ACCCF / अनुप्रयुक्त ज्ञान पुस्तकालय

02

खंड

अनुप्रयुक्त गोपनीयता, सुरक्षा और दस्तावेज़ित निर्णय

स्पेनिश संस्करण · 2026

व्यक्तिगत डेटा संरक्षण और अनुपालन प्रमाण मैनुअल

सूची, अधिकार, आपूर्तिकर्ता, घटनाएँ, संरक्षण और सत्यापन योग्य विलोपन

लोगों की रक्षा ऐसे निर्णयों के माध्यम से की जानी चाहिए जिन्हें समझाया और सत्यापित किया जा सके, न कि नकल की गई नीतियों या ऐसे दस्तावेज़ों के फ़ोल्डरों के माध्यम से जिन्हें कोई व्यवहार में नहीं लाता।

यह मैनुअल गोपनीयता उत्तरदायियों, कानूनी, सुरक्षा, प्रौद्योगिकी, मानव संसाधन और प्रबंधन टीमों तथा व्यक्तिगत जानकारी का प्रसंस्करण करने वाले आपूर्तिकर्ताओं के लिए है। इसमें छोटे संगठनों के लिए एक कार्यपथ और जटिल संचालनों के लिए दूसरा कार्यपथ शामिल है।

संपादकीय समन्वय: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

सामान्य तकनीकी मार्गदर्शिका और मुक्त शैक्षिक सामग्री। यह कानूनी सलाह, विद्वत्परक राय या अनधिकृत सिस्टम पहुँच के निर्देश नहीं है। उदाहरण और डेटा काल्पनिक हैं; आकृतियाँ संपादकीय पुनर्निर्माण हैं।

विषय-सूची

दिखाई देने वाली पृष्ठ संख्या PDF संस्करण से संबंधित है। Word दस्तावेज़ खुलने पर इस अनुक्रमणिका को अद्यतन कर सकता है; शीर्षक आंतरिक नेविगेशन बनाए रखते हैं।

प्रस्तुति: गोपनीयता का प्रमाण संचालन में होता है 3
अध्याय 1. निर्णय लेने में सहायक सूची 3
1.1 प्रसंस्करण का वर्णन किसी संक्षिप्ताक्षर के पीछे छिपाए बिना करना 3
1.2 अदृश्य प्रतियों का पता लगाना 4
अध्याय 2. उद्देश्य, आधार और न्यूनतमकरण 5
2.1 समान दिखने वाले उद्देश्यों को अलग करना 5
2.2 अनावश्यक डेटा की कसौटी 5
2.3 सूचना और समझने योग्य अधिसूचना 6
अध्याय 3. कृत्रिम बाधाओं के बिना व्यक्तियों के अधिकार 6
3.1 प्राप्ति, पहचान और दायरा 6
3.2 अन्य व्यक्तियों का डेटा उजागर किए बिना पहुँच 7
3.3 जब विलोपन का अर्थ सब कुछ नष्ट करना न हो 7
अध्याय 4. जाँची जा सकने वाली सुरक्षा 7
4.1 नियंत्रणों की सूची से पहले जोखिम 7
4.2 नियंत्रण और उनके काम करने का साक्ष्य 8
4.3 छद्म नाम का अर्थ गुमनामी नहीं है 8
अध्याय 5. आपूर्तिकर्ता, क्लाउड और स्थानांतरण 9
5.1 उत्तरदायित्व आपूर्तिकर्ता पर नहीं टल जाता 9
5.2 प्रवाह और स्थानांतरण का मानचित्र 9
5.3 नियंत्रित निकास और प्रौद्योगिकी निर्भरता 10
अध्याय 6. सुरक्षा उल्लंघन: रोकथाम, समझ और अधिसूचना 10
6.1 घटनास्थल मिटाए बिना प्रारंभिक कार्रवाइयाँ 10
6.2 अधिसूचना का निर्णय और उपयोगी सामग्री 11
6.3 क्षति, दायरा और समापन 11
अध्याय 7. संरक्षण, विलोपन और पोर्टेबिलिटी 12
7.1 कारणों पर आधारित कैलेंडर, मनमानी पर नहीं 12
7.2 वास्तव में उपयोग योग्य पोर्टेबिलिटी 12
अध्याय 8. तीन पूर्ण प्रक्रिया-पथ 13
8.1 मानव संसाधन: साझा फ़ोल्डर 13
8.2 स्वास्थ्यः गलत समूह को भेजा गया संदेश 13
8.3 विश्लेषिकी: वह रिपोर्ट जो व्यक्तियों को पहचानने योग्य बना देती थी 13
अनुलग्नक A. गोपनीयता की कार्यात्मक समकक्षताएँ 14
A.1 आधार चुनने के लिए तालिका, संख्याओं के अनुवाद के लिए नहीं 14
अनुलग्नक B. अनुकूलन के लिए तैयार प्रारूप 15
B.1 प्रसंस्करण गतिविधि का रिकॉर्ड 15
B.2 डेटा धारक के अनुरोध का प्रारूप 15
B.3 सुरक्षा उल्लंघन का कालक्रम 16
B.4 आपूर्तिकर्ता मूल्यांकन 16
B.5 विलोपन या अवरोधन का प्रमाण-पत्र 16
अनुलग्नक C. शब्दावली और आउटपुट नियंत्रण 16

प्रस्तुति: गोपनीयता का प्रमाण संचालन में होता है

कोई गोपनीयता नीति सही हो सकती है और फिर भी संगठन हर दिन ऐसी जानकारी उजागर कर सकता है जिसकी उसे आवश्यकता नहीं है। अनुपालन वहीं से शुरू होता है जहाँ लेखन समाप्त होता है: अनावश्यक डेटा माँगने वाले फ़ॉर्म में, बाहरी कर्मियों के साथ साझा फ़ोल्डर में, पूरा डेटाबेस डाउनलोड कर सकने वाले आपूर्तिकर्ता में, ऐसे बैकअप में जिसे कोई पुनर्स्थापित नहीं जानता और ऐसे विलोपन में जो केवल स्क्रीन पर होता है। उपयोगी प्रश्न यह नहीं है कि कोई दस्तावेज़ मौजूद है या नहीं, बल्कि यह है कि किसी विशिष्ट व्यक्ति और उसकी जानकारी के साथ, उसे एकत्र करने से लेकर अनावश्यक हो जाने तक, क्या होता है।

यह मैनुअल कार्य की एक सरल इकाई अपनाता है: डेटा → उद्देश्य → आधार → पहुँच → जोखिम → साक्ष्य → अंतिम गंतव्य। प्रत्येक कड़ी का उत्तर सामान्य वाक्यांशों पर भरोसा किए बिना दिया जाना चाहिए। यदि कोई रिकॉर्ड बिक्री साबित करने के काम आता है, तो यह पहचानें कि उस उद्देश्य के लिए कौन से फ़ील्ड आवश्यक हैं, उन्हें कौन प्रशासित करता है, उन्हें कब तक संरक्षित रखा जाता है और उनके साथ कौन सी अन्य जानकारी आई है। यदि कोई नया उद्देश्य सामने आए, तो फ़ोल्डर का नाम बदलना पर्याप्त नहीं है: वैधता, डेटा धारक को दी जाने वाली सूचना और पहुँच का दायरा फिर से जाँचना होगा।

अनुपालन का साक्ष्य भी केवल काम दिखाने के लिए स्क्रीनशॉट जमा करना नहीं है। इसका अर्थ है किसी निर्णय का संस्करण, उसे उचित ठहराने वाला स्रोत, उसे अधिकृत करने वाला व्यक्ति, लागू किया गया नियंत्रण और उसके सत्यापन का परिणाम संरक्षित करना। तुलनात्मक कानूनों का उपयोग किसी दूसरे देश की नीति नकल करने के लिए नहीं किया जाता। इनसे उस कार्य को पहचाना जाता है जिसे संगठन को दस्तावेज़ित करना है: न्यूनतमकरण, सुरक्षा, पारदर्शिता, अधिकार, प्रसंस्करणकर्ता, घटना या स्थानांतरण। आधार और समय-सीमा की समीक्षा हमेशा संबंधित भौगोलिक क्षेत्र, उद्योग और प्रसंस्करण की तिथि के अनुसार की जाती है।

> **पहला निर्णय**
> कोई उपकरण खरीदने या दूसरी नीति लिखने से पहले, कोई वास्तविक प्रक्रिया चुनें और उसे काल्पनिक डेटा के साथ पूरा करके देखें। यदि आप यह नहीं समझा सकते कि कौन सी जानकारी आती है, क्यों आती है, उसे कौन देखता है, वह कहाँ पहुँचती है और कोई अधिकार कैसे प्रयोग किया जाता है, तो यही आपका पहला ठोस कार्य है।

अध्याय 1. निर्णय लेने में सहायक सूची

1.1 प्रसंस्करण का वर्णन किसी संक्षिप्ताक्षर के पीछे छिपाए बिना करना

उपयोगी सूची की शुरुआत “ग्राहक डेटाबेस” जैसे नाम से नहीं होती, क्योंकि इस तरह का लेबल बिक्री, सहायता, वसूली, विपणन और कर्मियों के चयन को आपस में मिला सकता है। शुरुआत किसी समझने योग्य गतिविधि से होती है: खरीद दर्ज करना, वारंटी सेवा देना, रोज़गार के आवेदन का मूल्यांकन करना, वेतन देना, पूछताछ का उत्तर देना या किसी भवन की सुरक्षा बनाए रखना। प्रत्येक गतिविधि के लिए विशिष्ट उद्देश्य, आवश्यक फ़ील्ड, संबंधित व्यक्ति, सिस्टम, अभिरक्षक, प्रवेश-चैनल और नियोजित निकास दर्ज किया जाता है।

वर्गीकरण में केवल नामिक संवेदनशीलता नहीं, बल्कि परिणाम भी दिखने चाहिए। संपर्क निर्देशिका में नाम और फ़ोन नंबर कम जोखिम वाले हो सकते हैं, लेकिन जब इनसे धमकी झेल रहे व्यक्ति का स्थान पता चले तो ये उच्च जोखिम वाले हो जाते हैं। किसी जाँच की फ़ाइल में पहचान, स्वास्थ्य, आर्थिक स्थिति, संचार और असंबंधित तीसरे पक्षों की जानकारी शामिल हो सकती है। केवल “गोपनीय” लेबल पर्याप्त नहीं है: यह तय करना होगा कि इसका उपयोग कौन कर सकता है, किन नियंत्रणों के साथ, किस निर्णय के लिए और कब तक। संदर्भ सामान्य दिखने वाले डेटा के संयोजन को भी किसी व्यक्ति की अंतरंग प्रोफ़ाइल में बदल सकता है।

सूची का फ़ील्ड	पारंपरिक प्रश्न	काल्पनिक उदाहरण
गतिविधि	कौन सी विशिष्ट कार्य किया जाता है?	ऑनलाइन खरीद गई उपकरण की वारंटी सेवा।

सूची का फ़ील्ड	मार्गदर्शन प्रश्न	काल्पनिक उदाहरण
न्यूनतम डेटा	कौन से फ़ील्ड इस कार्य को पूरा करने के लिए हैं और कौन से केवल सहायक हैं?	आईडी, संपर्क, डिलीवरी का पता और निदान, रोज़गार का इतिहास नहीं।
व्यक्ति	डेटा धारक, तीसरे पक्ष, गवाह या कमज़ोर समूह?	खरीदार, पंजीकृत प्रतिनिधि और नियुक्त तकनीशियन।
प्रवाह	यह कहाँ से आता है और किसे भेजा जाता है?	दुकान → सहायता प्लेटफ़ॉर्म → फ़ील्ड सेवा, कोई सार्वजनिक प्रसारण नहीं।
धारण और अपील	कौन निर्णय लेता है और यह कब अनावश्यक हो जाता है?	बिक्री-पश्चात उत्तरदायी, संचालन और सत्यापनकर्ता दायित्वों द्वारा निर्धारित अवधि।
साक्ष्य	निर्णय और उसके निष्पादन का कैसे साबित किया जाता है?	आवेदनों का स्वीकरण, न्यूनताएँ, लॉग, अनुरोध और विलोपन रिकॉर्ड।

1.2 अदृश्य प्रतियों का पता लगाना

सूची में निर्यात की गई फ़ाइलें, संलग्नक, स्कैन किए गए कागज़ात, व्यक्तिगत फ़ोल्डर, एप्लिकेशन लॉग, बैकअप प्रतियाँ और तृतीय-पक्ष सेवाएँ शामिल होनी चाहिए। आधिकारिक डेटाबेस नियंत्रित हो सकता है, जबकि कोई Excel फ़ाइल बिना स्वामी या विलोपन-तिथि के मैसेजिंग से घूमती रहे। किसी प्रति को “अस्थायी” कह देने से उसका प्रसंस्करण समाप्त नहीं हो जाता। यह दस्तावेज़ित करें कि उसे किसने बनाया, क्यों आवश्यक थी, कहाँ रखी गई, कौन खोल सकता है और उसका काम पूरा होने पर उसे कैसे हटाया जाएगा।

सूची तैयार करने का अच्छा साक्षात्कार केवल यह पूछने तक सीमित नहीं होता कि विभाग कौन सा सिस्टम उपयोग करता है। इसमें किसी व्यक्ति से काल्पनिक जानकारी के साथ पूरे कार्यदिवस का प्रदर्शन कराने को कहा जाता है: अनुरोध कैसे आता है, वह क्या डाउनलोड करता है, किसे अग्रेषित करता है, नोट्स कहाँ रखता है, त्रुटि होने पर क्या होता है और छुट्टी पर जाने पर वह क्या करता है। वास्तविक चित्र अपवादों में दिखाई देता है। सूची में पासवर्ड नहीं लिखे जाते; नियंत्रण-प्रणाली और उसके उत्तरदायी को दर्ज किया जाता है।

> **आउटपुट नियंत्रण**
> किसी भी प्रक्रिया को “और अन्य आवश्यक डेटा” लिखकर पूरा नहीं किया जाता। फ़ील्ड, स्रोत, गंतव्य और कारण स्पष्ट किए जाते हैं। जो जानकारी अज्ञात हो उसे जाँच के लिए चिह्नित किया जाता है; उसे केवल संतोष देने वाले किसी चेकबॉक्स से नहीं बदला जाता।



चित्र 1. डेटा से अंतिम गंतव्य तक। प्रत्येक निर्णय एक स्रोत और एक सत्यापन छोड़ता है। संपादकीय पुनर्निर्माण; यह वास्तविक साक्ष्य नहीं है।

अध्याय 2. उद्देश्य, आधार और न्यूनतमकरण

2.1 समान दिखने वाले उद्देश्यों को अलग करना

उत्पाद बेचना, विज्ञापन भेजना और व्यवहार-प्रोफ़ाइल बनाना एक ही उद्देश्य नहीं हैं। पहला किसी संबंध के लिए आवश्यक हो सकता है; अन्य दोनों का अलग विश्लेषण आवश्यक है। जब संगठन “प्रशासनिक और व्यावसायिक उद्देश्य” जैसे वाक्यांश में उद्देश्य मिला देता है, तो यह तय करना कठिन हो जाता है कि वास्तव में कौन सा डेटा आवश्यक है और किन संचारों की अलग व्याख्या की जानी चाहिए। रिकॉर्ड में यह भेद बना रहना चाहिए, ताकि व्यक्ति किसी उपयोग को अस्वीकार करते हुए भी अनावश्यक रूप से आवश्यक सेवा से वंचित न हो।

सहमति एक संभावित आधार है, सार्वभौमिक कुंजी नहीं। कानूनी दायित्व, किसी संबंध का निष्पादन, सार्वजनिक कार्यों का पालन, अधिकारों की रक्षा या संबंधित क्षेत्राधिकार में उपलब्ध कोई अन्य आधार भी हो सकता है। फ़ॉर्म चुनने से पहले संबंधित स्पष्ट नियम पहचाना जाता है। हर चीज़ के लिए सहमति माँगने से उत्तरदायित्व का झूठा भार व्यक्ति पर डाला जा सकता है और ऐसी प्रक्रिया अस्पष्ट हो सकती है जिसका पहले से कोई दूसरा आधार हो। यदि प्रसंस्करण बदलता है, तो उसे लागू करने से पहले संगतता, सूचना और नियंत्रणों की समीक्षा की जाती है।

मेक्सिको में वैधता, उद्देश्य, निष्ठा, सहमति, गुणवत्ता, आनुपातिकता, सूचना और उत्तरदायित्व के सिद्धांत हैं; कोलंबिया में वैधता, उद्देश्य, स्वतंत्रता, गुणवत्ता, पारदर्शिता, प्रतिबंधित पहुँच, सुरक्षा और गोपनीयता के सिद्धांत विकसित किए गए हैं; इक्वाडोर सक्रिय और प्रदर्शित उत्तरदायित्व अपेक्षित करता है। सिद्धांतों की समानता कार्यविधि बनाने में सहायता करती है, लेकिन प्रत्येक परिस्थिति और अपवाद को लागू नियम तथा संबंधित क्षेत्र के अनुसार समझना होगा।[1][2][3]

2.2 अनावश्यक डेटा की कसौटी

कोई फ़ील्ड लें और उसे काल्पनिक उदाहरण से हटा दें। यदि गतिविधि उसके बिना पूरी हो सकती है, तो यह उचित ठहराना होगा कि वह क्यों माँगा जाता है। मापदंड यह नहीं कि वह भविष्य में उपयोगी लग सकता है, बल्कि यह कि वह वर्तमान उद्देश्य के लिए उपयुक्त और आवश्यक है या नहीं। डिलीवरी की सूचना के लिए फ़ोन नंबर पर्याप्त हो सकता है; यदि पहचान किसी कम अतिक्रमणकारी माध्यम से सत्यापित हो सकती है, तो पहचान-पत्र की प्रति आवश्यक नहीं है। सांख्यिकीय विश्लेषण में परिणाम के साथ नाम संरक्षित करना भी शायद आवश्यक न हो।

स्थिति	न्यूनतमकरण का निर्णय	ऐसा रिकॉर्ड जो तात्कालिक फ़ैसले से बचाए
खरीद समर्थन	जरूरत जारी सेवा-पत्र, ग्राहक का पूरा फ़ाइल नहीं।	जनुमोदित फ़ाइल और प्रवेशित फ़ोन का स्क्रीनशॉट।
पहचान सत्यापन	जारीकर्ता सुरक्षा देने वाली न्यूनतम अतिक्रमणकारी विधि चुनें।	मूल्यांकन किए गए विकल्प, जोखिम और अनुमोदन
समाप्त रिपोर्ट	पहचानकर्ता निकाले और पुनः पहचान योग्य संयोजनों की जांच करें।	छोटे समूहों को जोड़ और लागू किया गया विलोपन।
तीसरे पक्ष से परामर्श	अनुरोधकर्ता के डेटा को अन्य व्यक्तियों के डेटा से अलग करना।	दिया गया संस्करण और सामग्री का पूर्व-समीक्षा।
नया उद्देश्य	संगतता और आधार की समीक्षा तक काम रोकें।	अनुरोध, वि-लेखन और दिनांकित अनुमोदन।

[1] मेक्सिको. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, सुरक्षा उल्लंघन और अधिकार-अनुरोधों का समाधान। वर्तमान संघीय प्राधिकरण Secretaría Anticorrupción y Buen Gobierno है। आधिकारिक ऑनलाइन स्रोत

[2] कोलंबिया. Ley Estatutaria 1581 de 2012, अनुच्छेद 4, 8, 12, 17–18 और 26: सिद्धांत, अधिकार, सूचना, नियंत्रकों और प्रसंस्करणकर्ताओं के कर्तव्य तथा तीसरे देशों में स्थानांतरण। आधिकारिक ऑनलाइन स्रोत

[3] इक्वाडोर. Ley Orgánica de Protección de Datos Personales, Registro Oficial, Suplemento 459, 26-05-2021। अनुच्छेद 10, 37–44: सिद्धांत, सुरक्षा उपाय, डिज़ाइन से सुरक्षा, जोखिम और घटनाओं से निपटने की प्रक्रिया। आधिकारिक ऑनलाइन स्रोत

2.3 सूचना और समझने योग्य अधिसूचना

गोपनीयता अधिसूचना से व्यक्ति को यह जानना चाहिए कि कौन निर्णय लेता है, उसका डेटा किस उद्देश्य से उपयोग होता है, उसे किसके साथ साझा किया जाता है, वह अपने अधिकार कैसे प्रयोग कर सकता है और संदेह होने पर कहाँ पूछ सकता है। लंबा पाठ समय पर दी गई व्याख्या का विकल्प नहीं है। वास्तव में प्रस्तुत किया गया संस्करण और उसका संदर्भ—पृष्ठ, तिथि, प्रवाह, भाषा और परिवर्तन—संरक्षित किया जाता है। साइट बदलने पर अनुपालन रिकॉर्ड से पुराना संस्करण नहीं हटाया जाता।

अर्जेंटीना में उद्देश्य, प्राप्तकर्ता या प्राप्तकर्ताओं की श्रेणियाँ, उत्तरदायी और अधिकार प्रयोग करने की संभावना के बारे में पहले से सूचित किया जाता है। कोलंबिया में अनुमति माँगते समय स्पष्ट और सुव्यक्त जानकारी देना कर्तव्य है तथा इसके पालन का प्रमाण संरक्षित रखना आवश्यक है। इन उदाहरणों से स्पष्ट है कि साक्ष्य में पाठ और संदर्भ दोनों क्यों जुड़ने चाहिए: वर्तमान URL यह साबित नहीं करता कि व्यक्ति ने वर्षों पहले क्या देखा था।[4][5]

काल्पनिक मामला: वह प्रचार जिसने पूरा फ़ाइल माँगा।

एक व्यवसाय डिजिटल कूपन देने के लिए आधिकारिक पहचान-पत्र, वैवाहिक स्थिति और पता माँगता है। विश्लेषण के बाद नया संस्करण केवल ईमेल और विज्ञापन के लिए अलग सहमति माँगता है, तथा पहचान-पत्र की कोई प्रति नहीं माँगता। यह दस्तावेज़ित किया जाता है कि कौन सा डेटा एकत्र करना बंद किया गया और पहले प्राप्त प्रतियों का संगठन क्या करेगा। फ़ॉर्म सुधारने से अतीत की जिम्मेदारी समाप्त नहीं होती।

अध्याय 3. कृत्रिम बाधाओं के बिना व्यक्तियों के अधिकार

3.1 प्राप्ति, पहचान और दायरा

अधिकार-चैनल के लिए दिनांक, आवेदक के रूप में पहचाना गया व्यक्ति, अनुरोध का प्रकार, दायरा, उत्तरदायी, लागू समय-सीमा और स्थिति दर्ज करना आवश्यक है। पहचान की जाँच आनुपातिक होनी चाहिए: हर अनुरोध के लिए अत्यधिक दस्तावेज़ माँगना बाधा बन सकता है और नई जानकारी उजागर कर सकता है। यह देखना होगा कि अनुरोध प्रमाणित करने के लिए संगठन के पास पहले से कौन सी जानकारी है, किसी दूसरे व्यक्ति को डेटा देने का क्या जोखिम है और चैनल कौन से वैकल्पिक सत्यापन-विकल्प देता है।

इसके बाद यह स्पष्ट करें कि व्यक्ति वास्तव में क्या चाहता है: यह जानना कि उसके डेटा का प्रसंस्करण होता है या नहीं, प्रति प्राप्त करना, डेटा सुधारना, विज्ञापन का विरोध करना, विलोपन, अवरोधन, सहमति वापस लेना, डेटा स्थानांतरित कराना या शिकायत करना। हर अनुरोध को पूर्ण विलोपन में न बदलें और कारण तथा पुनर्विचार का मार्ग बताए बिना “यह लागू नहीं होता” न कहें। यदि उत्तर में तीसरे पक्ष शामिल हैं, तो उनके अधिकार सुरक्षित रखते हुए अलग डिलीवरी-संस्करण तैयार करें; मूल फ़ाइल के तथ्यों को मिटाने का दिखावा न करें।

चरण	क्या दस्तावेज़ित किया जाता है	किस त्रुटि से बचा जाता है
प्राप्ति	चैनल, दिनांक और समयक्षेत्र, मूल सामग्री और वापसी।	किसी के इसे देखने का निर्णय लेने के बाद से समय-सीमा गिनना।
पहचान	पुनः गढ़े विवरण, जोखिम और उपयोग किया गया डेटा, प्रारूप में कोई गोपनीय जानकारी नहीं।	पहचान-पत्र को अनावश्यक नई प्रति बनाना।
डेटा का पता लगाना	सिस्टम, बैकअप, प्रसंस्करणकर्ता और खोज-मानदंड।	केवल मुख्य डेटाबेस से उत्तर देना।
निर्णय	आधार, अपवाद, समीक्षा और दिया गया डेटा।	किसी तीसरे पक्ष की जानकारी मिलने पर बिना कारण इनकार करना।

[4] अर्जेंटीना. Ley 25.326, अद्यतन पाठ। अनुच्छेद 4–6, 9–10, 14–16 और 25: गुणवत्ता, सूचना, सुरक्षा, गोपनीयता, डेटा धारकों के अधिकार और तीसरे पक्ष की ओर से प्रसंस्करण सेवाएँ। आधिकारिक ऑनलाइन स्रोत

[5] कोलंबिया. Ley Estatutaria 1581 de 2012, अनुच्छेद 4, 8, 12, 17–18 और 26: सिद्धांत, अधिकार, सूचना, नियंत्रकों और प्रसंस्करणकर्ताओं के कर्तव्य तथा तीसरे देशों में स्थानांतरण। आधिकारिक ऑनलाइन स्रोत

चरण	क्या दस्तावेज़ित किया जाता है	जिस त्रुटि से बचा जाता है
समापन	विनाश, पैनल, डिलीवरी का साक्ष्य और सिस्टम में की गई कार्रवाइयाँ।	परिवर्तन को निष्पादित किए बिना हल के रूप में चिह्नित करें।

3.2 अन्य व्यक्तियों का डेटा उजागर किए बिना पहुँच

किसी निर्यात में कर्मचारियों, ग्राहकों, परिजनों या वार्तालाप के प्रतिभागियों का डेटा हो सकता है। पहुँच का अधिकार उसे स्वतः उजागर करने की अनुमति नहीं देता। फ़ील्ड, पहचानकर्ता, सामग्री, संलग्नक और मेटाडेटा की समीक्षा की जाती है; संरक्षित मूल से अलग डिलीवरी-संस्करण उपयोग किया जाता है। समीक्षा से अर्थ नहीं बदलना चाहिए और अनुरोधकर्ता का अपना डेटा भी नहीं छिपाना चाहिए।

अर्जेंटीना में जानकारी स्पष्ट और विस्तृत होनी चाहिए तथा संबंधित व्यक्ति से जुड़ा होने पर भी तीसरे पक्ष का डेटा उजागर नहीं होना चाहिए। सुधार, अद्यतन और विलोपन के अपने नियम और समय-सीमाएँ हैं; संरक्षण का कानूनी दायित्व या तीसरे पक्ष के अधिकार होने पर अपवाद भी हैं। इस समय-सीमा को दूसरे देश में नकल नहीं किया जाता: मामले पर लागू कानूनी व्यवस्था दर्ज की जाती है।[6]

3.3 जब विलोपन का अर्थ सब कुछ नष्ट करना न हो

विलोपन का अनुरोध संरक्षण के दायित्व या किसी अधिकार की रक्षा के साथ एक साथ मौजूद हो सकता है। उत्तर में अलग-अलग बताएँ कि कौन सा प्रसंस्करण बंद होगा, कौन सा रिकॉर्ड अवरुद्ध होगा, कौन सी प्रति प्रतिबंधित रूप से रखी जाएगी और किस आधार पर। केवल उत्तर लिखना पर्याप्त नहीं है; सिस्टमों और प्रसंस्करणकर्ताओं के स्तर पर भी कार्रवाई करनी होगी। यदि डेटाबेस कानूनी बचाव के लिए रखा गया है, तो उसका उपयोग उसी उद्देश्य तक सीमित रखें और बाद की पहुँच नियंत्रित करें।

> **काल्पनिक उदाहरण।**
> कोई व्यक्ति खाता बंद करने के बाद अपनी सारी जानकारी हटाने का अनुरोध करता है। संगठन आवश्यक कर-रसीद रखता है, उसकी विपणन-प्रोफ़ाइल अवरुद्ध करता है, विभाजन से जुड़े गुण हटाता है और उन सिस्टमों की सूची दस्तावेज़ित करता है जिनमें प्रत्येक कार्रवाई की गई। उत्तर में बताया जाता है कि क्या हटाया गया, क्या अवरुद्ध किया गया और क्या रखा गया; यह दावा नहीं किया जाता कि सब कुछ गायब हो गया।

अध्याय 4. जाँची जा सकने वाली सुरक्षा

4.1 नियंत्रणों की सूची से पहले जोखिम

विश्लेषण की शुरुआत व्यक्तियों और संभावित क्षति से होती है, उत्पादों की सूची से नहीं। यह पहचाना जाता है कि कौन पहुँच सकता है, कौन सी त्रुटि संभव है, कौन सी प्रति सबसे अधिक उजागर है और डेटा में बदलाव, हानि, अनुपलब्धता या प्रकटीकरण का क्या परिणाम होगा। इसके बाद पहुँच, एन्क्रिप्शन, लॉगिंग, पृथक्करण, बैकअप, प्रशिक्षण और समीक्षा के नियंत्रण चुने जाते हैं। महँगा नियंत्रण सार्वजनिक निर्देशिका के लिए असंगत रूप से अधिक और क्लिनिकल फ़ाइल के लिए अपर्याप्त हो सकता है।

इक्वाडोर प्रसंस्करण, संबंधित व्यक्तियों तथा डेटा की श्रेणियों और मात्रा को ध्यान में रखते हुए जोखिम, खतरों और भेद्यताओं का विश्लेषण अपेक्षित करता है। यूरोपीय संघ जोखिम के अनुरूप तकनीकी और संगठनात्मक उपाय तथा डिज़ाइन और डिफ़ॉल्ट रूप से सुरक्षा अपेक्षित करता है। इस मूल्यांकन का रिकॉर्ड “हमारे पास उच्चतम मानक हैं” कहने से अधिक उपयोगी है, क्योंकि इससे यह समझाया जा सकता है कि प्रत्येक उपाय क्यों चुना गया और संगठन ने कौन सा अवशिष्ट जोखिम स्वीकार किया।[7][8]

[6] अर्जेंटीना. Ley 25.326, अद्यतन पाठ। अनुच्छेद 4–6, 9–10, 14–16 और 25: गुणवत्ता, सूचना, सुरक्षा, गोपनीयता, डेटा धारकों के अधिकार और तीसरे पक्ष की ओर से प्रसंस्करण सेवाएँ। आधिकारिक ऑनलाइन स्रोत

[7] इक्वाडोर. Ley Orgánica de Protección de Datos Personales, Registro Oficial, Suplemento 459, 26-05-2021। अनुच्छेद 10, 37–44: सिद्धांत, सुरक्षा उपाय, डिज़ाइन से सुरक्षा, जोखिम और घटनाओं से निपटने की प्रक्रिया। आधिकारिक ऑनलाइन स्रोत

[8] यूरोपीय संघ. Reglamento (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से सुरक्षा, प्रसंस्करणकर्ता, सुरक्षा और सुरक्षा उल्लंघनों की अधिसूचना/सूचना। स्पेन में लागू राष्ट्रीय और क्षेत्रीय कानून की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत

4.2 नियंत्रण और उनके काम करने का साक्ष्य

नियंत्रण	काल्पनिक जानकारी से परीक्षण	संरक्षित साक्ष्य
न्यूनतम विशेषाधिकार	सहायता-उपयोगकर्ता पतन-पेज नहीं खोल सकता और न पूरा डेटाबेस डाउनलोड कर सकता है।	भूमिका, जोखिम, प्रयास का परिणाम और पहुँच की समीक्षा।
एन्क्रिप्शन और कुंजियाँ	एक प्रति एन्क्रिप्ट की जाती है और केवल जोखिम भूमिका उसे पुनः प्राप्त कर सकती है।	कॉन्फ़िगरेशन, उत्तरदाता, पुनर्प्राप्ति और जानलेवा न कुंजियों का न होना।
लॉग	परीक्षण-कार्यवाई से उपयोगकर्ता, दिनांक, समयक्षेत्र और ऑब्जेक्ट वाला इवेंट बनता है।	मूल स्वरूप में निर्यात, डेटा शब्दकोश, संरक्षण और समीक्षा।
बैकअप	काल्पनिक डेटा-सेट को पृथक वातावरण में पुनर्स्थापित किया जाता है।	दिनांक, जर्नल, पटनाई, हश और खोलने की सत्यापन।
कर्मचारी की पद छोड़ना	पहुँच हटाई जाती है और सत्यापित किया जाता है कि वह अब काम नहीं करती।	पद छोड़ने की तिथि, जारी गए सिस्टम और उत्तरदाता।
गुमनामीकरण	रिकॉर्ड को संयोजना और ज्ञात मानों से पहचानने का प्रयास किया जाता है।	विधि, जोखिम जोखिम, परीक्षण और प्रसारण का अनुमोदन।

साक्ष्य से केवल अस्तित्व नहीं, कार्यक्षमता सिद्ध होनी चाहिए। एन्क्रिप्टेड कंसोल का स्क्रीनशॉट सभी प्रतियों की सुरक्षा साबित नहीं करता; पासवर्ड नीति विशेषाधिकारों की समीक्षा का प्रमाण नहीं है; “बैकअप” नामक फ़ोल्डर पुनर्प्राप्ति का प्रमाण नहीं है। परीक्षण काल्पनिक डेटा से इस तरह तैयार किया जाता है कि किसी सुरक्षा उल्लंघन की जाँच करते समय दूसरा उल्लंघन न हो। यदि कोई अप्रत्याशित पहुँच सफल हो जाए, तो इवेंट संरक्षित करें और रिपोर्ट प्रकाशित करने से पहले समस्या ठीक करें।

4.3 छद्म नाम का अर्थ गुमनामी नहीं है

नामों की जगह संदर्भ-संख्याएँ लगाने से प्रत्यक्ष एक्सपोज़र घटता है, लेकिन दिनांक, पता, पद, शौक या किसी विशिष्ट लेनदेन को मिलाकर पहचान फिर से की जा सकती है। छद्म नामकरण में अतिरिक्त जानकारी के माध्यम से संबंध बनाने की संभावना बनी रहती है; गुमनामीकरण के लिए वास्तविक प्रसारण-संदर्भ में पुनःपहचान का विश्लेषण आवश्यक है। फ़ाइल में कार्य-संस्करण और सार्वजनिक संस्करण अलग रखें तथा संगतता-तालिका को भिन्न नियंत्रणों से सुरक्षित रखें।

कोई डेटा-सेट साझा करने से पहले छोटे समूह, अद्वितीय मान, संलग्नक, निर्देशांक, अनुक्रम और मेटाडेटा जाँचें। नाम हटाने के बाद भी किसी गवाही से गाँव और पद के आधार पर व्यक्ति की पहचान हो सकती है। ऐसे में विवरण को सामान्य बनाएँ, हटाएँ या प्रकाशित न करें। पूर्ण गुमनामी का दावा न करें: विधि, परिकल्पनाएँ, अवशिष्ट जोखिम और संदर्भ बदलने पर समीक्षा दस्तावेज़ित करें।

> **व्यावहारिक नियम**
> किसी गुमनामीकरण की प्रभावशीलता केवल “क्या मुझे कोई नाम दिख रहा है?” से साबित न करें। यह पूछें कि कोई व्यक्ति युक्तियुक्त रूप से कौन सा दूसरा स्रोत मिला सकता है और किसी असामान्य विशेषता से किस व्यक्ति की पहचान हो जाएगी।



चित्र 2. काइ नाात यह साबत नहा करता िक नियत्रण काम करता ह। काल्पानक डटा स पराक्षण आर सराक्षत पारणाम। सपादकाय पुनानमाण; यह वास्तावक साक्ष्य नहीं है।

अध्याय 5. आपूर्तिकर्ता, क्लाउड और स्थानांतरण

5.1 उत्तरदायित्व आपूर्तिकर्ता पर नहीं टल जाता

जब कोई आपूर्तिकर्ता संगठन की ओर से डेटा का प्रसंस्करण करता है, तो निर्देश, उद्देश्य, अधिकृत कर्मी, स्थान, उपठेकेदार, गोपनीयता, सुरक्षा-उपाय, घटनाओं में सहायता, अधिकार-अनुरोधों का समाधान, डेटा वापसी, विलोपन और समीक्षा के लिए उपलब्ध साक्ष्य स्पष्ट किए जाते हैं। केवल अनुबंध पर हस्ताक्षर पर्याप्त नहीं है: यह जानना होगा कि कौन सा बटन पूरा डेटाबेस डाउनलोड कर सकता है, उसे कौन पुनर्स्थापित कर सकता है और पहुँच-लॉग कहाँ हैं।

अर्जेंटीना में तीसरे पक्ष की ओर से कंप्यूटरीकृत सेवाएँ देने वाला व्यक्ति डेटा को अनुबंध से भिन्न उद्देश्य के लिए उपयोग नहीं कर सकता और न संरक्षण के लिए किसी को हस्तांतरित कर सकता है; सेवा पूरी होने पर कानून द्वारा निर्धारित विनाश या अधिकृत संरक्षण की व्यवस्था लागू होगी। कोलंबिया में नियंत्रक और प्रसंस्करणकर्ता में भेद किया गया है और दोनों पर विशिष्ट कर्तव्य हैं। अनुबंध में वर्गीकरण सेवा के व्यावसायिक नाम के बजाय इस बात के अनुरूप होना चाहिए कि प्रत्येक पक्ष वास्तव में क्या निर्णय लेता है।[9][10]

5.2 प्रवाह और स्थानांतरण का मानचित्र

किसी क्लाउड का प्रशासन एक देश में, भंडारण दूसरे देश में, सहायता तीसरे देश में और बैकअप कई देशों में हो सकते हैं। मानचित्र में ये मार्ग, निर्णय लेने वाली संस्था, प्रसंस्करणकर्ता, उप-प्रसंस्करणकर्ता, प्रत्येक पहुँच का कारण और कानून द्वारा अपेक्षित गारंटी या तंत्र दर्ज होते हैं। “सर्वर क्लाउड में है” कहने से न स्थान स्पष्ट होता है, न जोखिम। अंतरराष्ट्रीय स्थानांतरण के लिए केवल खंड नकल करना पर्याप्त नहीं है: दायरा, अपवाद, प्राप्तकर्ता और नियंत्रण जाँचने होते हैं।

आपूर्तिकर्ता से पूछें	अपेक्षित दस्तावेज़ी उत्तर	चेतावनी संकेत
किसकी पहुँच हो सकती है?	भूमिकाएँ, स्थान, प्रमाणीकरण, लॉगिंग और समीक्षा।	व्यक्तियों और रोल के बिना केवल “तकनीकी सहायता”।

[9] अर्जेंटीना. Ley 25.326, अद्यतन पाठ। अनुच्छेद 4–6, 9–10, 14–16 और 25: गुणवत्ता, सूचना, सुरक्षा, गोपनीयता, डेटा धारकों के अधिकार और तीसरे पक्ष की ओर से प्रसंस्करण सेवाएँ। आधिकारिक ऑनलाइन स्रोत

[10] कोलंबिया. Ley Estatutaria 1581 de 2012, अनुच्छेद 4, 8, 12, 17–18 और 26: सिद्धांत, अधिकार, सूचना, नियंत्रकों और प्रसंस्करणकर्ताओं के कर्तव्य तथा तीसरे देशों में स्थानांतरण। आधिकारिक ऑनलाइन स्रोत

जानकारी से पूछें	अपेक्षित दस्तावेज़ उत्तर	पहचानें सबूत
कौन से उप-प्रसंस्करणकर्ता शामिल हैं?	पहचान, कार्य, स्थान और परिवर्तन तक।	बिना सूचना के गुप्त सूची या परिवर्तन।
डेटा धारकों के अधिकार-अनुरोधों में कैसे सहायता करता है?	खोज, सुधार, अपराधन, निर्यात और समय-सीमाएँ।	यह केवल खोज और फ़िल्टर के बिना पोर्टेबिलिटी प्रदान करता है।
घटनाओं की सूचना कब दी जाती है?	पैनल, सबूत, कालक्रम, साक्ष्य और अपडेट।	बिना रिकॉर्ड के मौखिक आश्वासन।
रिश्ता कब समाप्त होता है?	निर्यात, पठनीयता, विलोपन, बैकअप और प्रमाण-पत्र।	जानकारी पुनः प्राप्त किए बिना खाता बंद करना।

5.3 नियंत्रित निकास और प्रौद्योगिकी निर्भरता

अनुबंध करने से पहले काल्पनिक डेटा से निकास की जाँच की जाती है। निर्यात डाउनलोड करके उसे स्वतंत्र उपकरण में खोलें और देखें कि फ़ील्ड, समयक्षेत्र, संबंध और डेटा शब्दकोश बने रहते हैं या नहीं। यदि प्लेटफ़ॉर्म केवल प्रिंट करने देता है, तो निर्भरता का जोखिम दर्ज करें। निकास में प्रोडक्शन, परीक्षण-प्रतियों, बैकअप और लॉग से विलोपन भी शामिल है; कुछ घटक कानूनी दायित्व या सुरक्षा के कारण रखे जा सकते हैं, लेकिन उनका दायरा स्पष्ट होना चाहिए।

> **काल्पनिक मामला**
>
> कोई संगठन सर्वेक्षण-आपूर्तिकर्ता बदलता है। निर्यात में उत्तर हैं, लेकिन फ़ॉर्म-पहचानकर्ता और समयक्षेत्र नहीं हैं। डेटा शब्दकोश सहित नई डिलीवरी माँगी जाती है, दोनों निर्यात अलग-अलग ऑब्जेक्ट के रूप में रखे जाते हैं और पहले निर्यात की सीमा दर्ज की जाती है। अंत में खाता हटाया जाता है और उस कार्रवाई के वास्तविक दायरे का प्रमाण-पत्र प्राप्त किया जाता है।

अध्याय 6. सुरक्षा उल्लंघन: रोकथाम, समझ और अधिसूचना

6.1 घटनास्थल मिटाए बिना प्रारंभिक कार्रवाइयाँ

पहला उद्देश्य व्यक्तियों की रक्षा और क्षति सीमित करना है, बिना घटना समझाने वाली जानकारी नष्ट किए। दर्ज करें कि घटना कब पता चली, किसने रिपोर्ट की, कौन से सिस्टम प्रभावित प्रतीत होते हैं, कौन सा डेटा शामिल हो सकता है और कौन सी कार्रवाइयाँ पहले हो चुकी हैं। पासवर्ड सुरक्षित चैनल से बदलें, लेकिन पहले संबंधित पहुँच-इवेंट संरक्षित करें। पुनर्स्थापना का उपयोग साक्ष्य मिटाने या समय से पहले यह घोषित करने के लिए न करें कि सब कुछ समाप्त हो गया।

NIST SP 800-61 Rev. 3 प्रतिक्रिया को तैयारी, पहचान, प्रतिक्रिया, पुनर्प्राप्ति और निरंतर सुधार में समाहित करता है। इससे संकीर्ण व्याख्या से बचा जाता है: घटना केवल “सर्वर बंद करने” तक सीमित नहीं है; दायरा, संचार, व्यक्तियों पर प्रभाव और बाद के परिवर्तन भी समझने हैं। डेटा उल्लंघन में यह भी संरक्षित करें कि कौन से फ़ील्ड, किस सटीकता के साथ उजागर हुए और तीसरा पक्ष कौन सी प्रतियाँ प्राप्त कर सका।[11][12]

कार्य	दस्तावेज़ित कार्रवाई	सहज प्रतिक्रिया न न करने योग्य कार्य
पता लगाना	समय, स्रोत, समय, उत्तरदाता और प्रारंभिक दायरा दर्ज करें।	पहले सबूत के आधार पर ही मूल कारण घोषित करना।
रोकथाम	आनुपातिक उपाय चुन और पहले से उपलब्ध साक्ष्य दर्ज करें।	लॉग। निर्यात किए बिना डिवाइस रीसेट करना या खाते हटाना।

[11] NIST SP 800-61 Rev. 3 (अप्रैल 2025)। CSF 2.0 में समाहित घटना-प्रतिक्रिया सिफ़ारिशें: तैयारी, पहचान, प्रतिक्रिया, पुनर्प्राप्ति और सुधार। यह संशोधन 2 को प्रतिस्थापित करता है। आधिकारिक ऑनलाइन स्रोत

[12] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. पद्धतिपूर्ण मार्गदर्शिका; न कानून, न न्यायालय में स्वीकार्यता की गारंटी। आधिकारिक ऑनलाइन स्रोत

कौशल	दस्तावेज़ीकृत कार्यवाई	सहज प्रतिक्रिया न न करने योग्य कार्य
मूल्यांकन	डेटा, डेटा धारक, पहुँच, उपयोग और संभावित परिणाम पहचानें।	पीड़ितों की संख्या को व्यक्तियों की संख्या समझ लेना।
जोखिसूचना	जोखिसूचना की दायित्ववारी, जोखिसूचना-सीमा, प्राप्तकर्ता, सामग्री और स्थानीय समय-सीमा लागू करें।	हर देश और क्षेत्र में 72 घंटे या 48 घंटे का नियम मानकर करना।
पुनर्प्राप्ति	नियंत्रण, निगरानी, प्रभावित व्यक्तियों की सहायता और परिवर्तन सत्यापित करें।	केवल नया फ़ाइंडर बनाकर और कोई सीख लिए बिना घटना बंद करना।

6.2 अधिसूचना का निर्णय और उपयोगी सामग्री

अधिसूचना लागू कानून, संगठन के प्रकार, घटना की प्रकृति और गंभीरता तथा प्रभावित व्यक्तियों पर निर्भर करती है। मेक्सिको में 2026 में प्रचलित कानून महत्वपूर्ण उल्लंघनों की सूचना प्रभावित व्यक्तियों को तत्काल देना अपेक्षित करता है, ताकि वे अपने अधिकारों की रक्षा कर सकें। पेरू में 2024 में अनुमोदित विनियम घटनाओं की समय पर रिपोर्ट प्राधिकरण को और एक्सपोज़र के अनुसार प्रभावित व्यक्तियों को सूचना देने की व्यवस्था लाता है; आधिकारिक स्रोत में सामान्यतः 48 घंटे का समय बताया गया है, यदि उचित कारण न हों। यूरोपीय संघ में अनुच्छेद 33 और 34 जोखिम के अनुसार प्राधिकरण को अधिसूचना और डेटा धारक को सूचना में भेद करते हैं। ये नियम परस्पर बदले नहीं जा सकते।[13][14][15]

उपयोगी अधिसूचना में उपलब्ध जानकारी के अनुसार बताएँ कि क्या हुआ, कौन सी श्रेणियों का डेटा प्रभावित हो सकता है, क्या किया जा रहा है, व्यक्ति कौन से उचित कदम उठा सकता है और अधिक जानकारी कहाँ मिलेगी। इसमें गोपनीय जानकारी या हमलावर के बारे में अटकलें न हों। तथ्य बदलने पर अधिसूचना अद्यतन करें और इतिहास संरक्षित रखें। प्रतिष्ठा बचाने के लिए घटना छिपाने से उसी क्षति में कई गुना वृद्धि हो सकती है जिसे टालना चाहते थे।

6.3 क्षति, दायरा और समापन

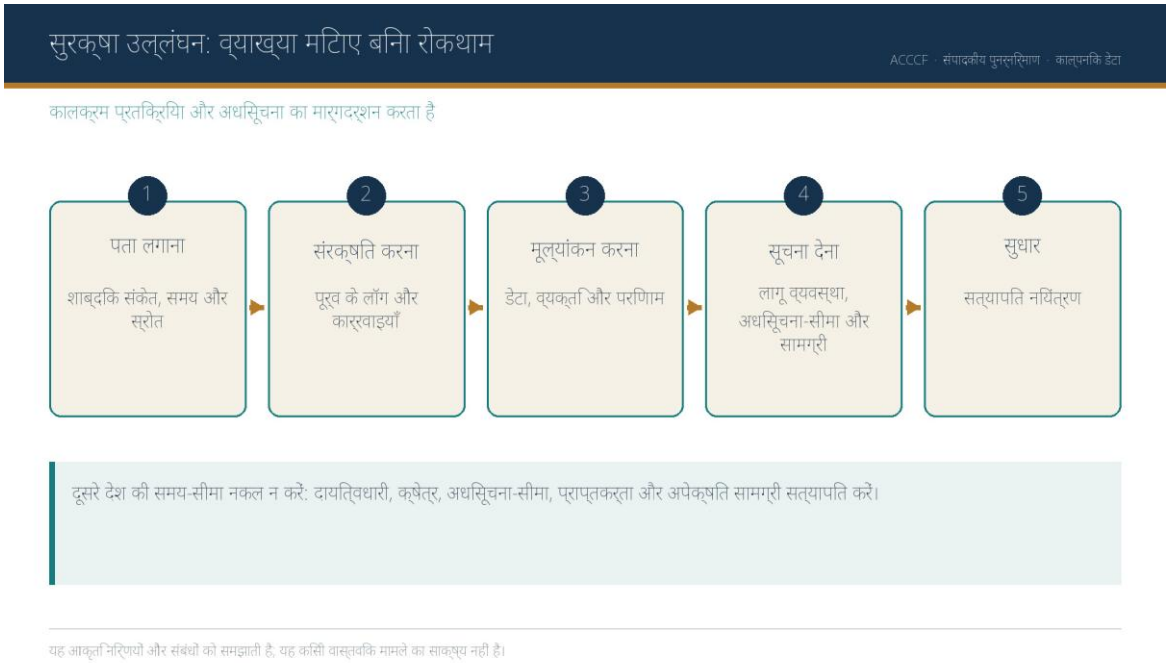
मूल्यांकन में उपयोग की संभावना, क्रेडेंशियल की गोपनीयता, संपर्क की सुविधा, व्यक्तियों की कमज़ोरी, पहुँच का प्रचार तथा शारीरिक, आर्थिक या भेदभावपूर्ण प्रभाव शामिल हों। “केवल नाम थे” कहना भी गंभीर हो सकता है यदि वे किसी संवेदनशील सेवा-केंद्र से जुड़ते हों। साक्ष्य एकत्र करते समय सार्वजनिक लिंक से लीक हुआ डेटा दोबारा डाउनलोड न करें और न उसे पूरी टीम में बाँटें।

> **वास्तविक समापन**
> सिस्टम पुनर्स्थापित हो जाने पर घटना समाप्त नहीं होती। समापन तब होता है जब व्यक्तियों को आवश्यकतानुसार सूचित कर दिया गया हो, नियंत्रण जाँचे गए हों, पहुँच की समीक्षा हुई हो, साक्ष्य संरक्षित हो और प्रक्रिया में ऐसा बदलाव हुआ हो जो वही अनुक्रम दोहराने से रोके। यदि कुछ अज्ञात रहता है, तो रिपोर्ट में उसे सीमा के रूप में दर्ज रखें।

[13] मेक्सिको. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, सुरक्षा उल्लंघन और अधिकार-अनुरोधों का समाधान। वर्तमान संघीय प्राधिकरण Secretaría Anticorrupción y Buen Gobierno है। आधिकारिक ऑनलाइन स्रोत

[14] पेरू. Ley 29733 और DS 016-2024-JUS द्वारा अनुमोदित उसका विनियम। उद्देश्य, आनुपातिकता, सुरक्षा और गोपनीयता के सिद्धांत; नया विनियम घटनाओं, निवारक मूल्यांकन और डेटा अधिकारी के क्रमिक कार्यों का विवरण देता है। आधिकारिक ऑनलाइन स्रोत

[15] यूरोपीय संघ. Reglamento (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से सुरक्षा, प्रसंस्करणकर्ता, सुरक्षा और सुरक्षा उल्लंघनों की अधिसूचना/सूचना। स्पेन में लागू राष्ट्रीय और क्षेत्रीय कानून की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत



चित्र 3. सुरक्षा उल्लंघन: व्याख्या मिटाए बिना रोकथाम। कालक्रम प्रतिक्रिया और अधिसूचना का मार्गदर्शन करता है। संपादकीय पुनर्समीक्षा; यह वास्तविक साक्ष्य नहीं है।

अध्याय 7. संरक्षण, विलोपन और पोर्टेबिलिटी

7.1 कारणों पर आधारित कैलेंडर, मनमानी पर नहीं

संरक्षण-अवधि उद्देश्य, कानूनी दायित्व, अनुबंध, अधिकारों की रक्षा और परिचालन आवश्यकता से तय होती है। “व्यक्तिगत डेटा” के लिए कोई सार्वभौमिक अवधि नहीं है। सामान्य उपयोग की अवधि, प्रतिबंधित अवरोधन और साक्ष्य हेतु संरक्षण में भेद किया जाता है। उद्देश्य बदलने पर कैलेंडर की समीक्षा करें। सब कुछ “शायद काम आए” इस सोच से रखने से एक्सपोज़र कई गुना बढ़ता है और किसी अनुरोध का सटीक उत्तर देना कठिन हो जाता है।

विलोपन में सिस्टम, निर्यात, उपयोगकर्ता, आपूर्तिकर्ता और उपलब्ध प्रतियाँ शामिल हों। बैकअप का तकनीकी चक्र अलग हो सकता है: दस्तावेज़ित करें कि उन्हें हटाया जाएगा, ओवरराइट किया जाएगा या समाप्ति तक दुर्गम रखा जाएगा। यदि पुनर्स्थापना से हटाया गया डेटा वापस आ सकता है, तो प्रक्रिया में उसे फिर से हटाने का तरीका शामिल हो। प्रमाण-पत्र में तकनीकी रूप से हुई कार्रवाई से अधिक का दावा न करें।

7.2 वास्तव में उपयोग योग्य पोर्टेबिलिटी

डेटा देने का अर्थ उसे प्रिंट करना नहीं है। जहाँ पोर्टेबिलिटी का अधिकार या माइग्रेशन की आवश्यकता हो, वहाँ दायरा, संरचित प्रारूप, मशीन-पठनीयता, अंतःप्रचालनीयता, फ़ील्ड, तिथियाँ और तालिकाओं के बीच संबंध जाँचें। निर्यात का परीक्षण काल्पनिक प्राप्तकर्ता के साथ करें, तीसरे पक्ष की जानकारी या गोपनीय तथ्य उजागर किए बिना। EML डिलीवरी का संदर्भ संरक्षित कर सकता है और हैश से भेजी गई फ़ाइल की प्राप्त फ़ाइल से तुलना की जा सकती है; इनमें से कोई भी अकेले सामग्री की पूर्णता प्रमाणित नहीं करता।[16][17]

कार्यवाई	उपयोगी साक्ष्य	वांछित समय
प्रोफ़ाइल का विलोपन	पहचानकर्ता, प्रणाली, तिथि, ऑपरेटर और अनुपस्थिति सत्यापन।	प्रशासित तकनीकी प्रतीक्षा और समाप्ति तिथि

[16] RFC Editor. RFC 5322, Internet Message Format: संदेश की संरचना, हेडर और बॉडी। यह ईमेल संरक्षित करने और समझने का तकनीकी संदर्भ है, मानव पहचान का स्वतः प्रमाण नहीं। आधिकारिक ऑनलाइन स्रोत

[17] इक्वाडोर. Ley Orgánica de Protección de Datos Personales, Registro Oficial, Suplemento 459, 26-05-2021। अनुच्छेद 10, 37–44: सिद्धांत, सुरक्षा उपाय, डिज़ाइन से सुरक्षा, जोखिम और घटनाओं से निपटने की प्रक्रिया। आधिकारिक ऑनलाइन स्रोत

कारवाई	उपयोगी साक्ष्य	यात्रा सलाह
संरक्षण के लिए जब्तीकरण	कारण, प्रतिबंधित पहुँच और जब्तीशुदा उद्धरण।	विज्ञापन या सामान्य विश्लेषण के लिए उपयोग न करना।
निर्यात	मूल स्वरूप, डेटा शब्दकोश, फ़िल्टर, पक्तियाँ, समयक्षेत्र और हैश।	खोज का कवरेज और बाहरी डेटा।
प्रसंस्करणकर्ता को वापस करना।	सूची, पैनल, प्राप्तकर्ता और डाउनलोड का सत्यापन।	प्रसंस्करणकर्ता के नियंत्रण में शेष प्रतियाँ।
बैकअप को बहाल करना।	पृथक वातावरण में परीक्षण और विलोपन दोबारा लागू करने की सूची।	यदि चक्र जमा पूरा नहीं हुआ है, तो विलोपन को दोहरा न करना।

सही प्रमाण-पत्र

“विपणन सिस्टम से प्रोफ़ाइल हटा दी गई और 10 नवंबर 2026 को उसकी अनुपस्थिति सत्यापित की गई। एन्क्रिप्टेड बैकअप समाप्ति तक दस्तावेज़ित चक्र में रहता है; यदि उसे पुनर्स्थापित किया जाता है, तो विलोपन फिर से लागू किया जाता है।” यह “सारी जानकारी नष्ट कर दी गई” कहने से अधिक सटीक है।

अध्याय 8. तीन पूर्ण प्रक्रिया-पथ

8.1 मानव संसाधन: साझा फ़ोल्डर

एक काल्पनिक कंपनी सामान्य पहुँच वाले फ़ोल्डर में बायोडेटा रखती है। समीक्षा में परिजनों का डेटा, संदर्भ, दस्तावेज़ और बिना अवधि के मूल्यांकन मिलते हैं। सक्रिय, अस्वीकृत और उचित कारण से संरक्षित फ़ाइलें अलग करने; भूमिकाएँ सीमित करने; सार्वजनिक लिंक हटाने; पहुँच दर्ज करने और निर्यात में विलोपन करने का निर्णय होता है। कोई व्यक्ति पहुँच का अनुरोध करता है और उसे अपना डेटा मिलता है, लेकिन मूल्यांकनकर्ताओं की वह जानकारी नहीं जिसे देना उचित नहीं है। बदलाव की जाँच परीक्षण-खाते से होती है, किसी वास्तविक फ़ाइल में जिज्ञासा से नहीं।

8.2 स्वास्थ्यः गलत समूह को भेजा गया संदेश

एक काल्पनिक क्लिनिक नाम और निदान वाली तालिका बाहरी समूह को भेज देती है। उसे आगे न बाँटने और हटाने के लिए कहा जाता है, बिना पूरी टीम को अग्रेषित किए; प्राप्तकर्ता, सामग्री और प्रति बनने की संभावना दर्ज की जाती है। पहुँच, संपर्क और प्राप्तकर्ता चुनने की प्रक्रिया की समीक्षा होती है। अधिसूचना का मूल्यांकन केवल पंक्तियों की संख्या पर नहीं, संवेदनशीलता और परिणामों पर भी आधारित होता है। अंतिम बदलाव में प्राप्तकर्ता की जाँच, निर्यात-नियंत्रण और व्यावहारिक अभ्यास शामिल हैं।

8.3 विश्लेषिकी: वह रिपोर्ट जो व्यक्तियों को पहचानने योग्य बना देती थी

कोई टीम क्षेत्र, तिथि और एक असाधारण खरीद वाला छद्म नामित डेटा-सेट प्रकाशित करती है। पाठक उसे पुराने प्रकाशन से जोड़कर ग्राहक को पहचान सकता है। प्रसारण वापस लिया जाता है, छोटे समूह जाँचे जाते हैं और विशिष्ट मान हटाए जाते हैं। नए संस्करण में प्रत्यक्ष पहचानकर्ता नहीं रहते, सांख्यिकीय उपयोगिता बनी रहती है और सीमाएँ बताई जाती हैं। यह मामला याद दिलाता है कि दोषपूर्ण गुमनामीकरण से रिपोर्ट देने के प्रयास में ही नया सुरक्षा उल्लंघन हो सकता है।

साझा विषय

तीनों मामले एक ही क्रम से हल होते हैं: डेटा और प्रतियाँ खोजना, पहुँच और प्रसारण सीमित करना, परिणाम समझना, संचार का निर्णय लेना, नियंत्रण लागू करना और साक्ष्य संरक्षित करना। व्यक्ति और प्रौद्योगिकी बदलते हैं, अनुशासन नहीं।

अनुलग्नक A. गोपनीयता की कार्यात्मक समकक्षताएँ

10 नवंबर 2026 तक दस्तावेज़ी समीक्षा। तुलना किए गए कार्यों का दायरा, आधार, अवधि या प्रभाव समान होना आवश्यक नहीं है। अनुच्छेद कानूनी व्यवस्था खोजने के लिए उद्धृत हैं, किसी फ़ाइल का स्वतः समाधान करने के लिए नहीं। चिली में नई व्यवस्था का विलंबित प्रारंभ स्पष्ट रूप से बताया गया है, ताकि उसे समय से पहले लागू न दिखाया जाए।

क्षेत्राधिकार	पहचाने गए कार्य	पारदर्शी सावधानी
मेक्सिको	LFPDPPP: सिद्धांत, सुरक्षा, गोपनीयता, अधिकार और महत्वपूर्ण उल्लंघनों की अधिसूचना।	2025 का नया कानून और वर्तमान संघीय प्राधिकरण, क्षेत्र और संशोधन की समीक्षा करें।
पेरू	कानून 29733 और विनियम DS 016-2024-JUS: सिद्धांत, सुरक्षा, घटनाएँ, रोकथाम और क्रमिक भूमिकाएँ।	विनियम को जर्मन सक्रमण और विशेष विवरण है, यूरोपीय समय-सीमाएँ नकल न करें।
चिली	कानून 21.719 कानून 19.628 में संशोधन करता है: सिद्धांत, अधिकार, सुरक्षा, उत्तरदायित्व और एजेंसी।	नई व्यवस्था का प्रारंभ 01-12-2026 के लिए स्थगित है; संबंधित तिथि पर लागू नियम जाँचें।
अर्जेंटीना	कानून 25.326: गुणवत्ता, सहमति, सूचना, सुरक्षा, अधिकार और तीसरे पक्ष की ओर से सेवाएँ।	अधिकारों को सामान्य फ़ाइल तक सीमित न करें और तीसरे पक्ष का डेटा उजागर न करें।
कोलंबिया	कानून 1581: सिद्धांत, श्रेणियाँ, अधिकार, सूचना, नियंत्रक, प्रसंस्करणकर्ता और स्थानांतरण।	अपवाद, विशेष नियम और प्रत्येक श्रेणी के विशिष्ट कर्तव्य जाँचें।
इक्वाडोर	LOPDP: सिद्धांत, सुरक्षा, जोखिम, डिज़ाइन और डिफ़ॉल्ट रूप से सुरक्षा, घटनाएँ और अधिकार।	उत्तर देने के लिए पहुँच अनुमति प्रसंस्करण की स्वायत्त संरक्षण की अनुमति नहीं देती।
स्पेन/यूरोपीय संघ	RGPD: सिद्धांत, डिज़ाइन, प्रसंस्करणकर्ता, सुरक्षा और उल्लंघन; राष्ट्रीय और क्षेत्रीय पूरक।	प्राधिकरण की अधिसूचना के लिए जोखिम और डेटा धारक को सूचना के लिए उच्च जोखिम में भेद करें; LOPDGDD और संबंधित क्षेत्र जाँचें।

तालिका के स्रोत:[18]192021222324

A.1 आधार चुनने के लिए तालिका, संख्याओं के अनुवाद के लिए नहीं

किसी मामले में पहले आवश्यक कार्य लिखें: डेटा एकत्र करना, उद्देश्य बदलना, प्रसंस्करणकर्ता चुनना, क्षेत्र से बाहर स्थानांतरण, अधिकार-अनुरोध का उत्तर, घटना की अधिसूचना या विलोपन। फिर लागू विधि-दस्तावेज़ को अनुच्छेद, विषय, दायित्वधारी, तिथि और अपवादों सहित देखें। यदि नियम केवल सार्वजनिक, वित्तीय या स्वास्थ्य क्षेत्र पर लागू होता है, तो उसे सार्वभौमिक नियम न बनाएँ। यदि कोई अपवाद सत्यापित नहीं हुआ है, तो मनगढ़ंत उत्तर न दें।

[18]मेक्सिको. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, सुरक्षा उल्लंघन और अधिकार-अनुरोधों का समाधान। वर्तमान संघीय प्राधिकरण Secretaría Anticorrupción y Buen Gobierno है। आधिकारिक ऑनलाइन स्रोत

[19]पेरू. Ley 29733 और DS 016-2024-JUS द्वारा अनुमोदित उसका विनियम। उद्देश्य, आनुपातिकता, सुरक्षा और गोपनीयता के सिद्धांत; नया विनियम घटनाओं, निवारक मूल्यांकन और डेटा अधिकारी के क्रमिक कार्यों का विवरण देता है। आधिकारिक ऑनलाइन स्रोत

[20]चिली. Ley 21.719, जो व्यक्तिगत डेटा संरक्षण संबंधी Ley 19.628 में संशोधन करती है। नई व्यवस्था वाले संस्करण का प्रारंभ 01-12-2026 के लिए स्थगित है; उससे पहले उस समय लागू नियम जाँचना होगा और भविष्य के दायित्वों को वर्तमान में लागू नहीं मानना होगा। आधिकारिक ऑनलाइन स्रोत

[21]अर्जेंटीना. Ley 25.326, अद्यतन पाठ। अनुच्छेद 4–6, 9–10, 14–16 और 25: गुणवत्ता, सूचना, सुरक्षा, गोपनीयता, डेटा धारकों के अधिकार और तीसरे पक्ष की ओर से प्रसंस्करण सेवाएँ। आधिकारिक ऑनलाइन स्रोत

[22]कोलंबिया. Ley Estatutaria 1581 de 2012, अनुच्छेद 4, 8, 12, 17–18 और 26: सिद्धांत, अधिकार, सूचना, नियंत्रकों और प्रसंस्करणकर्ताओं के कर्तव्य तथा तीसरे देशों में स्थानांतरण। आधिकारिक ऑनलाइन स्रोत

[23]इक्वाडोर. Ley Orgánica de Protección de Datos Personales, Registro Oficial, Suplemento 459, 26-05-2021। अनुच्छेद 10, 37–44: सिद्धांत, सुरक्षा उपाय, डिज़ाइन से सुरक्षा, जोखिम और घटनाओं से निपटने की प्रक्रिया। आधिकारिक ऑनलाइन स्रोत

[24]यूरोपीय संघ. Reglamento (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से सुरक्षा, प्रसंस्करणकर्ता, सुरक्षा और सुरक्षा उल्लंघनों की अधिसूचना/सूचना। स्पेन में लागू राष्ट्रीय और क्षेत्रीय कानून की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत

सातों कानूनी व्यवस्थाओं के इलेक्ट्रॉनिक दस्तावेज़-नियम निर्णयों का साक्ष्य रखने में मदद करते हैं: मान्यता, आरोपण, अखंडता, मूलरूप, अभिगम्यता और संरक्षण। लेकिन हस्ताक्षर, मुहर या हैश अवैध प्रसंस्करण को वैध नहीं बनाता और न यह साबित करता है कि व्यक्ति ने अधिसूचना समझी। गोपनीयता, रिकॉर्ड की अखंडता और सामग्री की सत्यता का अलग-अलग मूल्यांकन किया जाता है।[25][26][27][28][29][30][31]

अनुलग्नक B. अनुकूलन के लिए तैयार प्रारूप

B.1 प्रसंस्करण गतिविधि का रिकॉर्ड

फ़ील्ड	भूमिका शामिल	स्वीकृत निष्कर्ष
गतिविधि और उत्तरदायी	विशेष कार्य, प्रक्रिया-स्वामी और प्रतिनिधि।	किसी और व्यक्ति को पता चल सकता है कि कौन निर्णय लेता है।
उद्देश्य और आधार	विशेष उद्देश्य, आधार और चार्ट किए हुए जवाबदेही।	इसमें "प्रबंधन" को पूरा उत्तर का रूप में उपयोग नहीं किया जाता।
डेटा और व्यक्ति	फ़ील्ड, संवेदनशीलता, तीसरे पक्ष और प्राथमिकता से सहायता अपेक्षित समूह।	प्रत्येक फ़ील्ड की आवश्यकता समझाई गई है।
प्रवाह और प्रसंस्करणकर्ता	प्रवेश, सिस्टम, पहुंच, स्थानांतरण और गंतव्य।	इसमें निर्यात और बैकअप शामिल है।
संरक्षण और जवाबदार	जवाब, जवाबदेही, विलोपन और सहायता-चैनल।	बिना कारण की "जानकारी" जवाब नहीं।
जोखिम और निष्कर्ष	संभावित नुकसान, उपाय, परिणाम और जवाबदेह जोखिम।	कार्यक्षमता को संक्षेप साझा है।

B.2 डेटा धारक के अनुरोध का प्रारूप

आंतरिक पंजीकरण के लिए काल्पनिक प्रारूप

आईडी: PRIV-DEMO-2026-001
प्राप्ति: [दिनांक, समय, समयक्षेत्र, चैनल]
मूल अनुरोध: [पहुँच, सुधार, विलोपन, विरोध, अन्य]
पहचान: [आनुपातिक विधि; इस पत्रक में दस्तावेज शामिल नहीं]
दायरा: [अवधि, सिस्टम, व्यक्ति और बहिष्करण]
लागू समय-सीमा: [नियम, अनुच्छेद, प्रारंभ और समाप्ति]
खोज: [सिस्टम, फ़िल्टर, प्रसंस्करणकर्ता और बैकअप]
निर्णय: [आधार, समीक्षा, तीसरे पक्ष का डेटा]
की गई कार्रवाइयाँ: [सिस्टम, दिनांक, ऑपरेटर, सत्यापन]
डिलीवरी: [प्रारूप, चैनल, प्राप्तकर्ता, दिनांक और सत्यापन]
लंबित और सीमाएं: [क्या हल नहीं हुआ और क्यों]

[25] मेक्सिको. Código de Comercio de México, अनुच्छेद 89–94 और 1205: तटस्थता, आरोपण, लिखित रूप, मूलरूप, अखंडता, अभिगम्यता और डेटा संदेशों की स्वीकार्यता। आधिकारिक संकलन। आधिकारिक ऑनलाइन स्रोत

[26] कोलंबिया. Ley 527 de 1999, अनुच्छेद 5–13, 16–25 और 28: डेटा संदेश, लिखित रूप, मूलरूप, अखंडता, स्वीकार्यता, संरक्षण, प्रेषण, प्राप्ति और डिजिटल हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[27] इक्वाडोर. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, अनुच्छेद 2, 6–8, 10–16: समकक्षता, लिखित रूप, मूलरूप, संरक्षण, उत्पत्ति, प्रेषण, प्राप्ति और इलेक्ट्रॉनिक हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[28] विनियम (UE) 910/2014 eIDAS, अनुच्छेद 25–26 और 46: प्रारूप के कारण इलेक्ट्रॉनिक हस्ताक्षरों और दस्तावेज़ों के साथ भेदभाव न करना, उन्नत हस्ताक्षर और योग्य हस्ताक्षर के प्रभाव। आधिकारिक ऑनलाइन स्रोत

[29] अर्जेंटीना. Ley 25.506 de Firma Digital, अनुच्छेद 1 और 5–9: डिजिटल दस्तावेज़, अस्वीकृत इलेक्ट्रॉनिक हस्ताक्षर के आधार पर दावा करने का भार और सीमांकित धारणाएँ। आधिकारिक ऑनलाइन स्रोत

[30] चिली. इलेक्ट्रॉनिक दस्तावेज़ों और इलेक्ट्रॉनिक हस्ताक्षर संबंधी Ley 19.799, अनुच्छेद 1–5: समकक्षता, लिखित रूप, साधारण/उन्नत हस्ताक्षर, तिथि और साक्ष्य-मूल्य। आधिकारिक ऑनलाइन स्रोत

[31] पेरू. Reglamento de la IOFE, DS 052-2008-PCM, अनुच्छेद 3 और 4: डिजिटल रूप से हस्ताक्षरित इलेक्ट्रॉनिक दस्तावेज़ों की अपेक्षा और स्वीकार्यता। आधिकारिक ऑनलाइन स्रोत

B.3 सुरक्षा उल्लंघन का कालक्रम

घटना	जानबूझ कर्मचारी	सहयोगी निगरानी
प्रारंभिक संकेत	खाते, मूल मांग, समयक्षेत्र, उत्तरदायी और साक्ष्य।	रिकॉर्ड खोले और संरक्षित करें।
रोकथाम	उपाय, प्राधिकार, दायरा, प्रभाव और चूक साक्ष्य।	संदर्भ को मिटाए बिना नुकसान को सीमित करें।
दायरा	डेटा, व्यक्ति, पहुंच, प्रतिबंध, उपयोग और संदर्भ।	जांचकर्ता को तथ्यों को साथ वर्गीकृत करें।
सुधार	प्रासंगिकता, सामग्री, पैनल, समय और सत्यापन।	स्थानीय कानून। व्यवस्था का पालन करें और आवश्यकता से अधिक जानकारी न दें।
पुनर्प्राप्ति	पुनर्स्थापना, पहुंच, निगरानी और परीक्षण।	जांच कि नियंत्रण काम करता है।
सुधार	कारण, प्रक्रिया में बदलाव, उत्तरदायी और सत्यापन।	दोहराव से बचें, न केवल बंद करें।

B.4 आपूर्तिकर्ता मूल्यांकन

वास्तविक डेटा उपयोग में लाने से पहले जांच-सूची

1. प्रत्येक पक्ष की भूमिका और अनुबंध का उद्देश्य।
2. न्यूनतम डेटा, स्थान, अधिकृत व्यक्ति और उप-प्रसंस्करणकर्ता।
3. प्रमाणीकरण, न्यूनतम विशेषाधिकार, लॉग, एन्क्रिप्शन और कुंजियाँ।
4. सत्यापनयोग्य सुरक्षा साक्ष्य, केवल व्यावसायिक घोषणा नहीं।
5. घटना-चैनल, सामग्री और संचार का प्रमाण।
6. अधिकार-अनुरोधों में सहायता, खोज और मूल स्वरूप में निर्यात।
7. स्थानान्तरण, गारंटी और स्थान परिवर्तन।
8. निकास: प्रारूप, डेटा शब्दकोश, अभिगम्यता और खोलने का परीक्षण।
9. विलोपन, बैकअप और सीमाओं सहित प्रमाण-पत्र।
10. नियमित रूप से समीक्षा और आंतरिक जिम्मेदार।

B.5 विलोपन या अवरोधन का प्रमाण-पत्र

काल्पनिक उदाहरण

विषय: EXP-DEMO-2026-001
दायरा: विपणन-प्रोफ़ाइल और अभियान का निर्यात
कार्रवाई: सक्रिय प्रोफ़ाइल का विलोपन और अपेक्षित रसीद का अवरोधन
प्रणालीः [नाम, संस्करण, स्थान और उत्तरदायी]
निष्पादन: [दिनांक, समयक्षेत्र, ऑपरेटर और विधि]
सत्यापन: [खोज, अनुपस्थिति, पहुँच और परिणाम]
बैकअप: [चक्र, पहुँच और पुनर्स्थापना पर पुनः लागू करना]
प्रसंस्करणकर्ता: [अधिसूचना और उत्तर]
अवशिष्ट संरक्षण: [आधार, उद्देश्य और अवधि]
सीमा: [जो नहीं कहा जा सकता]
समीक्षाः [व्यक्ति, तिथि और लिंक किए गए साक्ष्य]

अनुलग्नक C. शब्दावली और आउटपुट नियंत्रण

पद	इस मैनुअल में व्यावहारिक उपयोग
नियंत्रक	वह व्यक्ति या संस्था जो लागू कानूनी व्यवस्था के भीतर जोखिम और प्रसंस्करण के बारे में निर्णय लेता है।
प्रसंस्करणकर्ता	वह जो नियंत्रक की ओर से उसके निर्देशों के अनुसार प्रसंस्करण करता है और जिसके अपने कर्तव्य भी होते हैं।
डेटा मानचित्रण	आंतरिक जानकारी से संबंध बनाना। समय, पृथक्करण और नियंत्रण आवश्यक है।
पुनर्मानचित्रण	समय में संबंध बनाना। पुरानीपुरानी रूप से जरूरी, परीक्षण और समीक्षा आवश्यक है।
अवरोधन	उचित कारण से आज्ञाकारी हटाए बिना प्रसंस्करण को प्रतिबंधित।

पद	इस मॉड्यूल में व्यावहारिक उपयोग
पारदर्शिता	उपयुक्त दायरे की सीमा संरक्षित और अतःप्रवाहशील।
सुरक्षा उल्लंघन	व्यक्तिगत डेटा की सुरक्षा को प्रभावित करने वाली घटना, इसकी गंभीरता की जांचकर्ता की जाती है।
अनुपालन की लागत	एक रिकॉर्ड जो निर्णय, निष्पादन और परिणाम को समझने की अनुमति देता है, न कि केवल इरादा।

प्रक्रिया समझने से पहले	अपेक्षित उत्तर
कौन से डेटा और कौन से प्रतिभा मौजूद हैं?	फ़ाइलें, बैकअप और आपूर्तिकर्ताओं सहित सूची।
प्रत्येक फ़ाइल क्या जानकारी है?	उद्देश्य, आधार और न्यूनतमकरण दस्तावेज़ित है।
किसको पहुंच हो सकती है और उसका क्या प्रमाण है?	भूमिकाएं, लॉग और कालिमनिक डेटा से परीक्षण।
एक व्यक्ति अपने अधिकारों का प्रयोग कैसे करता है?	पैनल, खोज, निर्णय, वितरण और निष्पादन।
घटना या निकास की स्थिति में क्या होता है?	कॉलेक्शन, सुधार, निर्यात और विलोपन सत्यापित है।
क्या पता नहीं चला?	स्पष्ट सीमा, उत्तरदायी और जांचा गया।

सारांश

डेटा सुरक्षा का अर्थ है किसी संगठनात्मक निर्णय के व्यक्ति की क्षति में बदलने की संभावना घटाना। साक्ष्य इस सावधानी की समीक्षा और सुधार के लिए होता है, उसे प्रशासनिक दिखावे में बदलने के लिए नहीं।