

ISO/IEC 27018:2025, Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre: Leitfaden zum Schutz personenbezogener Daten (PII) in Public Clouds, die als PII-Auftragsverarbeiter handeln (3. Ausgabe, 2025-08)

PII-Schutz in der Public Cloud

36 Anforderungen. Für diese Norm gibt es kein akkreditiertes Zertifikat. Stand 07/2026.

ISO/IEC 27018 ist kein Managementsystem-Standard, sondern ein Leitfaden mit erweiterten Maßnahmen zu ISO/IEC 27002:2022. Es gibt kein eigenständiges, akkreditiertes Zertifikat nach ISO/IEC 27018: Die Maßnahmen werden in die Erklärung zur Anwendbarkeit eines ISO/IEC 27001-Systems aufgenommen, das Zertifikat lautet dann auf ISO/IEC 27001 mit Verweis auf ISO/IEC 27018. Adressat der Norm ist der Anbieter eines öffentlichen Cloud-Dienstes, der personenbezogene Daten im Auftrag seiner Cloud-Kunden verarbeitet. Wer Cloud-Dienste lediglich nutzt, nimmt diese Rolle nicht ein und prüft die Anforderungen sinnvollerweise gegen seine Anbieter, nicht gegen sich selbst. Für Leanshift ist diese Checkliste damit vor allem ein Lieferanten-Prüfraster: Jeder Punkt lässt sich als Frage an den Anbieter stellen und über den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO absichern. Ergebnis einer Prüfung ist ein interner Konformitätsnachweis oder ein Anbieter-Bewertungsprofil, kein Zertifikat. Zur Nummerierung: Kapitel A.2 bis A.12 folgen den Datenschutzgrundsätzen im Anhang A der Norm, Punkte mit Nummern wie A.11.6 sind die dort aufgeführten Zusatzmaßnahmen. Punkte mit Nummern wie 8.10 oder 5.34 verweisen auf Maßnahmen aus ISO/IEC 27002:2022, die die Norm für die Cloud konkretisiert. Punkte mit dem Zusatz Grundsatz leiten sich aus dem Grundsatz des Kapitels ab, für den der Anhang A keine eigene Zusatzmaßnahme führt.

Betrieb	Datum	Bearbeiter
---------	-------	------------

A.2 Einwilligung und Wahlmöglichkeit2

A.2.1Der Cloud-Anbieter unterstützt den Cloud-Kunden dabei, die Rechte der betroffenen Personen zu erfüllen, etwa Auskunft, Berichtigung, Löschung und Widerspruch. Zuständigkeiten und Fristen sind vertraglich geregelt.

Dokument

Woran man es festmacht: Beleg ist der Auftragsverarbeitungsvertrag nach Art. 28 DSGVO mit einer Klausel zur Unterstützung bei Betroffenenrechten, ergänzt um die technischen Mittel im Dienst selbst: Export-, Korrektur- und Löschfunktion oder eine dokumentierte Support-Prozedur mit Reaktionsfrist. Anbieterfrage: Welche Funktion oder welchen Prozess stellen Sie bereit, damit wir ein Auskunfts- oder Löschbegehren innerhalb eines Monats bedienen können?

Offen	In Arbeit	Erfüllt	Nicht anwendbar
-------	-----------	---------	-----------------

Nachweis / Begründung

A.2 (Grundsatz)Personenbezogene Daten der Cloud-Kunden werden ausschließlich auf Weisung des Kunden verarbeitet. Eine Einwilligung der betroffenen Personen einzuholen bleibt Sache des Kunden als Verantwortlicher, der Anbieter greift dem nicht vor.

Woran man es festmacht: Beleg ist die Weisungsklausel im Auftragsverarbeitungsvertrag plus ein Nachweis, dass es keine anbieterseitige Zweitnutzung gibt, etwa die Datenschutzerklärung des Dienstes und die Produktdokumentation. Anbieterfrage: Verarbeiten Sie unsere Kundendaten in irgendeiner Form außerhalb unserer Weisung, zum Beispiel für Produktverbesserung oder Modelltraining?

Offen	In Arbeit	Erfüllt	Nicht anwendbar
-------	-----------	---------	-----------------

Nachweis / Begründung

A.3 Zweckbindung und Rechtmäßigkeit2

A.3.1Der Zweck der Verarbeitung personenbezogener Daten durch den Anbieter ist auf die Erbringung des vereinbarten Dienstes begrenzt und im Vertrag benannt. Eine Verarbeitung für eigene Zwecke des Anbieters findet nicht statt.

Dokument

Woran man es festmacht: Beleg ist der Auftragsverarbeitungsvertrag mit Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie der Kategorien betroffener Personen nach Art. 28 Abs. 3 DSGVO. Anbieterfrage: Bitte um die Vertragsanlage, die den Verarbeitungszweck abschließend beschreibt. Für kleine Betriebe genügt das Standard-Data-Processing-Addendum des Anbieters, sofern es diese Angaben enthält.

Offen	In Arbeit	Erfüllt	Nicht anwendbar
-------	-----------	---------	-----------------

Nachweis / Begründung

A.3.2	Eine Nutzung der anvertrauten personenbezogenen Daten für Werbung, Marketing oder sonstige kommerzielle Eigenzwecke des Anbieters erfolgt nicht ohne vorherige ausdrückliche Einwilligung. Die Erbringung des Dienstes ist nicht an eine solche Einwilligung gekoppelt.
	Woran man es festmacht: Beleg ist eine ausdrückliche Vertragsklausel, die kommerzielle Zweitnutzung ausschließt, sowie die Nutzungsbedingungen des Dienstes. Anbieterfrage: Bestätigen Sie schriftlich, dass Kundendaten nicht für Werbung, Profilbildung oder das Training von KI-Modellen verwendet werden. Fehlt diese Zusage, ist der Dienst für personenbezogene Daten ungeeignet.
	Offen In Arbeit Erfüllt Nicht anwendbar
	Nachweis / Begründung

A.4 Beschränkung der Erhebung1	
A.4 (Grundsatz)	Der Anbieter erhebt über die vom Kunden eingestellten Daten hinaus keine weiteren personenbezogenen Daten für eigene Zwecke, etwa Telemetrie, Nutzungsprofile oder Inhaltsauswertungen. Erhobene Betriebs- und Metadaten sind benannt und begründet.
	Woran man es festmacht: Beleg ist eine Aufstellung der Daten, die der Dienst neben den Inhaltsdaten erfasst (Zugriffsprotokolle, Telemetrie, Diagnosedaten), mit Zweck und Speicherdauer, plus die Einstellmöglichkeit zum Abschalten optionaler Telemetrie als Screenshot. Anbieterfrage: Welche Nutzungs-, Telemetrie- und Diagnosedaten erheben Sie zusätzlich, wofür verwenden Sie diese, und können wir die Erhebung abschalten?
	Offen In Arbeit Erfüllt Nicht anwendbar
	Nachweis / Begründung

A.5 Datenminimierung2	
A.5.1	Temporäre Dateien, die bei der Verarbeitung personenbezogener Daten entstehen, etwa Zwischenspeicher, Caches oder Rollback-Journale, werden innerhalb eines festgelegten Zeitraums sicher gelöscht.
	Woran man es festmacht: Beleg ist eine Betriebs- oder Löschroutine mit benannter Aufbewahrungsfrist für temporäre Daten, ergänzt durch die Konfiguration der Systeme, etwa Cache-TTL oder ein geplanter Bereinigungsjob mit Ausführungsprotokoll. Anbieterfrage: Nach welcher Frist werden Caches, temporäre Dateien und Zwischenstände gelöscht, und wie wird das überwacht?
	Offen In Arbeit Erfüllt Nicht anwendbar
	Nachweis / Begründung
8.11 Wo für Betrieb, Test oder Support keine Echtdateien nötig sind, werden personenbezogene Daten maskiert, pseudonymisiert oder anonymisiert. Der Umfang verarbeiteter Daten bleibt auf das für den Dienst Erforderliche begrenzt.	
	Woran man es festmacht: Beleg ist eine Festlegung, welche Umgebungen Echtdateien sehen dürfen, plus Screenshots oder Skripte der Maskierung in Test- und Entwicklungssystemen. Anbieterfrage: Arbeiten Ihre Support- und Entwicklungsteams mit Produktivdaten, und wenn ja, unter welchen Schutzmaßnahmen? Für kleine Betriebe reicht die Regel, dass Testsysteme ausschließlich mit erzeugten Beispieldaten laufen.
	Offen In Arbeit Erfüllt Nicht anwendbar
	Nachweis / Begründung

A.6 Begrenzung von Nutzung, Aufbewahrung und Offenlegung3	
A.6.1	Erhält der Anbieter eine rechtlich verbindliche Anfrage zur Offenlegung personenbezogener Daten, etwa von einer Behörde, informiert er den Cloud-Kunden vorab, soweit dies gesetzlich zulässig ist.
	Woran man es festmacht: Beleg ist eine vertragliche Benachrichtigungsklausel und ein interner Prozess für behördliche Anfragen mit benannter Zuständigkeit. Anbieterfrage: Benachrichtigen Sie uns vor einer Datenherausgabe, und veröffentlichen Sie einen Transparenzbericht über behördliche Anfragen? Ein aktueller Transparenzbericht ist ein starker Beleg.
	Offen In Arbeit Erfüllt Nicht anwendbar
	Nachweis / Begründung

A.6.2

8.10

<

A.7 Richtigkeit und Qualität 2

A.7 (Grund)	Der Anbieter verändert die anvertrauten personenbezogenen Daten nicht eigenmächtig. Berichtigungen und Aktualisierungen erfolgen ausschließlich auf Weisung des Cloud-Kunden oder über Funktionen, die der Kunde selbst bedient.			
	Woran man es festmacht: Beleg sind die Bearbeitungsfunktionen des Dienstes samt Änderungshistorie sowie die Weisungsklausel im Auftragsverarbeitungsvertrag. Anbieterfrage: Können wir Datensätze eigenständig korrigieren, und wird jede Änderung nachvollziehbar protokolliert?			
	Offen	In Arbeit	Erfüllt	Nicht anwendbar
Nachweis / Begründung				

8.13

<

A.8 Offenheit, Transparenz und Benachrichtigung 2

A.8.1	Der Einsatz von Unterauftragnehmern, die personenbezogene Daten verarbeiten, ist vor Vertragsschluss offengelegt. Änderungen an der Liste werden dem Kunden rechtzeitig mitgeteilt, sodass er widersprechen oder kündigen kann.				Dokument
	Woran man es festmacht: Beleg ist eine aktuelle, öffentlich oder vertraglich verfügbare Subprozessorenliste mit Name, Land und Verarbeitungszweck sowie eine Benachrichtigungsregel nach Art. 28 Abs. 2 DSGVO. Anbieterfrage: Wo finden wir Ihre Subprozessorenliste, mit welcher Vorlaufzeit informieren Sie über Änderungen, und wie können wir widersprechen?				
	Offen	In Arbeit	Erfüllt	Nicht anwendbar	
Nachweis / Begründung					

A.8 (Grund)	Der Anbieter stellt vor Vertragsschluss verständliche Informationen darüber bereit, wie personenbezogene Daten verarbeitet werden, welche Schutzmaßnahmen bestehen und in welchen Rechtsordnungen die Verarbeitung stattfindet.			
	Woran man es festmacht: Beleg sind Datenschutzerklärung, Sicherheits-Whitepaper, Trust-Center-Seite und der Auftragsverarbeitungsvertrag samt technisch-organisatorischen Maßnahmen als Anlage. Anbieterfrage: Bitte um das aktuelle Maßnahmenverzeichnis (TOM) als Vertragsanlage, nicht nur um Marketingmaterial.			
	Offen	In Arbeit	Erfüllt	Nicht anwendbar
Nachweis / Begründung				

A.9 Beteiligung des Betroffenen und Zugang

2

A.9 (Grund) Der Dienst bietet dem Cloud-Kunden die technischen Mittel, um Auskunfts-, Berichtigungs- und Löschbegehren betroffener Personen selbst zu bedienen, etwa über Export-, Such- und Löschfunktionen.

Woran man es festmacht: Beleg ist die Produktdokumentation der Export- und Löschfunktion, ergänzt um einen internen Testlauf: Ein Auskunftersuchen einmal durchspielen und die Dauer notieren. Anbieterfrage: Können wir alle Daten einer einzelnen Person ohne Ihren Support finden, exportieren und löschen?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

5.34 Kann der Kunde ein Betroffenenbegehren nicht selbst umsetzen, unterstützt der Anbieter innerhalb einer vereinbarten Frist. Direkte Anfragen betroffener Personen leitet der Anbieter an den Kunden weiter, statt sie eigenständig zu beantworten.

Woran man es festmacht: Beleg ist die entsprechende Klausel im Auftragsverarbeitungsvertrag mit konkreter Reaktionsfrist sowie ein Support-Ticket-Verlauf als Praxisbeispiel. Anbieterfrage: Welche Frist sagen Sie für die Unterstützung bei Betroffenenrechten zu, und was kostet sie?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.10 Rechenschaftspflicht

4

A.10.1 Verletzungen des Schutzes personenbezogener Daten werden dem Cloud-Kunden unverzüglich gemeldet, mit Angaben zu Umfang, betroffenen Daten, Ursache und ergriffenen Maßnahmen. Ein Meldeprozess mit Zuständigkeiten und Fristen ist festgelegt.

[Dokument](#)

Woran man es festmacht: Beleg sind der Incident-Response-Plan mit Meldekette, die vertragliche Meldefrist (praxistauglich sind 24 bis 48 Stunden, damit der Kunde die 72-Stunden-Frist nach Art. 33 DSGVO halten kann) und Protokolle vergangener Vorfälle oder einer Übung. Anbieterfrage: Innerhalb welcher Frist melden Sie einen Vorfall, an welchen Kanal, und welche Informationen liefern Sie mit?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.10.2 Sicherheitsrichtlinien, Verfahrensanweisungen und zugehörige Aufzeichnungen werden für einen festgelegten Zeitraum aufbewahrt, damit die Verarbeitung im Nachhinein rekonstruierbar bleibt.

[Dokument](#)

Woran man es festmacht: Beleg ist eine Aufbewahrungsregel mit Versionshistorie der Richtlinien, etwa über ein Dokumentenverzeichnis oder eine Versionsverwaltung mit Freigabedatum. Anbieterfrage: Wie lange bewahren Sie Richtlinienstände und zugehörige Nachweise auf, und erhalten wir im Auditfall Einsicht?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.10.3 Für Rückgabe, Übertragung und Vernichtung personenbezogener Daten am Vertragsende besteht eine festgelegte Regelung, die Formate, Fristen und den Umgang mit Kopien benennt.

[Dokument](#)

Woran man es festmacht: Beleg ist die Exit-Klausel im Auftragsverarbeitungsvertrag plus eine Löschbestätigung nach Vertragsende. Anbieterfrage: In welchem Format und innerhalb welcher Frist erhalten wir unsere Daten zurück, wann werden alle Kopien vernichtet, und bekommen wir das schriftlich bestätigt?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

5.35 Die Wirksamkeit der Schutzmaßnahmen wird regelmäßig unabhängig überprüft, etwa durch interne Audits, Penetrationstests oder Prüfberichte Dritter. Ergebnisse stehen dem Cloud-Kunden in geeigneter Form zur Verfügung.

Woran man es festmacht: Beleg sind ISO/IEC 27001-Zertifikat mit Erklärung zur Anwendbarkeit, in der die ISO/IEC 27018-Maßnahmen enthalten sind, oder ein SOC-2-Bericht sowie aktuelle Pentest-Zusammenfassungen. Anbieterfrage: Bitte um Zertifikat, Geltungsbereich und die Bestätigung, dass ISO/IEC 27018 in der Erklärung zur Anwendbarkeit berücksichtigt ist. Prüfen Sie dabei, ob der Geltungsbereich den genutzten Dienst wirklich abdeckt.

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11 Informationssicherheit

13

A.11.1 Alle Personen mit Zugriff auf personenbezogene Daten sind zur Vertraulichkeit verpflichtet, unabhängig davon, ob sie angestellt oder extern tätig sind.[Dokument](#)

Woran man es festmacht: Beleg sind unterschriebene Vertraulichkeitsvereinbarungen oder Verpflichtungserklärungen, die auch nach Ende der Tätigkeit fortgelten. Anbieterfrage: Sind alle Mitarbeitenden und Dienstleister mit Datenzugriff schriftlich zur Vertraulichkeit verpflichtet?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.2 Ausdrucke und sonstige Papierkopien mit personenbezogenen Daten entstehen nur, wo sie zwingend nötig sind. Der zulässige Umfang ist geregelt.

Woran man es festmacht: Beleg ist eine Regelung zum Umgang mit Ausdrucken, in Rechenzentren typischerweise ein generelles Druckverbot in Bereichen mit Kundendaten. Anbieterfrage: Werden Kundendaten in Ihrem Betrieb überhaupt gedruckt, und wenn ja, unter welchen Auflagen?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.3 Wiederherstellungen aus Sicherungen werden vorab genehmigt und protokolliert, einschließlich der Person, die die Wiederherstellung ausgelöst hat, und der betroffenen Daten.[Dokument](#)

Woran man es festmacht: Beleg ist das Restore-Protokoll mit Zeitstempel, Auslöser und Umfang, meist automatisch im Backup-Werkzeug. Anbieterfrage: Protokollieren Sie jede Wiederherstellung, und können wir diese Protokolle im Auditfall einsehen?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.4 Datenträger mit personenbezogenen Daten, die das Betriebsgelände verlassen, sind vor unbefugtem Zugriff und Verlust geschützt, in der Regel durch Verschlüsselung und ein Transportprotokoll.

Woran man es festmacht: Beleg sind Verschlüsselungsnachweis (Datenträger-Vollverschlüsselung), Transport- und Übergabeprotokolle sowie ein Datenträgerverzeichnis. Anbieterfrage: Verlassen Datenträger mit Kundendaten Ihre Standorte, etwa für Backups, und wie sind sie dabei geschützt?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.5 Der Einsatz unverschlüsselter portabler Datenträger und Geräte für personenbezogene Daten ist untersagt oder auf begründete Ausnahmen mit dokumentierter Genehmigung beschränkt.

Woran man es festmacht: Beleg ist eine Richtlinie zu Wechselmedien plus technische Durchsetzung, etwa erzwungene Geräteverschlüsselung oder gesperrte USB-Ports über die Geräteverwaltung. Anbieterfrage: Können Mitarbeitende Kundendaten auf unverschlüsselte Geräte kopieren, und was verhindert das technisch?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.6 Personenbezogene Daten, die über öffentliche Netze übertragen werden, sind verschlüsselt. Die eingesetzten Verfahren entsprechen dem aktuellen Stand der Technik.

Woran man es festmacht: Beleg sind die TLS-Konfiguration (aktuelle Protokollversion, keine veralteten Cipher) und ein externer Konfigurationstest als Bericht. Praktikabel für kleine Betriebe: einmal jährlich einen kostenlosen TLS-Scan laufen lassen und das Ergebnis ablegen. Anbieterfrage: Welche Transportverschlüsselung erzwingen Sie, und ist Verschlüsselung im Ruhezustand aktiv?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.7 Papierunterlagen mit personenbezogenen Daten werden so vernichtet, dass eine Rekonstruktion ausgeschlossen ist.

Woran man es festmacht: Beleg sind Aktenvernichter mit passender Sicherheitsstufe oder Vernichtungsnachweise eines Dienstleisters nach DIN 66399. Anbieterfrage: Wie vernichten Sie Papierunterlagen mit Kundenbezug, und liegen Vernichtungsnachweise vor?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.8 Benutzerkennungen sind eindeutig einer Person zugeordnet und werden nicht mehrfach vergeben oder geteilt. Gemeinsam genutzte Konten bestehen nur in begründeten Ausnahmen mit zusätzlicher Nachvollziehbarkeit.

Woran man es festmacht: Beleg ist eine Benutzerliste aus dem Identitätssystem ohne Sammelkonten sowie die Regel, dass administrative Tätigkeiten mit persönlichem Konto erfolgen. Anbieterfrage: Arbeitet Ihr Betriebspersonal mit personenbezogenen Konten, und ist Mehrfaktor-Authentisierung Pflicht?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.9 Der Anbieter kann jederzeit benennen, welche Personen oder Rollen auf personenbezogene Daten zugreifen dürfen, und hält diese Übersicht aktuell.

Dokument

Woran man es festmacht: Beleg ist eine Berechtigungsübersicht mit Rollen, ergänzt um eine wiederkehrende Berechtigungsprüfung mit Datum und Ergebnis. Für kleine Betriebe genügt ein halbjährlicher Export der Benutzerliste mit Abzeichnung. Anbieterfrage: Wie viele Ihrer Mitarbeitenden können auf unsere Daten zugreifen, und wie oft prüfen Sie das nach?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.10 Benutzerkonten werden über den gesamten Lebenszyklus verwaltet: Anlage, Änderung und zeitnahe Deaktivierung beim Ausscheiden oder Rollenwechsel.

Woran man es festmacht: Beleg sind ein Onboarding- und Offboarding-Ablauf mit Checkliste sowie Protokolle deaktivierter Konten mit Zeitstempel. Anbieterfrage: Innerhalb welcher Frist entziehen Sie ausgeschiedenen Mitarbeitenden den Zugriff, und wie belegen Sie das?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.11 Die Sicherheits- und Datenschutzpflichten des Anbieters sind vertraglich fixiert, einschließlich der technisch-organisatorischen Maßnahmen, der Weisungsbindung und der Prüfrechte des Kunden.

Dokument

Woran man es festmacht: Beleg ist der unterzeichnete Auftragsverarbeitungsvertrag nach Art. 28 DSGVO mit Maßnahmenanlage und Audit- oder Auskunftsrecht. Anbieterfrage: Bitte um den unterzeichneten Auftragsverarbeitungsvertrag samt Anlagen, nicht nur um einen Verweis auf allgemeine Nutzungsbedingungen.

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.12 Unterauftragnehmer, die personenbezogene Daten verarbeiten, unterliegen mindestens den gleichen Pflichten wie der Anbieter selbst. Ihre Auswahl und laufende Überwachung ist geregelt.

Woran man es festmacht: Beleg sind die Weiterreichung der Pflichten in den Verträgen mit Unterauftragnehmern (Art. 28 Abs. 4 DSGVO) und eine Lieferantenbewertung mit Datum. Anbieterfrage: Wie prüfen Sie Ihre Unterauftragnehmer, und welche Nachweise fordern Sie von ihnen ein?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.11.13 Vor der Wiederverwendung von Speicherbereichen ist sichergestellt, dass keine Daten früherer Nutzer zugänglich bleiben, weder auf physischen Datenträgern noch in virtualisierten Umgebungen.

Woran man es festmacht: Beleg sind die Bereinigungs- oder Überschreibprozedur bei der Freigabe von Speicher, Nachweise zur Datenträgervernichtung sowie die Mandantentrennung im Architekturdokument. Anbieterfrage: Wie stellen Sie sicher, dass wiederverwendeter Speicher keine Restdaten anderer Kunden enthält?

Offen In Arbeit Erfüllt Nicht anwendbar

Nachweis / Begründung

A.12 Datenschutz-Compliance		3
A.12.1	Die Länder, in denen personenbezogene Daten gespeichert und verarbeitet werden, sind benannt und dem Cloud-Kunden bekannt. Änderungen der Speicherorte werden mitgeteilt.	Dokument
Woran man es festmacht: Beleg ist eine Standort- und Regionenübersicht des Anbieters, im Vertrag oder in der Dokumentation, sowie die Regionseinstellung des genutzten Dienstes als Screenshot. Anbieterfrage: In welchen Ländern liegen unsere Daten im Ruhezustand, in welchen wird zugegriffen, etwa im Support, und können wir die Region festlegen?		
Offen In Arbeit Erfüllt Nicht anwendbar		
Nachweis / Begründung		
A.12.2	Übermittlungen personenbezogener Daten in Drittländer sind bekannt, begründet und durch geeignete Garantien abgesichert.	Dokument
Woran man es festmacht: Beleg sind Standardvertragsklauseln oder eine Angemessenheitsentscheidung, ergänzt um ein Transfer Impact Assessment, das für kleine Betriebe kurz ausfallen darf: betroffene Datenarten, Zielland, Risiko, ergriffene Zusatzmaßnahmen. Anbieterfrage: Auf welcher Rechtsgrundlage übermitteln Sie Daten in Drittländer, und welche Zusatzmaßnahmen setzen Sie ein?		
Offen In Arbeit Erfüllt Nicht anwendbar		
Nachweis / Begründung		
5.31	Die rechtlichen und vertraglichen Anforderungen an die Verarbeitung personenbezogener Daten sind ermittelt und werden bei Änderungen der Rechtslage nachgeführt. Kollidierende Rechtsordnungen sind bewertet.	
Woran man es festmacht: Beleg ist eine Übersicht der anwendbaren Vorgaben (DSGVO, nationale Regelungen, branchenspezifische Pflichten) mit Zuständigkeit und Prüfdatum, im kleinen Betrieb eine einseitige Liste, die jährlich überprüft wird. Anbieterfrage: Unterliegen Sie oder Ihre Unterauftragnehmer Rechtsordnungen, die einen Behördenzugriff auf unsere Daten ermöglichen, und wie gehen Sie damit um?		
Offen In Arbeit Erfüllt Nicht anwendbar		
Nachweis / Begründung		