

## DSGVO-Tipps: Was lernen wir aus den bisherigen Verfahren?

Teil 2 unserer Serie mit Praxis-Tipps für die tägliche Umsetzung der DSGVO.

---

Im vorigen BAV-Newsletter haben wir uns angesehen, mit welchen Themen sich die bisherigen Verfahren vor der Datenschutzbehörde beschäftigten (Auskunfts-, Löschbegehren, Video-Überwachung, Aufbewahrung von Daten, Verfahrensverzeichnis, Datenschutz-Folgenabschätzung) und welche **Urteile dazu gefällt** wurden.

[Zum Nachlesen hier klicken...](#)

### TIPPS: Was können wir aus den obigen Urteilen bzw. beschriebenen Problemen lernen?

- **Keinesfalls** sollte man Auskunfts- bzw. Löschbegehren **ignorieren**, weil andernfalls eine Beschwerde bei der Datenschutzbehörde droht und diese dann das Nichtreagieren zum Anlass nimmt, eine Prüfung bei Ihnen durchzuführen. Wie vorzugehen ist, sollten Sie in einem **Auskunfts- und Löschkonzept definieren** und im Unternehmen entsprechend kommunizieren und schulen. Und regelmäßig „durchspielen“, also die Probe aufs Exempel machen. Lassen Sie doch einfach nach Ihren eigenen Daten suchen.
- **Tipps** zum praktischen Umgang mit **„Auskunfts- und Löschwünschen“**: Wir haben schon im Vorjahr in der Vorbereitung auf die DSGVO auf die Wichtigkeit des **„Auskunfts- & Löschkonzeptes“ verwiesen**. Immer mehr Menschen werden ihr **Recht auf Auskunft, Korrektur und Löschung** der gespeicherten Daten in Anspruch nehmen.

Ganz vereinfacht geht es bei diesem „Auskunfts- und Löschkonzept“ darum, zu definieren, **wer was und vor allem wie tut, wenn jemand anruft oder anderswie sonst Auskunft verlangt**, welche Daten von ihm/ihr gespeichert sind, diese korrigieren oder sogar löschen lassen möchte.

**Weder dürfen solche Anfragen ignoriert werden, noch dürfen Daten in vorseilendem Gehorsam sofort gelöscht werden** (womöglich muss man sie aufgrund rechtlicher Pflichten aufbewahren, trotzdem die Löschung gewünscht wird). Auch müssen Sie sich vergewissern, dass der Anfrager wirklich der ist, der er behauptet zu sein, also **gilt es, die Identität zu klären. Hier Fehler zu machen, kann Sie teuer zu stehen kommen.**

- **Tipps zum Identitäts-Nachweis bei Auskunfts- und Löschbegehren**: Wenn es nur um eine Abmeldung von einem Newsletter geht, dann können Sie dem E-Mail-Sender dies wohl problemlos per Mail beantworten. „Habe Sie aus dem Verteiler gelöscht.“

Geht es aber um eine **komplette Daten-Auskunft oder Löschbegehren**, sollten Sie zur Sicherheit einen **Ausweis anfordern**, wenn der Wunsch via E-Mail herein kam, denn E-Mail-Adressen kann man ganz leicht fälschen. Auch ein Anruf kann umgeleitet worden sein. Und Daten an Nichtbefugte weiterzugeben wäre ein Datenleck. Wie man da vorgehen sollte, darüber mehr im nächsten Newsletter.

Enthält Ihre **Beauskunftung heikle oder sogar sensible Daten** der betreffenden Person (also etwa

Finanz-, Vermögensinfos oder sogar Gesundheitsdaten), dann sollten Sie auf jeden Fall vorher die Identität durch einen persönlichen Besuch, zumindest via Ausweis geprüft haben. Und die Auskunft dann entweder per eingeschriebener Post oder einer verschlüsselten E-Mail oder mit Passwort versperrem Word-Dokument in einer E-Mail versenden (und das Passwort über einen anderen Weg – etwa SMS – nachsenden).

- **Zum Verfahrensverzeichnis:** Um wie oben beschrieben die Daten für eine Beauskunftung oder Löschung finden zu können, sollten Sie ein Verfahrensverzeichnis haben, **in dem alle Verfahren aufgelistet sind**, wo von wem welche Daten zu welchem Zweck gespeichert sind, welchen Grund für die Speicherung es gibt, wann gelöscht wird, an wen Daten weitergegeben werden usw. Das ist eines der **zentralen Dokumente der DSGVO**. Dieses wird die Behörde sicherlich kontrollieren. Und dann auch bei Ihren Lieferanten weiter prüfen (ob auch dort die DSGVO eingehalten wird).

Bedenken Sie, dass Sie womöglich **so ein Verzeichnis als Verantwortlicher, aber auch als Auftragsverarbeiter führen müssen**. Als Agent/Makler sind Sie selbstständig, daher Verantwortlicher nach DSGVO. Aber womöglich kümmern Sie sich im Auftrag der Versicherung auch um Schadensabwicklung etc. In diesem Falle wären Sie dann Auftragsverarbeiter und müssten hierfür ein eigenes Verfahrensverzeichnis führen.

- **Tipp zur Rechtsgrundlage für die Datenspeicherung:** Hier sollten Sie weniger mit Einwilligungen der Kunden/Partner arbeiten, weil die können prompt wieder zurückgezogen werden. Und dann müssten Sie prompt die Daten löschen. Besser wäre es, wenn Sie **„gesetzliche Vorgaben“** oder **„berechtigtes Interesse des Unternehmens“** im Verfahrensverzeichnis anführen könnten.

**Tipp zur Einwilligung:** Sie brauchen wegen der DSGVO keine neue, ausdrückliche Zustimmung Ihrer Kunden, Partner etc. einzuholen. Wenn Sie **deren Daten vor Inkrafttreten der DSGVO zu Recht hatten** und niemand sich seither „abgemeldet“ hat, dann können Sie von einer konkludenten Zustimmung ausgehen.

Aber Achtung: **Wann brauchen Sie auf jeden Fall eine Einwilligung?** Z.B. bei Personen, die noch nicht 14 Jahre alt sind.

- **Windows 7 läuft per 1.1.2020 ab! Alternative suchen!**  
Auf IT und EDV schaut die Behörde ganz genau. Bedenken Sie in diesem Zusammenhang, dass **per 1.1.2020 Windows 7 abläuft**, d. h. von Microsoft nicht mehr mit Updates versorgt wird. Sollten Sie dieses Betriebssystem also immer noch nutzen, schauen Sie sich **rechtzeitig um eine Alternative** um. Denn passiert Ihnen ein Hackerangriff oder ein anderes Datenleck, wird Ihnen die Behörde vorwerfen, dass Sie wegen des dann unsicher gewordenen Systems (mit-)schuld waren am eingetretenen Datenverlust.
- Die **FMA hat IT-Leitlinien** für die unterschiedlichen Branchen veröffentlicht. Schauen Sie sich an, was die Behörde sich hier von Ihnen erwartet. [Zum Nachlesen hier klicken...](#)
- **Vorsicht bei Nutzung von Videoüberwachung.** Damit beschäftigten sich bis dato die **meisten Verfahren bei der Datenschutzbehörde (DSB)**. Klären Sie also vorher ab: Haben Sie ein berechtigtes Interesse (z.B. Überwachung Server-Raum), wird kein Externer dadurch in seinen Rechten beeinträchtigt? Wird die Überwachung deutlich gekennzeichnet? Löschen Sie nach 72 Stunden etc.

Finaler Tipp für heute: Die **Adresse der Datenschutzbehörde hat sich geändert**. Viele von Ihnen haben sie aber in Formularen oder auf Webseiten stehen. Daher sollte das geändert werden.

**Neue Adresse der DSB lautet:**

Österreichische Datenschutzbehörde  
Barichgasse 40-42, 1030 Wien  
Telefon: +43 1 521 52-25 69  
E-Mail: [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

Quellen: Homepage der Datenschutzbehörde, DER STANDARD, Salzburger Nachrichten

Mitarbeit: Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche ([www.b2b-projekte.at](http://www.b2b-projekte.at))



**RA Mag. Stephan Novotny**  
Weihburggasse 4/2/26  
1010 Wien  
[kanzlei@ra-novotny.at](mailto:kanzlei@ra-novotny.at)