bewertungen und die schrittweise ausgestalteten Funktionen des Datenschutzbeauftragten. Offizielle Online-Quelle

[15]Europäische Union. Reglamento (UE) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit sowie Meldung/Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten. Für Spanien sind außerdem die einschlägigen nationalen und sektoralen Rechtsvorschriften zu prüfen. Offizielle Online-Quelle

6.3 Schaden, Umfang und Abschluss

Die Bewertung berücksichtigt die Missbrauchsmöglichkeit, die Vertraulichkeit der Zugangsdaten, die Möglichkeit, betroffene Personen zu kontaktieren, deren besondere Schutzbedürftigkeit, die Öffentlichkeit des Zugriffs sowie körperliche, wirtschaftliche oder diskriminierende Folgen. „Es waren nur Namen“ kann schwerwiegend sein, wenn diese mit einer sensiblen Betreuungseinrichtung verknüpft werden. Die Beweiserhebung erfolgt, ohne die durchgesickerten Daten erneut über einen öffentlichen Link herunterzuladen oder an das gesamte Team zu verteilen.

Tatsächlicher Abschluss

Ein Vorfall ist nicht mit der Wiederherstellung des Systems abgeschlossen. Abgeschlossen ist er erst, wenn Personen entsprechend den Vorgaben informiert wurden, Kontrollen überprüft und Zugriffe untersucht wurden, Beweise gesichert sind und der Prozess so geändert wurde, dass sich derselbe Ablauf nicht wiederholt. Bleibt etwas unbekannt, wird dies im Bericht ausdrücklich als Einschränkung festgehalten.



Abbildung 3. Datenschutzverletzung: eindämmen, ohne die Spuren des Vorfalls zu löschen. Die Chronologie leitet die Reaktion und die Meldung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Nachweis dar.

Kapitel 7. Aufbewahrung, Löschung und Datenübertragbarkeit

7.1 Ein Zeitplan mit Begründungen statt Willkür

Die Aufbewahrungsdauer richtet sich nach Zweck, rechtlicher Verpflichtung, Vertrag, Rechtsverteidigung und betrieblicher Notwendigkeit. Es gibt keine allgemeingültige Zahl für „personenbezogene Daten“. Die normale Nutzungsdauer ist von der eingeschränkten Sperrung und der Aufbewahrung zu Beweiszwecken zu unterscheiden. Ändert sich der Zweck, wird der Zeitplan überprüft. Alles für alle Fälle aufzubewahren erhöht das Risiko einer Offenlegung und erschwert präzise Antworten auf Anfragen.

Die Löschung muss Systeme, Exporte, Benutzer, Anbieter und verfügbare Kopien einbeziehen. Für Sicherungskopien kann ein anderer technischer Zyklus gelten: Dokumentiert wird, ob sie gelöscht, überschrieben oder bis zum Ablauf unzugänglich aufbewahrt werden. Kann eine Wiederherstellung

gelöschte Daten erneut einführen, muss das Verfahren auch ihre erneute Löschung regeln. Es wird kein Nachweis ausgestellt, der über die tatsächlich erfolgten technischen Maßnahmen hinausgeht.

7.2 Datenübertragbarkeit, die tatsächlich nutzbar ist

Daten bereitzustellen bedeutet nicht, sie auszudrucken. Besteht ein Recht auf Datenübertragbarkeit oder ein Migrationsbedarf, werden Umfang, strukturiertes Format, maschinelle Lesbarkeit, Interoperabilität, Felder, Datumsangaben und Beziehungen zwischen Tabellen geprüft. Der Export wird mit einem fiktiven Empfänger getestet, ohne Daten Dritter oder Geheimnisse offenzulegen. Eine EML-Datei kann den Übermittlungskontext bewahren, und Hashwerte ermöglichen den Vergleich der gesendeten mit der empfangenen Datei; keines der beiden Elemente bestätigt für sich allein die Vollständigkeit des Inhalts.[16][17]

Aktion	Nützlicher Nachweis	Angegebene Einschränkung
Profil löschen	Kennung, System, Datum, Bearbeiter und Prüfung des Nichtvorhandenseins.	Ausstehende technische Kopien und Ablaufdatum.
Zur Aufbewahrung sperren	Grund, eingeschränkter Zugriff und verbleibender Zweck.	Nicht für Werbung oder gewöhnliche Analysen verwenden.
Exportieren	Natives Format, Datenwörterbuch, Filter, Zeilen, Zeitzone und Hashwert.	Abdeckung der Abfrage und ausgeschlossene Daten.
An den Auftragsverarbeiter zurückgeben	Inventar, Kanal, Empfänger und Überprüfung des Downloads.	Verbleibende Kopien unter der Kontrolle des Auftragsverarbeiters.
Sicherungskopie wiederherstellen	Test in einer isolierten Umgebung und Liste der erneut anzuwendenden Löschungen.	Keine Löschung behaupten, solange der Zyklus noch nicht abgeschlossen ist.

Der korrekte Nachweis

„Das Profil wurde aus dem Marketingsystem gelöscht und sein Nichtvorhandensein am 10. November 2026 überprüft. Die verschlüsselte Sicherungskopie wird entsprechend dem dokumentierten Zyklus bis zu ihrem Ablauf aufbewahrt; bei einer Wiederherstellung wird die Löschung erneut ausgeführt.“ Diese Formulierung ist präziser als „alle Informationen wurden vernichtet“.

Kapitel 8. Drei vollständige Beispielabläufe

8.1 Personalwesen: der freigegebene Ordner

Ein fiktives Unternehmen bewahrt Lebensläufe in einem allgemein zugänglichen Ordner auf. Die Prüfung deckt Daten von Angehörigen, Referenzen, Dokumente und Bewertungen ohne Aufbewahrungsfrist auf. Beschlossen wird, aktive und abgelehnte Bewerbungsakten sowie Fälle begründeter Aufbewahrung zu trennen, Rollen einzuschränken, öffentliche Links zu entfernen, Zugriffe zu protokollieren und Exporte zu löschen. Eine Person verlangt Auskunft und erhält ihre Daten ohne diejenigen Informationen über die Bewertenden, die nicht herausgegeben werden dürfen. Die Änderung wird mit einem Testkonto überprüft, nicht durch neugieriges Einsehen einer echten Akte.

[16] RFC Editor. RFC 5322, Internet Message Format: Aufbau der Nachricht, Kopfzeilen und Nachrichtentext. Technische Referenz zur Aufbewahrung und zum Verständnis von E-Mails, kein automatischer Beweis der Identität einer natürlichen Person. Offizielle Online-Quelle

[17] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Verarbeitung bei Vorfällen. Offizielle Online-Quelle

8.2 Gesundheitswesen: die Nachricht an die falsche Gruppe

Eine fiktive Klinik sendet eine Tabelle mit Namen und Diagnosen an eine externe Gruppe. Die Empfänger werden aufgefordert, die Tabelle nicht weiterzuverbreiten und zu löschen, ohne sie an das gesamte Team weiterzuleiten; Empfänger, Inhalt und Kopierbarkeit werden dokumentiert. Zugriffe, Kontakte und das Verfahren zur Empfängerauswahl werden überprüft. Bei der Entscheidung über eine Meldung werden Sensibilität und Folgen berücksichtigt, nicht nur die Zahl der Zeilen. Die abschließende Änderung umfasst eine Empfängerkontrolle, Exportkontrollen und eine praktische Übung.

8.3 Analytik: der Bericht, der Personen wieder identifizierbar machte

Ein Team veröffentlicht einen pseudonymisierten Datensatz mit Region, Datum und einem außergewöhnlichen Kauf. Ein Leser kann ihn mit einer früheren Veröffentlichung verknüpfen und den Kunden erkennen. Die Verbreitung wird eingestellt, kleine Gruppen werden überprüft und einmalige Werte unterdrückt. Die neue Fassung behält ihren statistischen Nutzen ohne direkte Identifikatoren und weist ihre Grenzen aus. Der Fall zeigt, dass eine fehlerhafte Anonymisierung selbst eine neue Datenschutzverletzung verursachen kann – ausgerechnet durch den Versuch, zu informieren.

> **Gemeinsame Methode**
> Alle drei Fälle werden nach derselben Abfolge bearbeitet: Daten und Kopien auffinden, Zugriff und Verbreitung begrenzen, Folgen verstehen, über die Kommunikation entscheiden, Kontrollen umsetzen und Nachweise aufbewahren. Personen und Technologie ändern sich, die methodische Disziplin bleibt gleich.

Anhang A. Funktionale Entsprechungen im Datenschutz

Stand der Dokumentenprüfung: 10. November 2026. Die verglichenen Funktionen haben nicht zwangsläufig denselben Umfang, dieselbe Rechtsgrundlage, Frist oder Wirkung. Die Artikel werden genannt, um das jeweilige Rechtsregime einzuordnen, nicht um einen Fall automatisch zu lösen. Für Chile wird der spätere Wirksamkeitsbeginn des neuen Regimes ausdrücklich angegeben, damit es nicht vorzeitig als anwendbar dargestellt wird.

Jurisdiktion	Erfasste Funktionen	Vorsicht im praktischen Betrieb
Mexiko	LFPDPPP: Grundsätze, Sicherheit, Vertraulichkeit, Rechte und Mitteilung erheblicher Datenschutzverletzungen.	Neues Gesetz von 2025 und aktuelle Bundesbehörde; Branchenrecht und Reform prüfen.
Peru	Gesetz 29733 und Verordnung DS 016-2024-JUS: Grundsätze, Sicherheit, Vorfälle, Prävention und schrittweise ausgestaltete Rollen.	Die Verordnung enthält eigene Übergangsregelungen und Einzelheiten; europäische Fristen dürfen nicht übernommen werden.
Chile	Gesetz 21.719 ändert Gesetz 19.628: Grundsätze, Rechte, Sicherheit, Rechenschaftspflicht und Datenschutzbehörde.	Neues Regime mit verschobenem Beginn am 01-12-2026; die zum jeweiligen Datum geltende Vorschrift prüfen.
Argentinien	Gesetz 25.326: Datenqualität, Einwilligung, Information, Sicherheit, Rechte und Dienstleistungen im Auftrag Dritter.	Rechte nicht auf ein allgemeines Formular reduzieren und keine Daten Dritter offenlegen.
Kolumbien	Gesetz 1581: Grundsätze, Kategorien, Rechte, Informationen, Verantwortliche, Auftragsverarbeiter und Datenübermittlungen.	Ausnahmen, Sonderregeln und konkrete Pflichten jeder Rolle prüfen.

Jurisdiktion	Erfasste Funktionen	Vorsicht im praktischen Betrieb
Ecuador	LOPDP: Grundsätze, Sicherheit, Risiko, Datenschutz durch Technikgestaltung und Voreinstellungen, Vorfälle und Rechte.	Der Zugriff zur Bearbeitung einer Anfrage berechtigt weder zu einer unbegrenzten Verarbeitung noch zu einer unbefristeten Aufbewahrung.
Spanien / EU	DSGVO: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit und Verletzungen des Schutzes personenbezogener Daten; nationale und sektorale Ergänzungen.	Zwischen Risiko für die Meldung an die Behörde und hohem Risiko für die Benachrichtigung der betroffenen Person unterscheiden; LOPDGDD und Branchenrecht prüfen.

Quellen der Tabelle:[18][19][20][21][22][23][24][25][26][27][28][29][30][31]

A.1 Die Tabelle dient der Wahl der Rechtsgrundlage, nicht der Übertragung von Artikelnummern

Für einen konkreten Fall wird zunächst die erforderliche Funktion formuliert: Daten erheben, den Zweck ändern, einen Auftragsverarbeiter beauftragen, Daten außerhalb des jeweiligen Gebiets übermitteln, einen Antrag auf Rechtsausübung bearbeiten, einen Vorfall melden oder Daten löschen. Anschließend wird das einschlägige Rechtsinstrument mit Artikel, Regelungsgegenstand, Normadressat, Datum und Ausnahmen geprüft. Eine Vorschrift, die nur den öffentlichen, Finanz- oder Gesundheitssektor betrifft, wird nicht zu einer allgemeingültigen Regel. Wurde eine Ausnahme nicht überprüft, wird keine Antwort erfunden.

Die Regeln für elektronische Dokumente in den sieben Rechtssystemen helfen, Nachweise für Entscheidungen aufzubewahren: Anerkennung, Zurechenbarkeit, Integrität, Original, Zugänglichkeit und Aufbewahrung. Eine Signatur, ein Siegel oder ein Hashwert macht jedoch keine unrechtmäßige Verarbeitung rechtmäßig und beweist nicht, dass die betroffene Person einen Hinweis verstanden hat. Datenschutz, Integrität des Datensatzes und Richtigkeit des Inhalts werden getrennt bewertet.[25][26][27][28][29][30][31]

[18] Mexiko. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, veröffentlichter Text vom 20-03-2025 und Reform vom 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Datenschutzverletzungen und Bearbeitung von Anträgen auf Rechtsausübung. Derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno. Offizielle Online-Quelle

[19] Peru. Ley 29733 und die zugehörige, durch DS 016-2024-JUS genehmigte Verordnung. Grundsätze der Zweckbindung, Verhältnismäßigkeit, Sicherheit und Vertraulichkeit; die neue Verordnung konkretisiert Vorfälle, vorbeugende Bewertungen und die schrittweise ausgestalteten Funktionen des Datenschutzbeauftragten. Offizielle Online-Quelle

[20] Chile. Ley 21.719, mit der die Ley 19.628 über den Schutz personenbezogener Daten geändert wird. Die Fassung mit dem neuen Regime tritt am 01-12-2026 in Kraft; vor diesem Datum ist die dann geltende Vorschrift zu prüfen, und künftige Pflichten dürfen nicht als bereits geltend dargestellt werden. Offizielle Online-Quelle

[21] Argentinien. Ley 25.326, aktualisierter Text. Artikel 4–6, 9–10, 14–16 und 25: Datenqualität, Information, Sicherheit, Vertraulichkeit, Rechte betroffener Personen und Erbringung von Verarbeitungsdienstleistungen im Auftrag Dritter. Offizielle Online-Quelle

[22] Kolumbien. Ley Estatutaria 1581 de 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Informationen, Pflichten der Verantwortlichen und Auftragsverarbeiter sowie Datenübermittlungen in Drittländer. Offizielle Online-Quelle

[23] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Verarbeitung bei Vorfällen. Offizielle Online-Quelle

[24] Europäische Union. Reglamento (UE) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit sowie Meldung/Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten. Für Spanien sind außerdem die einschlägigen nationalen und sektoralen Rechtsvorschriften zu prüfen. Offizielle Online-Quelle

[25] Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechenbarkeit, Schriftform, Original, Integrität, Zugänglichkeit und Zulässigkeit von Datennachrichten. Amtliche Zusammenstellung. Offizielle Online-Quelle

[26] Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur. Offizielle Online-Quelle

[27] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[28] Reglamento (UE) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene elektronische Signatur und Rechtswirkungen qualifizierter elektronischer Signaturen. Offizielle Online-Quelle

[29] Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen. Offizielle Online-Quelle

[30] Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert. Offizielle Online-Quelle

[31] Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung an und Zulassung von digital signierten elektronischen Dokumenten. Offizielle Online-Quelle

Anhang B. Vorlagen zur Anpassung

B.1 Verzeichnis von Verarbeitungstätigkeiten

Feld	Mindestinhalt	Abnahmeprüfung
Tätigkeit und Verantwortlicher	Konkrete Aufgabe, Prozessinhaber und Vertretung.	Eine andere Person kann feststellen, wer entscheidet.
Zweck und Rechtsgrundlage	Konkreter Zweck, Rechtsgrundlage und gegebenenfalls Ausnahme.	Als vollständige Antwort genügt nicht „Verwaltung“.
Daten und Personen	Felder, Sensibilität, Dritte und besonders zu berücksichtigende Gruppen.	Für jedes Feld ist der Bedarf begründet.
Datenfluss und Auftragsverarbeiter	Eingang, Systeme, Zugriffe, Datenübermittlungen und Verbleib.	Umfasst Exporte und Sicherungskopien.
Aufbewahrung und Rechte	Frist, Sperrung, Löschung und Kontaktkanal.	„Unbefristet“ ist nicht ohne Begründung zulässig.
Risiko und Kontrollen	Plausibler Schaden, Maßnahmen, Test und Restrisiko.	Nachweise für die Funktionsweise liegen vor.

B.2 Antragsformular für betroffene Personen

Fiktive Vorlage für die interne Registrierung

```
ID: PRIV-DEMO-2026-001
Eingang: [Datum, Uhrzeit, Zeitzone, Kanal]
Wörtliche Anfrage: [Auskunft, Berichtigung, Löschung, Widerspruch, sonstige]
Identität: [verhältnismäßige Methode; keine Dokumente in dieses Formular aufnehmen]
Umfang: [Zeitraum, Systeme, Personen und Ausschlüsse]
Geltende Frist: [Vorschrift, Artikel, Beginn und Ablauf]
Suche: [Systeme, Filter, Auftragsverarbeiter und Sicherungskopien]
Entscheidung: [Rechtsgrundlage, Prüfung, Daten Dritter]
Ausgeführte Maßnahmen: [System, Datum, Bearbeiter, Überprüfung]
Übermittlung: [Format, Kanal, Empfänger, Datum und Überprüfung]
Offene Punkte und Grenzen: [was nicht geklärt wurde und warum]
```

B.3 Chronologie einer Datenschutzverletzung

Ereignis	Obligatorische Dokumentation	Verknüpfte Entscheidung
Erstes Signal	Quelle, wörtlicher Wert, Zeitzone, Verantwortlicher und Nachweis.	Akte anlegen und Beweise sichern.
Eindämmung	Maßnahme, zuständige Stelle, Umfang, Wirkung und zuvor gesicherte Beweise.	Schaden begrenzen, ohne den Kontext zu löschen.
Umfang	Daten, Personen, Zugriff, Kopien, Nutzung und Unklarheiten.	Risiko anhand von Tatsachen einstufen.
Mitteilungen	Empfänger, Inhalt, Kanal, Uhrzeit und Version.	Das lokale Rechtsregime einhalten, ohne weitere Daten offenzulegen.
Wiederherstellung	Wiederherstellung, Zugriffe, Überwachung und Tests.	Überprüfen, ob die Kontrolle funktioniert.
Verbesserung	Ursache, Prozessänderung, Verantwortlicher und Validierung.	Wiederholung verhindern, nicht nur den Vorgang abschließen.

B.4 Anbieterbewertung

Checkliste vor dem Einsatz echter Daten

```
1. Rolle jeder Partei und vertraglicher Zweck.
2. Erforderliche Mindestdaten, Standort, befugte Personen und Unterauftragsverarbeiter.
3. Authentifizierung, minimale Berechtigungen, Protokolle, Verschlüsselung und Schlüssel.
4. Überprüfbare Sicherheitsnachweise, nicht nur kommerzielle Zusicherungen.
5. Meldekanal für Vorfälle, Inhalt und Test der Kommunikation.
6. Unterstützung bei Rechten, Suchvorgängen und nativen Exporten.
7. Datenübermittlungen, Garantien und Standortwechsel.
8. Ausstieg: Format, Datenwörterbuch, Zugänglichkeit und Öffnungstest.
9. Löschung, Sicherungskopien und Nachweis mit Angabe der Grenzen.
10. Regelmäßige Überprüfung und interner Verantwortlicher.
```

B.5 Nachweis der Löschung oder Sperrung

Ein fiktives Beispiel

```
Objekt: EXP-DEMO-2026-001
Umfang: Marketingprofil und Kampagnenexport
Maßnahme: Löschung des aktiven Profils und Sperrung des erforderlichen Nachweises
Systeme: [Name, Version, Standort und Verantwortlicher]
Ausführung: [Datum, Zeitzone, Bearbeiter und Methode]
Überprüfung: [Abfrage, Nichtvorhandensein, Zugriff und Ergebnis]
Sicherungskopie: [Zyklus, Zugriff und erneute Löschung nach Wiederherstellung]
Auftragsverarbeiter: [Benachrichtigung und Antwort]
Verbleibende Aufbewahrung: [Rechtsgrundlage, Zweck und Frist]
Einschränkung: [was nicht behauptet werden kann]
Prüfung: [Person, Datum und verknüpfte Nachweise]
```

Anhang C. Glossar und Abschlusskontrolle

Begriff	Praktische Verwendung in diesem Handbuch
Verantwortlicher	Wer im Rahmen des geltenden Rechtsregimes über Rechtsgrundlage und Verarbeitung entscheidet.
Auftragsverarbeiter	Wer die Daten im Auftrag des Verantwortlichen nach Weisung verarbeitet und eigene Pflichten hat.
Pseudonymisierung	Zuordnung mithilfe zusätzlicher Informationen möglich; erfordert Trennung und Kontrolle.
Anonymisierung	Eine Zuordnung ist im jeweiligen Kontext vernünftigerweise ausgeschlossen; erfordert Nachweis und Überprüfung.
Sperrung	Begründete Einschränkung der Verarbeitung ohne Löschung des Datenbestands.
Datenübertragbarkeit	Strukturierte und interoperable Bereitstellung innerhalb des zulässigen Umfangs.
Datenschutzverletzung	Vorfall, der die Sicherheit personenbezogener Daten beeinträchtigt; der Schweregrad wird bewertet.
Nachweis der Einhaltung	Aufzeichnung, mit der sich Entscheidung, Ausführung und Ergebnis – nicht bloß die Absicht – überprüfen lassen.

Vor Abschluss eines Prozesses	Erforderliche Antwort
Welche Daten und Kopien gibt es?	Inventar mit Dateien, Sicherungskopien und Anbietern.
Warum ist jedes Feld notwendig?	Zweck, Rechtsgrundlage und Datenminimierung dokumentiert.
Wer kann zugreifen und wie wird dies nachgewiesen?	Rollen, Protokolle und Test mit fiktiven Daten.

Vor Abschluss eines Prozesses	Erforderliche Antwort
Wie kann eine Person ihre Rechte ausüben?	Kanal, Suche, Entscheidung, Übermittlung und Umsetzung.
Was geschieht bei einem Vorfall oder Ausstieg?	Chronologie, Kommunikation, Export und Löschung überprüft.
Was bleibt unbekannt?	Ausdrückliche Einschränkung, Verantwortlicher und nächste Überprüfung.

Abschluss

Daten zu schützen bedeutet, die Wahrscheinlichkeit zu verringern, dass eine organisatorische Entscheidung einer Person Schaden zufügt. Nachweise dienen dazu, diese Sorgfalt zu überprüfen und zu korrigieren, nicht, sie zur reinen administrativen Fassade werden zu lassen.