Self-Hosting als berufliche Praxis

Ein Server ist nichts weiter als ein Computer. Die Frage ist nicht, ob man einen haben sollte, sondern wo die Daten Ihrer Kunden leben, wer sie instand hält und wer die Verantwortung übernimmt, wenn etwas schief geht.

Um es kurz zu machen: Ihre Daten leben immer auf dem Computer von jemandem: auf dem eines Riesen, dem Sie alles anvertrauen, auf einem gemieteten, den Sie verwalten, oder auf Ihrem eigenen. Je mehr Kontrolle Sie wollen, desto mehr Verantwortung übernehmen Sie. Die Delegation an einen großen Dritten beruhigt, entbindet aber nicht: Die Information gehört Ihnen — und Ihren Kunden — und die verantwortliche Person sind Sie.

Die Frage zwischen Cloud und Keller

Es ist gut, mit der Entmystifizierung eines Wortes zu beginnen, das ohne Grund Angst macht: Server. Ein Server ist keine mysteriöse Maschine in einem gekühlten Raum. Er ist ganz einfach der Computer einer anderen Person — oder Ihr eigener —, der Informationen speichert und sie demjenigen übergibt, der sie anfordert. Jahrzehntelang haben wir die Informationen unserer Kunden in einem Ordner, in einem Karteischrank, auf dem Schreibtisch aufbewahrt, und niemand hat deswegen schlecht geschlafen. Informationen waren nicht beängstigend, weil sie auf Papier waren; sie müssen es auch nicht sein, nur weil sie auf einer Festplatte sind.

«Die Cloud» ist auch nicht ätherisch. Es ist der Computer eines Unternehmens, fast immer weit weg und fast immer der eines anderen. Ich habe das unfreiwillig an dem Tag gelernt, als ich im Vertrauen darauf, dass meine Dateien bei Google Drive sicher seien, entdeckte, dass der Ordner auf meinem Computer nicht meine Dokumente enthielt, sondern Verknüpfungen zu Dokumenten, die ganz woanders lebten. Wenn dieser andere Ort entscheiden würde zu schließen, den Preis zu ändern oder den Dienst zu kündigen, wäre mein Seelenfrieden mit ihm dahin. Ich besaß meine Sachen nicht: ich hatte die Erlaubnis, auf sie zuzugreifen.

Daraus entsteht die Frage dieses Heftes, die einfacher zu stellen als zu beantworten ist: Wo sollten die Daten Ihrer Kunden leben? Und Ihre eigenen? Die öffentliche Diskussion stellt es so dar, als gäbe es nur zwei gegensätzliche Antworten — die Cloud der großen Plattformen oder der Eigenbau —, fast eine Frage der Lagerzugehörigkeit. Aber es sind nicht zwei Wege: es sind drei, und keiner ist ein Glaubensakt. Bei genauem Hinsehen haben sie mehr Nuancen und verlangen mehr, als es scheint.

Dies betrifft Sie, egal was Sie verkaufen

Man denkt leicht, dass Vertraulichkeit eine Angelegenheit von Anwälten, Ärzten oder Journalisten sei und dass der Rest nichts zu verbergen habe. Das ist ein Fehler, und ein teurer dazu. Fast jedes Unternehmen bewahrt gesetzlich geschützte Kundendaten auf, und viele bewahren, ohne es zu wissen, Informationen auf, die weit sensibler sind, als es den Anschein hat.

Ein Sofaladen notiert sich Namen, Adresse und Telefonnummer des Käufers; bei einer Finanzierung auch dessen Wirtschaftsdaten. Ein Renovierungs- oder Dekorationsunternehmen bewahrt Fotos aus dem Inneren der Häuser seiner Kunden und komplette Pläne ihrer Wohnungen auf. Ein Reinigungsunternehmen verwaltet Pläne der Büros, die es reinigt, oft markiert mit Farben und Nummern, die angeben, welcher Mitarbeiter wo, zu welcher Zeit und mit welchem Schlüssel eintritt. Nichts davon scheint eine große Sache zu sein, bis man fragt, für wen es

sonst noch von Wert wäre: Diese Reinigungspläne sind, mit anderen Augen gesehen, die perfekte Karte für jeden, der einbrechen möchte, um zu stehlen.

Dass ein Unternehmen klein ist oder Sofas verkauft, anstatt Prozesse zu führen, macht seine Daten nicht wertlos und führt auch nicht dazu, dass das Gesetz nicht mehr für es gilt. Es führt nur dazu, dass sein Eigentümer dazu neigt, weniger darüber nachzudenken. Und wenig über etwas nachzudenken, das in Ihrer Verantwortung liegt, ist genau der Punkt, an dem die Probleme beginnen.

Wo leben Ihre Daten?

Auf diese Frage gibt es im Wesentlichen drei Antworten. Und es ist gut, sich daran zu erinnern, dass «die Daten» nicht nur das Dossier eines Kunden oder der Block von Rechnungen und Angeboten sind: es sind auch Ihre Gespräche mit ihm — über WhatsApp, über einen professionellen Chat-Dienst, über Solo2. Die drei folgenden Antworten sind keine Reinheitsgrade oder eine Stufenleiter von gut bis schlecht: es sind drei verschiedene Arten, dasselbe — Kontrolle und Verantwortung — aufzuteilen.

Alles an einen Anbieter delegieren. Dies ist der häufigste Fall und für die Mehrheit das Einzige, was sie kennen. Ich lege alles in die Google Workspace oder Microsoft 365 und vertraue es ganz dem Anbieter an. Ich zahle meine Gebühr und denke nicht mehr darüber nach. Die extremste Form davon sind Dienste, bei denen Sie nicht einmal mehr über Ihre Daten verfügen: Bestimmte Abrechnungsprogramme in der Cloud zum Beispiel speichern Rechnungen und Angebote für Sie — und funktionieren sehr gut —, aber die Informationen leben in deren System, nicht in Ihrem. Solange Sie zahlen, haben Sie Zugriff; am Tag, an dem Sie gehen, stellen Sie fest, dass es schwierig oder unmöglich ist, Ihre eigene Historie mitzunehmen. Ihre Daten quasi als Geisel zu haben, ist für manchen Anbieter genau das, was Sie davon abhält, zur Konkurrenz zu wechseln. Im Austausch für Komfort gebe ich die Kontrolle ab und — ohne es laut auszusprechen — das Gefühl, dass die Verantwortung nicht mehr bei mir liegt. Hier gibt es eine Nuance, die fast nie gemacht wird: Delegieren ist nicht gleichbedeutend mit „amerikanisch“. Ich kann alles ebenso bequem an einen europäischen Anbieter delegieren — zum Beispiel Infomaniak — und mit einem Schlag einen Großteil der Zweifel an internationalen Übermittlungen lösen, die wir in «Schrems II» gesehen haben, ohne selbst etwas zu hosten. Es geht nicht um USA gegen den Rest des Universums: Innerhalb der reinen Delegation gibt es bereits Entscheidungen, die zählen.

Einen eigenen Server mieten und verwalten. Ich habe dasselbe, was mir Microsoft oder Google geben würden, aber ich baue es selbst auf. Ich miete einen Server bei einem europäischen Anbieter — Hetzner, OVH, Scaleway —, installiere freie Software (zum Beispiel Nextcloud für Dateien) und verwalte das Ergebnis selbst. Ich gewinne echte Kontrolle: Ich weiß, was läuft, wo und warum. Aber die Maschine befindet sich immer noch im Rechenzentrum eines Dritten und vor allem ändert sich, wer die Konsequenzen trägt. Durch Delegieren haben Sie jemanden, dem Sie die Schuld geben können, wenn etwas schief geht. Durch Selbstverwaltung ist die Wahrscheinlichkeit hoch, dass die Schuld bei Ihnen liegt.

Es auf dem eigenen Computer haben. Dies ist die Option, von der fast niemand erzählt, und sie ist das Herzstück dieses Heftes. Man braucht keinen riesigen Server, der vierundzwanzig Stunden am Tag in einem Makro-Rechenzentrum läuft, um seine Sachen zu hosten. Ihr Bürocomputer ist bereits ein Server: Er dient Ihnen. Sie lassen ihn im Büro eingeschaltet und verbinden sich von Ihrem Laptop beim Kunden oder vom Handy aus, wenn Sie zu Hause sind. Wir nennen es «Bürocomputer», nicht «Server», aber er tut genau das gleiche wie die beiden vorherigen Optionen. Die Kontrolle ist maximal und die Nähe ebenso: Ihre Daten sind dort, wo Sie sind. Die Kehrseite der Medaille, ungeschminkt gesagt, ist, dass auch die Verantwortung maximal ist. Wenn der Strom ausfällt, gibt es keinen Bereitschaftstechniker in Nürnberg: Es liegt an Ihnen, die Sicherung wieder einzulegen. Und damit dieser Computer von außen erreichbar ist, braucht es etwas, das die Brücke zwischen Ihrem Laptop und ihm schlägt. Das ist keine Magie, und es ist gut, das zu wissen, bevor man diesen Weg wählt.

Und Sie müssen nicht einmal den Bürocomputer weiterverwenden: Es gibt ein Gerät, das genau dafür gedacht ist, das NAS (hergestellt von Synology, QNAP und anderen). Wie fast alles, was wir in diesen Cuadernos gesehen haben, steckt im Inneren keine Magie: Es ist ein spezialisierter Computer, dieselbe Art von Maschine, die Sie in einem Rechenzentrum mieten würden, nur dafür gebaut, Daten zu speichern und sie über das Netzwerk

bereitzustellen, ohne Monitor oder Tastatur dazwischen. Schließen Sie einen Bildschirm und eine Tastatur an und Sie haben einen gewöhnlichen Computer; installieren Sie die passende Software auf Ihrem PC und Sie haben ein NAS. Der Unterschied ist, dass das NAS bereits einsatzbereit geliefert wird. Sie kaufen es, schließen es zu Hause oder im Büro an, und es gehört Ihnen. Sie zahlen keine monatliche Gebühr; Sie zahlen einmal und es gehört Ihnen, wie jedes andere Werkzeug Ihres Unternehmens. Sie schalten es ein, schalten es aus, nehmen es bei Bedarf woanders hin mit. Und da es Ihnen gehört, hindert Sie nichts daran, zwei zu haben —eines zu Hause, eines im Büro— oder drei, indem Sie eines an einem sicheren Ort hinzufügen, miteinander synchronisiert: Ihre eigene Redundanz, ohne darauf angewiesen zu sein, dass ein Dritter sie pflegt. Selbst-Hosting ist letztlich nicht eine einzige Sache: Es ist eine Kombination aus Maschinen, aus Eigentum, aus Standorten und aus Software.

Hier ist es unumgänglich, das zu benennen, was wir tun, und wir tun es ohne Maske: In Solo2 wird diese Brücke von der Anwendung selbst geschlagen. Ihr Bürocomputer bleibt nur für Ihre vertrauenswürdigsten Geräte erreichbar, und das immer unter Verschlüsselung, und Ihre anderen Geräte verbinden sich von selbst wieder mit ihm. Wenn ein Kunde mit Ihnen spricht, ist es Ihr Computer — nicht der eines Dritten —, der mit dem Kunden spricht. Wir lösen nicht den Stromausfall; wir lösen die Brücke. Und wir sind nicht die Einzigen: für fast jedes Bedürfnis gibt es heute Programme — frei oder proprietär —, die genau dies ermöglichen: die Daten auf dem eigenen Gerät zu haben und von außen darauf zuzugreifen. Unser Programm ist ein Beispiel; wichtig ist die Idee, nicht die Marke.

Redundanz ist keine Superkraft

Hier erhebt sich der unmittelbare Einwand, und er ist berechtigt: Wenn ich alles auf meinem Bürocomputer habe, was passiert, wenn er kaputt geht? Die Frage ist gut. Die Antwort ist, dass das Sicherheitsnetz, das wir uns bei den großen Anbietern vorstellen, bescheidener — und leichter nachahmbar — ist, als es scheint.

Wenn ich meine Daten im Rechenzentrum eines multinationalen Konzerns lasse, vertraue ich darauf, dass dieser Kopien an mehreren Orten hat. Und wahrscheinlich hat er sie: an einem zweiten Standort, vielleicht an einem dritten. Aber diese Redundanz ist nicht unendlich und vor allem ist sie nicht meine: Es bleibt eine Festplatte, deren Eigentümer ich nicht bin, verwaltet von jemandem, dem ich ein Vertrauen schenke, das ich fast nie überprüfe.

Dasselbe Netz kann ich selbst weben, und mit einem entscheidenden Vorteil. Mein täglicher Dienst lebt auf dem Bürocomputer. Von dort aus bewahre ich eine verschlüsselte Kopie auf dem Computer einer befreundeten Firma auf — eines Berufskollegen, eines anderen vertrauenswürdigen Büros — und eine weitere verschlüsselte Kopie, wenn ich will, bei demselben europäischen Anbieter, von dem wir gesprochen haben. Der Unterschied ist alles: Was ich draußen lasse, ist nicht mein Dienst und auch nicht meine Daten im Klartext, sondern eine verschlüsselte Kopie, die nur ich öffnen kann. Der externe Anbieter bewahrt eine verschlossene Truhe auf, für die er keinen Schlüssel hat. Ich vertraue ihm meine Informationen nicht an: Ich vertraue ihm einige Bytes an, die ohne mich nichts bedeuten.

Es war sicher, bis es das nicht mehr war

Lassen Sie mich eine persönliche Geschichte erzählen, denn sie illustriert dies besser als jedes Argument. Über zehn Jahre lang war ich ein treuer Kunde von CrashPlan, einem technisch außergewöhnlichen Backup-Dienst. Ich sicherte in deren Cloud alle meine Computer und die meiner Familie — die der Firma und die von zu Hause, alles —, mit Versionen, die ich in jeder gewünschten Häufigkeit wiederherstellen konnte, wobei ich in der Zeit bis zu einer spezifischen Datei von vor Monaten zurückreisen konnte. Nach der ersten Kopie wurden nur die Änderungen verschlüsselt und komprimiert übertragen, sodass ich ohne nennenswerten Aufwand ein riesiges Backup auf dem neuesten Stand hielt. Es hat mich oft gerettet, von einem unbedeutenden Dokument bis hin zu einer ganzen Festplatte. Der Preis stieg im Laufe der Jahre und es war mir egal: Ich zahlte gerne.

Was ich nicht wusste, war, dass CrashPlan einen Rechenfehler gemacht hatte: Sie hatten vertraglich unbegrenzten Speicherplatz versprochen, sowohl räumlich als auch zeitlich. Und Raum multipliziert mit Zeit —

Jahre an Historie, Versionen alle paar Minuten — wächst, bis es unhaltbar wird. Eines Tages teilten sie uns allen mit, dass der Dienst eingestellt wird. Sie taten dies mit Eleganz und einer großzügihen Frist von fast einem Jahr und gaben uns die Mittel, unsere Daten herunterzuladen. Aber wo geht man hin mit mehr als zehn Jahren versionierter Kopien aller seiner Festplatten? Da stellt man fest, dass man weder die Möglichkeit hat, alles herunterzuladen, noch einen Platz, um es unterzubringen, und dass, selbst wenn man es könnte, das neue Lager ein Vermögen kosten würde.

Ich rettete vier lebensnotwendige Dinge. Der Rest war weg, als sie den Schalter umlegten. Ich war beruhigt, meine Informationen waren sicher ... bis sie es nicht mehr waren. Und nicht wegen eines Verrats: CrashPlan hat sich tadellos verhalten — im Gegensatz zu Evernote, das Jahre später eine Schande war —; mein Schutzengel in der Cloud entschied einfach mit vollem Recht, keiner mehr zu sein. Das Ergebnis für mich war identisch: Was ich für sicher hielt, verschwand.

Was diese Geschichte wirklich lehrt, hat mehr mit der menschlichen Natur als mit Technik zu tun. Wenn jemand fühlt, dass etwas in seiner Verantwortung liegt, handelt er präventiv: Er macht Kopien, sichert sich ab, ist mit gutem Urteilsvermögen misstrauisch. Wenn er — fälschlicherweise — glaubt, dass die Verantwortung von einem großen und solventen Dritten getragen wird, entspannt er sich und lässt die Dinge laufen. Diese delegierte Ruhe ist keine Vorsicht: Sie ist, ungeschminkt, eine Form von Verantwortungslosigkeit.

Bezahlen ist nicht dasselbe wie Erfüllen

Diese stille Verantwortungslosigkeit ähnelt sehr der von Eltern, die ihren Sohn an der teuersten Schule anmelden, ihm danach ein Masterstudium bezahlen und damit glauben, ihre Pflicht erfüllt zu haben. Das haben sie nicht. Eltern zu sein bedeutet, sich darum zu kümmern, was er heute gelernt hat, was er nicht versteht, um seine Werte, sein Selbstvertrauen. Wenn dieser Sohn mit fünfundzwanzig Jahren weder zu arbeiten noch sich zu benehmen weiß, liegt die Schuld nicht bei der Schule, die das Geld kassiert hat: Sie liegt bei demjenigen, der delegiert und bezahlt hat im Glauben, dass das genug sei. Die Zahlung an einen Dritten entbindet nicht von der Verantwortung. Das hat sie nie getan.

Mit Daten verhält es sich genauso, und die jüngere Geschichte bestätigt dies. Vor fünfzig oder hundert Jahren bewahrte ein Fachmann das Seine seiner Kunden in Ordnern, in seinem Büro oder bei sich zu Hause auf und fühlte sich für sie verantwortlich. Selten ging etwas verloren. Wir sind in die digitale Welt übergegangen und mit einer erstaunlichen Leichtigkeit laden wir alles in «die Cloud» hoch — was nichts anderes als der Computer eines multinationalen Konzerns ist — und hören auf, uns Sorgen zu machen. Und oft passieren Unfälle, und es gibt Unternehmen, die alles verlieren, und dann heißt es: Schuld war Google, Schuld war Microsoft. Nein. Die Information gehört Ihnen oder Ihren Kunden, aber der Verantwortliche sind Sie.

Das Hosten des Seinen ist keine technische Laune: Es ist die Wiedergewinnung jener Gelassenheit von vor Jahrzehnten, zu wissen, wo sich jedes Ding befindet und warum. Der Datenschutz hat unterdessen eine abrupte Pendelbewegung erlebt — von der Abwesenheit jeglicher Norm, als jeder ohne Nachzudenken Kundendaten zur Schau stellte, bis hin zu einer Anforderung, die mit unverhältnismäßiger Härte den Kleinsten trifft, den Freiberufler, der dem Boten die Telefonnummer eines Kunden gibt. Ich diskutiere nicht über das Ziel; ich beobachte das Missverhältnis. Aber das Missverhältnis entbindet uns nicht: An dem Tag, an dem die Verwaltung über die Mittel verfügt, in großem Stil nachzuverfolgen und zu sanktionieren, wird die Größe niemanden mehr schützen, und es ist klug, diesen Tag nicht mit einem unordentlichen Haus abzuwarten. Die Daten unter eigener Kontrolle zu haben, hilft bei der Einhaltung und hilft, diese nachzuweisen. Und vor allem rückt es die Dinge wieder an ihren Platz: Wenn die Information Ihnen gehört, liegt die Verantwortung vollständig bei Ihnen — es gibt keinen Dritten, dem man die Schuld geben könnte, und keinen Dritten, dessen Versagen Sie gefährdet.

Die Verantwortung schützt auch

Es wäre unredlich, dies ohne Schatten zu malen. Den Platz des Vermittlers einzunehmen bedeutet, dessen Last zu tragen: Kopien aktuell zu halten, Updates anzuwenden und eine rechtliche Verantwortung —die der DSGVO—,

die in Wirklichkeit nie ganz aufgehört hat, die Ihre zu sein (die Referenzen am Ende führen die Artikel im Detail auf). Es gibt Arbeit, und es gibt den Tag, an dem zur Unzeit etwas schief geht. Wir verheimlichen es nicht.

Aber die Angst, die dieses Wort, Verantwortung, umgibt, ist falsch kalibriert. Es ist viel einfacher, Ihre Dateien bei einem Cloud-Dienst zu verlieren, der schließt, oder Ihre Fotos bei Google Fotos, als diesen Ordner mit wichtigen Dokumenten zu verlieren, den Sie auf Ihrem eigenen Computer haben: den, von dem Sie wissen, wo er ist, und bei dem Sie sofort merken würden, dass er fehlt, sobald er verschwindet. Was man als sein Eigen empfindet, das pflegt man; was man in den Händen eines anderen in Sicherheit glaubt, das vernachlässigt man.

Denken Sie an die Fotoalben von früher, die aus entwickeltem Papier in einer Schublade. Haben Sie jemals jemanden sagen hören, dass er sein Familienalbum «verloren» hat? Man hört von dem Haus, das mit dem Album darin abgebrannt ist; es einfach so zu verlieren, nein. Und im Gegensatz dazu Leute, die alle ihre Fotos bei Google Fotos oder Apple Fotos hatten und plötzlich vor dem Nichts standen: diese Geschichte kehrt alle paar Monate zurück, weil sie glaubten, es sei sicher. Google Fotos hütet Ihre Fotos, natürlich; aber es hütet sie nicht so, wie Eltern das Album hüten, in dem ihre Kinder und Enkelkinder sind. Dieser Unterschied lässt sich durch kein Rechenzentrum beheben: Die Verantwortung ist, wenn es die Ihre ist, nicht nur eine Last; sie ist auch die beste Garantie.

Vier Fragen vor der Entscheidung

Wenn Sie erwägen, diesen Schritt in einer seiner Formen zu tun, ist es gut, zuerst vier Fragen mit leidenschaftsloser Ehrlichkeit zu beantworten:

1. Welcher Teil Ihrer Daten würde Ihnen wehtun, wenn Sie ihn verlieren oder nicht mitnehmen könnten? Und Vorsicht davor, das «Routinemäßige» abzutun: die Rechnungshistorie erscheint als das Alltäglichste der Welt, bis man das Programm wechselt und feststellt, dass diese Rechnungen dem Anbieter gehörten, nicht Ihnen — dass man sie allenfalls als PDF ausdrucken kann, ohne darin noch suchen zu können. Es ist nicht nur eine Frage der Sensibilität: es ist eine Frage dessen, wem das, was Sie aufbewahren müssen, wirklich gehört.
2. Welche Option steht im Verhältnis zu Ihrer tatsächlichen technischen Kapazität? Ein gut gepflegter eigener Computer ist für jeden erreichbar; einen ganzen Server zu verwalten, weniger. Seien Sie ehrlich darüber, was Sie wissen und was nicht. Und denken Sie daran, dass es zwischen dem Aufbau eines ganzen Servers und der vollständigen Delegation einen sehr vernünftigen Mittelweg gibt: Programme — freie oder proprietäre —, die Ihre Daten auf Ihrem eigenen Gerät speichern und Sie von außen darauf zugreifen lassen. Für viele Leute ist das das beste Gleichgewicht.
3. Welchen Plan haben Sie für den schlimmsten Tag? Eine Sicherheitsverletzung, eine sterbende Festplatte, ein Anbieter, der schließt, der Techniker ist krankgeschrieben. Wenn der Plan mit „das sollte nicht passieren“ beginnt, ist es kein Plan.
4. Wüssten Sie nachzuweisen, dass Sie die Regeln einhalten, wenn Sie morgen kontrolliert würden? Etwas gut zu machen und nachweisen zu können, dass man es gut macht, ist nicht dasselbe. Das Gesetz verlangt Letzteres.

Es gibt keine universelle Antwort. Es gibt eine angemessene Antwort, die mit Ehrlichkeit darüber angenommen wurde, was man gewinnt und was man als Verantwortung erbt. Und über der Technik steht eine einfache Gewissheit: Ihre Daten leben auf dem Computer von jemandem. Die einzige Frage, die wirklich zählt, ist, wessen Computer das Ihrer Meinung nach sein soll.

Self-Hosting ist weder eine Tugend noch ein Laster: Es ist ein Werkzeug mit einem konkreten Profil an Fähigkeiten und Verantwortlichkeiten. Die Frage war nie, ob Sie das Ihre hosten sollten, sondern was, wie und mit welchem Unterstützungsnetzwerk. Die Kontrolle über die Daten zurückzugewinnen bedeutet nicht, in den Keller zurückzukehren oder allem zu misstrauen: Es bedeutet, sich wieder für das verantwortlich zu fühlen, was uns gehört, so wie damals, als jenes in einem Ordner auf dem Schreibtisch lebte. Diese Verantwortung ist, richtig verstanden, die eigentliche Dienstleistung, die ein Fachmann seinen Kunden erbringt.

Quellen und weiterführende Literatur

- Verordnung (EU) 2016/679 — Artikel 28 (Auftragsverarbeiter), Artikel 32 (Sicherheit der Verarbeitung), Artikel 33 (Meldung von Verletzungen), Artikel 37 (Benennung eines Datenschutzbeauftragten).
- Spanische Datenschutzagentur (AEPD) — *Praktischer Leitfaden zur Risikoanalyse bei der Verarbeitung personenbezogener Daten* (aktuelle Fassung). Rahmen für Verantwortliche, die eigene technische Funktionen übernehmen.
- Europäischer Datenschutzausschuss — *Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage berechtigter Interessen*. Auch anwendbar für die Verhältnismäßigkeitsprüfung bei Entscheidungen über die eigene Infrastruktur.
- Europäische Kommission — öffentliches Verzeichnis der in europäischer Gerichtsbarkeit ansässigen Informationsdienstleister. Administrativer Ausgangspunkt zur Identifizierung europäischer Managed-Hosting-Optionen.
- Nextcloud GmbH (Deutschland) — *Nextcloud Enterprise Architektur und Compliance-Dokumentation*. Dokumentierter Fall freier Software mit Self-Hosted- und von einem europäischen Anbieter verwalteten Modellen; nützlich als technische Referenz eines seit 2016 in europäischer Gerichtsbarkeit unterhaltenen Projekts.

← ZurückDie 24 Wörter: Was eine kryptografische Identität istWeiter →Echte vs. scheinbare Privatsphäre: Die Fragen, die man sich stellen sollte

Aktuelle Lektüre

- Reflexion · 29. Juni 2026 Du bist nicht anonym
- Reflexion · 27. Mai 2026 Was eine Unterschrift nicht in Ordnung bringen kann
- Analyse · 26. Mai 2026 Echte vs. scheinbare Privatsphäre: Die Fragen, die man sich stellen sollte

Nehmen Sie diesen Artikel mit, wohin Sie ihn brauchen.

↓ Markdown ↓ Klartext ↓ PDF

Die Datei wird auf Ihr Gerät heruntergeladen. Von dort aus können Sie sie speichern, in Solo2 importieren oder teilen, wo immer Sie möchten. Cuadernos entscheidet nicht über den Zielort für Sie.

Siegellack-Siegel · SHA-256 812e6499a71d3cf47b6b9b86ec796a54ad0850c0265a39c0c6d9c230ee70b40b

Cuadernos Lacre · Eine Publikation von Menzuri Gestión S.L. ·
geschrieben von R.Eugenio · herausgegeben vom Team von Solo2.