// KI-Hub VON STRUKTURAFLOW

COMPLIANCE

Löschpflicht und Backup-Retention: Österreichische Rechtslage für Firmen

§ 4 Abs. 2 DSG erlaubt verzögerte Löschung in Backups – mit Einschränkungspflicht. Was das konkret für IT-Architektur und Restore-Prozesse bedeutet.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
8. August 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/loeschpflicht-und-backup-retention-oesterreichische-rechtslage-fuer-firmen/

Ein Kunde verlangt Löschung. Im CRM ist der Datensatz in Sekunden weg. In der Bandsicherung, im inkrementellen Backup, im Offsite-Snapshot und im WORM-Speicher ist er es nicht — und dort soll er technisch auch gar nicht punktuell entfernbar sein. Genau diese Unveränderbarkeit ist es, die das Backup gegen Ransomware und Manipulation absichert.

Dieselbe Verordnung, die die Löschung verlangt, verlangt an anderer Stelle die Fähigkeit, Daten nach einem Zwischenfall rasch wiederherzustellen. Art. 17 gegen Art. 32 Abs. 1 lit. c. In der deutschen Fachliteratur wird dieser Konflikt seit acht Jahren als weitgehend unlösbar diskutiert.

Mir ist es ein Anliegen, an dieser Stelle die österreichische Rechtslage sauber zu klären. Denn sie ist eine andere — und deutlich weiter aufgelöst. Österreich hat seit 2018 eine Norm, die genau diese Situation regelt: **§ 4 Abs. 2 DSG**. Sie existiert im deutschen Recht nicht. Ein deutscher Ratgeber kann sie strukturell nicht enthalten, egal wie gut er sonst ist — ähnlich wie bei anderen nationalen Sonderregelungen zum Newsletter-Recht. Und die meisten österreichischen Betriebe kennen sie nicht, weil sie ihre Informationen aus genau diesen deutschen Quellen beziehen.

Dieser Artikel richtet sich an Geschäftsführung, IT-Verantwortliche und an IT-Dienstleister, die für ihre Kunden Backup-Architektur bauen. Er ersetzt keine Rechtsberatung — er soll verhindern, dass Sie ein Löschkonzept auf einer Rechtslage aufbauen, die für Ihr Unternehmen gar nicht gilt.

Zuerst: Was „Löschen„ überhaupt heißt

Bevor es um Backups geht, ein Punkt, der überraschend viel entscheidet. **Die DSGVO definiert „Löschen" nicht.** Sie zählt es in Art. 4 Z 2 neben „Vernichtung„ als eigenständige Verarbeitungsart auf — beides ist also ausdrücklich nicht dasselbe.

Daraus folgt: Der Verantwortliche hat ein **Auswahlermessen hinsichtlich des Mittels**. Entscheidend ist das Ergebnis, nicht das physische Überschreiben jedes einzelnen Sektors.

Das ist keine kreative Auslegung, sondern eine ausdrückliche Feststellung der österreichischen Datenschutzbehörde. In einem Bescheid vom 5. Dezember 2018 (GZ DSB-D123.270/0009-DSB/2018) hatte eine Versicherung nach einem Löschbegehren Name und Adresse durch Musterdaten ersetzt und die endgültige Vernichtung erst für später angekündigt. Die DSB gab der Versicherung recht: **Anonymisierung kann ein taugliches Mittel der Löschung sein** — unter der Bedingung, dass weder der Verantwortliche noch ein Dritter den Personenbezug ohne unverhältnismäßigen Aufwand wiederherstellen kann.

Für IT-Projekte hat das handfeste Folgen. Damit ist die Tür offen für:

- **kryptografische Löschung (Crypto-Shredding)** — der Schlüssel wird vernichtet, die Daten bleiben physisch liegen, sind aber ohne Schlüssel wertlos
- **Überschreiben mit Zufallswerten** — vom Europäischen Datenschutzausschuss ausdrücklich als Best Practice genannt

Beides ist rechtlich Löschung, nicht Umgehung. Aber die Latte liegt hoch: **bloße Pseudonymisierung oder Teilmaskierung genügt nicht.** Wer eine Kundennummer stehen lässt, über die sich der Datensatz jederzeit rekonstruieren lässt, hat nichts gelöscht.

Eine Ergänzung aus der jüngeren Judikatur: Der EuGH hat im September 2025 (C-413/23 P, EDSB gegen SRB) erstmals ausdrücklich betont, dass der Personenbezug **relativ** ist. Daten, die für den Verantwortlichen eindeutig personenbezogen sind, können für einen Empfänger ohne Zuordnungsschlüssel anonym sein. Das entlastet die Lieferkette — ein verschlüsseltes Offsite-Backup kann für den Hoster anonym sein — aber es entlastet **nicht Sie selbst**. Wer den Schlüssel hält, für den bleiben die Daten personenbezogen. Wer Ihnen das anders verkauft, verkauft falsch.

Die Fristenverwechslung, die fast alle machen

Zwei Fristen, die ständig durcheinandergehen:

- **Art. 17 Abs. 1 DSGVO:** Löschung „unverzüglich"
- **Art. 12 Abs. 3 DSGVO:** Antwort an die betroffene Person **binnen eines Monats**, verlängerbar um zwei weitere Monate bei komplexen Anträgen — mit Information innerhalb des ersten Monats

Die Monatsfrist ist eine **Kommunikationsfrist, keine Vollzugsfrist.** Sie müssen binnen eines Monats antworten und darlegen, was Sie getan haben — auch wenn die endgültige Vernichtung im Backup später erfolgt.

Genau das ist der Ansatzpunkt für die österreichische Lösung.

Der österreichische Sonderweg: § 4 Abs. 2 DSG

> **§ 4 Abs. 2 DSG:** „Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.„

Lesen Sie den Satz noch einmal mit dem Backup im Kopf. Er beschreibt exakt die Situation: Löschung technisch nur zyklisch möglich.

Die Rechtsfolge ist **keine Ausnahme von der Löschpflicht**, sondern eine **Verschiebung mit Sicherungsauflage**. Bis zur endgültigen Löschung sind die Daten mit der Wirkung des Art. 18 Abs. 2 DSGVO einzuschränken — sie dürfen also nur noch gespeichert und im Übrigen nur mit Einwilligung, zur Rechtsverfolgung, zum Schutz der Rechte Dritter oder aus wichtigem öffentlichen Interesse verarbeitet werden.

Für ein Backup ist das nahezu deckungsgleich mit dem, was ein Backup ohnehin ist: ein Datenbestand, der liegt und nicht angefasst wird.

Drei Punkte, die dabei regelmäßig übersehen werden

1. „ist einzuschränken" ist eine Pflicht, kein Wahlrecht. Wer sich auf § 4 Abs. 2 DSG beruft, muss die Einschränkung auch technisch und organisatorisch umsetzen — und nachweisen können. Ein Backup, aus dem im Alltag Einzelabfragen gefahren werden („schau mal, was da 2023 drinstand„), ist nicht eingeschränkt. Dann trägt die Norm nicht.

2. Die Norm ändert nichts an Art. 12 Abs. 3. Die betroffene Person muss binnen Monatsfrist erfahren, dass gelöscht wurde, dass Kopien in Sicherungen noch bestehen, dass diese eingeschränkt sind — und **wann** sie endgültig verschwinden. Schweigen ist keine Option.

3. „zu bestimmten Zeitpunkten" heißt: Der Zeitpunkt muss bestimmt sein. Ein dokumentierter Sicherungszyklus mit definierter Retention erfüllt das. „Wenn der Speicher voll ist„ oder „wenn es irgendwann überschrieben wird" erfüllt es nicht. Das ist der Punkt, an dem die meisten Konzepte in der Praxis scheitern — nicht am Recht, sondern an der fehlenden Dokumentation dessen, was der Backup-Server ohnehin tut.

Das Restrisiko, das ich nicht verschweigen will

§ 4 Abs. 2 DSG ist eine **nationale Beschränkung eines Betroffenenrechts**. Die einzige unionsrechtliche Öffnungsklausel dafür ist Art. 23 DSGVO, der an solche Maßnahmen inhaltliche Mindestanforderungen stellt. Ob § 4 Abs. 2 DSG diese erfüllt, ist bislang **weder vom EuGH noch vom VwGH geklärt**. Die Kommentarliteratur hält die Frage offen.

Zur Einordnung des Risikos hilft ein Präzedenzfall: Bei den österreichischen Sonderregeln zur Bildverarbeitung (§§ 12 und 13 DSG) hat das Bundesverwaltungsgericht im November 2019 in zwei Erkenntnissen entschieden, dass die nationalen Bestimmungen gegen die DSGVO verstoßen und unangewendet zu lassen sind. Dass es § 4 Abs. 2 DSG einmal ebenso ergehen könnte, ist nicht auszuschließen.

Die Konsequenz für die Praxis ist nicht, die Norm zu ignorieren — sondern sie nicht allein tragen zu lassen.

Nutzen Sie § 4 Abs. 2 DSG als primäre Begründung. Bauen Sie das Löschkonzept aber so, dass es auch ohne die Norm trägt:

- dokumentierte Interessenabwägung
- kurze Retention-Zeiten
- Nachlöschroutine bei Restore

Wer sich ausschließlich auf § 4 Abs. 2 DSG stützt, hat einen Single Point of Failure im Compliance-Konzept. Das ist genau die Art von Abhängigkeit, die man in der IT-Architektur vermeidet — und im Rechtskonzept sollte man es genauso halten.

Der Fall, an dem sich alles entscheidet: der Restore

Hier sind sich alle einig — der Europäische Datenschutzausschuss, die österreichische Literatur und die ISPA (Internet Service Providers Austria): **Beim tatsächlichen Einspielen eines Backups sind die zwischenzeitlich gelöschten Datensätze erneut zu löschen.**

Das klingt banal und ist in der Praxis der am häufigsten fehlende Baustein. Denn dafür brauchen Sie eine fortgeschriebene **Liste der Löschvorgänge, die den Restore überlebt** — also außerhalb des Systems liegt, das wiederhergestellt wird.

Diese Liste ist selbst eine Verarbeitung personenbezogener Daten und muss minimal gehalten werden. In der Regel genügen ein Hashwert und ein Datum. Kein Name, keine Adresse, keine Kundennummer im Klartext.

Die Kontrollfrage für Ihr nächstes IT-Meeting: **Wenn Sie das Backup morgen einspielen müssten — welche gelöschten Datensätze wären wieder da, und wer würde es merken?**

Wenn die Antwort „niemand„ lautet, haben Sie kein Rechtsproblem, sondern ein Prozessproblem. Und das ist die bessere Nachricht, weil es lösbar ist.

Der wichtigste Hebel ist Architektur, nicht Jurisprudenz

Backup und Archiv sind zwei verschiedene Dinge mit zwei verschiedenen Rechtsgrundlagen. Wer sie im selben Speicher liegen hat, hat kein Rechtsproblem, sondern ein Architekturproblem.

	BACKUP	ARCHIV
Zweck	Wiederherstellbarkeit nach einem Zwischenfall	Erfüllung gesetzlicher Aufbewahrungspflichten
Rechtsgrundlage	Art. 32 Abs. 1 lit. c DSGVO	z. B. § 132 BAO, § 212 UGB
Retention	kurz — die Rechtfertigung wird mit jedem Monat dünner	gesetzlich vorgegeben, meist 7 Jahre
Zugriff	technisch beschränkt	beschränkt, aber gezielt auffindbar
Umfang	technisch bedingt vollständig	**nur die tatsächlich aufbewahrungspflichtigen Daten**

Die letzte Zeile ist die teuerste in der Praxis. Eine Rechnung sieben Jahre aufzubewahren rechtfertigt **nicht**, den vollständigen CRM-Datensatz samt Kontakthistorie, Newsletter-Öffnungsraten und Support-Tickets sieben Jahre lang produktiv zu halten. Die Frist rechtfertigt nur den notwendigen Datenumfang.

Die richtige Antwort ist Trennung: gesetzlich Aufzubewahrendes in ein zugriffsbeschränktes Archiv, der Rest wird gelöscht.

Ebenso wenig trägt der umgekehrte Fehler — die längste anwendbare Frist einfach auf alles anzuwenden. Das ist ein eigenständiger Verstoß gegen die Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO, und er wird von den Aufsichtsbehörden auch als solcher beanstandet.

Was das für die Backup-Architektur konkret heißt

- **Retention-Zeiten definieren und dokumentieren**, nicht nur konfigurieren. Was der Server tut, muss auch auf Papier stehen.
- **Backup und Archiv technisch trennen.** Der wichtigste architektonische Hebel überhaupt, weil er zwei rechtlich völlig verschiedene Bestände auseinanderzieht.
- **Zugriffsbeschränkung auf Sicherungsbestände technisch durchsetzen** — sonst greift die Einschränkung nach § 4 Abs. 2 DSG nicht.
- **Nachlöschroutine für den Restore-Fall** samt Löschliste, die den Restore überlebt.
- **Verschlüsselung mit getrennter Schlüsselverwaltung**, damit Crypto-Shredding als Löschoption überhaupt zur Verfügung steht.

Und Logfiles? Die sind ein anderes Thema

Logfiles werden regelmäßig mit Backups in einen Topf geworfen. Rechtlich ist das falsch, und der Unterschied ist die Zweckbindung.

Ein Backup ist eine Kopie desselben Datenbestands zum selben Zweck. Ein Logfile dient einem **eigenständigen Zweck** — IT-Sicherheit, Betriebsstabilität, Nachweis — auf einer eigenen Rechtsgrundlage (Art. 6 Abs. 1 lit. f, gestützt auf Erwägungsgrund 49).

Die praktische Folge: Wer im CRM gelöscht wird, hat **nicht automatisch** einen Anspruch darauf, aus dem Webserver-Log zu verschwinden. Der Anspruch scheitert dort regelmäßig daran, dass die Daten für den Sicherheitszweck noch erforderlich sind.

Aber: Das trägt nur, solange die Speicherdauer kurz und begründet ist. Ein Log mit unbegrenzter Retention verliert diese Rechtfertigung. Dazu gibt es einen eigenen Artikel, weil das Thema eigene Fallstricke hat.

Was ab Oktober 2026 dazukommt

Ein Terminhinweis, der viele Betriebe unvorbereitet trifft: Mit dem **NISG 2026** treten am 1. Oktober 2026 verbindliche Pflichten zu Backup-Management und Protokollierung für rund 4.000 bis 5.000 österreichische Einrichtungen in Kraft — plus deren Zulieferer über die Lieferkettenpflicht.

Wer NISG-pflichtig wird, muss Backups und Protokollierung nachweisbar betreiben. Und steht damit erstmals genau in dem Spannungsverhältnis, das dieser Artikel beschreibt. Die gute Nachricht: Wer sein Löschkonzept jetzt sauber aufsetzt, erschlägt beide Anforderungen mit derselben Dokumentation.

Die Kurzfassung für Ihr nächstes IT-Meeting

1. **Löschen heißt nicht vernichten.** Anonymisierung und Crypto-Shredding sind zulässige Mittel — Pseudonymisierung nicht.
2. **§ 4 Abs. 2 DSG erlaubt die Verschiebung der Löschung im Backup**, verlangt dafür aber Einschränkung, einen bestimmten Zeitpunkt und Kommunikation binnen Monatsfrist.
3. **Die Norm ist unionsrechtlich nicht abgesichert.** Bauen Sie das Konzept so, dass es auch ohne sie trägt.
4. **Der Restore ist der kritische Moment.** Ohne Löschliste, die den Restore überlebt, holen Sie sich alles zurück.
5. **Backup ist kein Archiv.** Wer das trennt, löst das Problem in der Architektur statt in der Datenschutzerklärung.

Wann ein Gespräch sinnvoller ist als weiteres Lesen

Was Sie selbst gut erledigen können: Retention-Zeiten dokumentieren, Backup und Archiv auseinanderziehen, eine Antwortvorlage für den Backup-Fall schreiben.

Sobald es an die Frage geht, ob Ihre konkrete Backup-Architektur die Einschränkung nach § 4 Abs. 2 DSG technisch überhaupt abbildet — oder wie eine Nachlöschroutine aussieht, die im Ernstfall auch funktioniert — wird es eine Architekturfrage. Und die lässt sich nicht aus einem Ratgeber beantworten, sondern nur an Ihrem tatsächlichen Setup.

In einem unverbindlichen 30-Minuten-Gespräch schauen wir uns an, wo Ihr Betrieb steht: Wo liegen personenbezogene Daten überhaupt, was passiert im Restore-Fall, und welche zwei bis drei Schritte bringen am meisten. Kein Verkaufsgespräch — eine Einschätzung auf Basis Ihrer Situation.

FAQ

Muss ich Daten aus dem Backup löschen, wenn jemand einen Löschantrag stellt? Ja — die Löschpflicht erfasst auch Sicherungskopien. In Österreich erlaubt § 4 Abs. 2 DSG allerdings, den Vollzug bis zum nächsten Löschzeitpunkt des dokumentierten Sicherungszyklus zu verschieben, sofern die Verarbeitung bis dahin eingeschränkt wird. Ein pauschaler Ausschluss von Backups aus dem Löschanspruch ist nicht zulässig und wird von den Aufsichtsbehörden ausdrücklich beanstandet.

Wie lange darf ich Backups aufbewahren? Das Unionsrecht nennt keine Frist. Maßgeblich ist, dass die Retention definiert, dokumentiert und begründet ist — und dass sie nicht länger läuft als für den Wiederherstellungszweck nötig. Je länger die Frist, desto dünner die Rechtfertigung.

Reicht es, den Kundenaccount zu deaktivieren? Nein. Die Deaktivierung eines Benutzerkontos ist keine Löschung. Das ist einer der Punkte, die der Europäische Datenschutzausschuss in seiner Prüfaktion 2025 ausdrücklich beanstandet hat.

Gilt § 4 Abs. 2 DSG auch für mein deutsches Tochterunternehmen? Nein. Die Norm ist österreichisches Recht und gilt nur für Verarbeitungen, die dem österreichischen DSG unterliegen. Für einen deutschen Standort brauchen Sie eine andere Begründung — üblicherweise über eine dokumentierte Interessenabwägung.

Was muss ich der betroffenen Person konkret schreiben? Vier Punkte: was gelöscht wurde, dass Kopien in Sicherungen bestehen, dass diese in ihrer Verarbeitung eingeschränkt sind, und bis wann sie endgültig verschwinden. Und das binnen eines Monats ab Eingang des Antrags.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.it.com