# DSGVO: Erste Urteile und Konkretisierungen

## Vor-Ort-Prüfungen, Whitelist zur Folgenabschätzung, Urteil zur Speicherdauer

Die erste Aufregung hat sich gelegt. Bis zum 25.5.2018 waren alle damit beschäftigt, „irgendwie" die DSGVO rechtzeitig zu meistern. In vielen Bereichen war unklar, wie die DSGVO korrekt umzusetzen ist. Daher **warten nun alle auf Konkretisierungen durch die Datenschutzbehörde** DSB bzw. **Entscheidungen von Gerichtsseite,** die die Auslegung der DSGVO und des österreichischen Datenschutzgesetzes präzisieren werden.

Die **Redaktion des BAV-Newsletters** wird daher in den nächsten Monaten sehr aufmerksam die DSB- bzw. Gerichtsurteile verfolgen und Ihnen, werte Leserin, werter Leser, in regelmäßigen Abständen über die Neuheiten berichten. Damit Sie am Letztstand sind und Ihre praktische Handhabung der DSGVO in Ihrem Unternehmen rechtskonform ist und bleibt.

**A) Vor-Ort-Prüfung der Datenschutzbehörde (DSB)!**
Auch **Sie können mithelfen, die Informationsbasis zu verbessern.** Konkret ersuchen wir um Informationen, wie die Vorort-Prüfungen der DSB ablaufen.

Wir erfuhren, dass die DSB **in Oberösterreich mit Vor-Ort-Kontrollen begonnen** habe und man sich da besonders für den Bereich „**Versicherungsvermittlung"** interessieren würde. Das ist insofern sehr logisch, als es sich bei uns um eine Branche handelt, wo sehr **viele personenbezogenen und auch zahlreiche sensible Daten** anfallen (Gesundheit, etc.).

Da noch sehr wenig über den **Ablauf/Inhalt** von Vor-Ort-Kontrollen der DSB bekannt ist, ersuchen wir alle, die darüber Details wissen, uns ein Mail mit Infos an **g.wagner@b2b-projekte.at** zu senden. Selbstverständlich behandeln wir Ihre Angaben **vertraulich** und würden nur allgemeine Informationen weitergeben.

**Für alle wäre etwa interessant zu wissen:**

- Hat sich die DSB **vorab angekündigt** und wie lange vorher?
- Bekam man im Vorfeld der Prüfung eine **Frageliste** zum Vorbereiten?
- **Wie lief die Vor-Ort-Prüfung ab** und wie lange dauerte sie?
- Was wollte die DSB im Detail sehen und **worauf legte sie besonders Wert?**
- Ging es „nur um **formale" Anforderungen** (Verfahrensverzeichnis, Vereinbarungen mit Mitarbeitern, Lieferanten, etc.) oder wurde etwa die Notwendigkeit von Datenschutzbeauftragten geprüft?
- Wurde die verwendete **Hardware-, Software-, IT-Lösung** bzw. z.B. das E-Mail-Programm (Verschlüsselung?) überprüft etc.
- Sah man sich den **Aufbau etwa der Kundendatei** näher an und kontrollierte man, welche Daten wie lange aufbewahrt werden?
- Wurden die **TOMs** überprüft? Wenn ja, wie genau und in welchem Umfang?
- Gab es **Verbesserungsaufträge bzw. Strafen?**
- usw.

Wir freuen uns über Ihren I**nput, den wir zum Nutzen aller aufarbeiten werden,** damit Sie sich noch besser auf die tägliche Praxis vorbereiten können. Nochmals unsere Garantie: Selbstverständlich behandeln wir Ihren Input anonym. Bitten also um ein E-Mail an g.wagner@b2b-projekte.at

**B) Whitelist der Datenschutzbehörde zur Datenschutz-Folgenabschätzung**

Da es nach wie vor viele Unklarheiten gibt, wird in den nächsten Monaten die Datenschutzbehörde sogenannte Whitelisten (was ist erlaubt) und Blacklisten (was ist verboten) herausgeben, um den Beaufsichtigten klarere Hinweise für die praktische Umsetzung zu geben.

Eine **erste Whitelist** betrifft die Frage, wann eine Datenschutz-Folgenabschätzung nötig bzw. nicht nötig ist! Insgesamt wurden **22 Verarbeitungen** bzw. Bereiche definiert, die keine Folgenabschätzung machen müssen.
Juristisch umgesetzt wurde die Whitelist in Form einer Verordnung der Datenschutzbehörde, diese können Sie hier als PDF näher ansehen und nachlesen, was alles genau unter die Begriffe fällt.

Für unseren Bereich könnte interessant sein, dass für folgende Datenverarbeitungen **KEINE** Folgenabschätzung nötig ist (Anmerkung in der Klammer durch die BAV-Redaktion):

DSFA-A01: **Kundenverwaltung,** Rechnungswesen, Logistik, Buchführung
DSFA-A02: **Personalverwaltung** für privatrechtliche und öffentlich-rechtliche Dienstverhältnisse (Anmerkung: inkludiert auch Lohn- und Gehaltsverrechnung)
DSFA-A03: **Mitgliederverwaltung** (inkl. Aufzeichnung von Förderbeiträgen)
DSFA-A04: **Kundenbetreuung und Marketing** für eigene Zwecke (gilt für eigene und zugekaufte Daten zum Zwecke der Geschäftsanbahnung, Newsletter-Versand, etc.)
DSFA-A05: **Sach-und Inventarverwaltung** (inkl. Anschaffungskosten, Lieferanten etc.)
DSFA-A07: **Zugriffsverwaltung für EDV-Systeme** (inkl. Benutzernamen, Passwörter, Zugriffsprotokollierung etc.)
DSFA-A08: **Zutrittskontrollsysteme** (aber nur, wenn keine biometrischen Daten – Fingerabdruck etc. – verarbeitet werden)
DSFA-A09: **Stationäre Bildverarbeitung** und die damit verbundene Akustikverarbeitung zu Überwachungszwecken – **Videoüberwachung!** (Achtung: gilt nur für „Örtlichkeiten, über die der Verantwortliche verfügungsbefugt ist", Speicherdauer max. 72 Stunden, Kennzeichnungspflicht! Nicht im „höchstpersönlichen Lebensbereich von Personen").
DSFA-A10: **Bild-und Akustikdatenverarbeitung in Echtzeit** (gemeint ist KEINE Aufzeichnung; Einschränkungen wie bei Punkt 9 beschrieben).
DSFA-A11: **Bild-und Akustikverarbeitungen zu Dokumentationszwecken** (darf nicht auf identifizierbare Erfassung unbeteiligter Personen abzielen)

**C) Urteil zu Speicherdauer – Darf man für alte Kontoauszüge Geld verlangen?**

Der **erste Bescheid der Datenschutzbehörde (DSB) nach dem 25.5.2018** beschäftigte sich genau mit obiger Frage. Zwar betraf der **Anlassfall eine Bank,** könnte aber genauso auf die Versicherungsbranche zutreffen. Denn es geht um die Frage, kann ein Unternehmen für die **nachträgliche Aushändigung von Daten Geld verlangen** oder **fällt das unter das Auskunftsrecht,** das die DSGVO dem Einzelnen nun ausdrücklich einräumt.

Wie schon oben angerissen, wird die DSB im Laufe der nächsten Jahre viele Unklarheiten in der Auslegung der DSGVO klarstellen. Dazu **werden Anlassfälle aus der täglichen Praxis** herangezogen werden. Diese wird die DSB **prüfen**, sich darüber ein Urteil bilden und ihre **Erkenntnisse in Bescheiden festlegen.**

Solche Entscheidungen sollte man **nicht ignorieren, sondern nutzen, um zu prüfen**, ob das bisherige eigene Vorgehen richtig war und falls nein, dieses zu adaptieren.

Und noch etwas kann man **aus diesem Fall lernen**, nämlich, dass man **Kundenanfragen keinesfalls ignorieren sollte.** Denn verärgerte Kundinnen und Kunden beschweren sich daraufhin bei der DSB und der Fall kommt ins Rollen, wie wir gleich lesen werden.

Worum genau ging es beim Anlassfall? Es begann harmlos, in dem der Kunde offensichtlich alte Kontoauszüge nachgedruckt haben wollte, wofür die Bank aber EUR 30 pro Jahr verlangte. Darüber verärgert, stellte der Kunde ein **Auskunftsbegehren nach der DSGVO UND ERHIELT KEINE ANTWORT.**

**Tipp:** Von so einem Vorgehen können wir nur **ABRATEN,** wenn Sie Auskunfts- und Löschanfragen erhalten. Denn die Folge war, dass sich der Auskunftswerber bei der Datenschutzbehörde DSB beschwerte.

**Über das korrekte Vorgehen** (wann, in welcher Form, wie stellt man Identität fest, welche Formulare etc.) haben wir in einem Artikel des BAV-Newsletters bereits genau berichtet. Hier zum Nachlesen…

Nach Prüfung des Sachverhalts **entschied die DSB,** dass es sich hier um eine **Verletzung des Rechts auf Auskunft** handle. Die Bank müsse „die ersuchten Kontoauszüge innerhalb einer Frist von zwei Wochen zur Verfügung stellen – und künftig kostenlos Auskunft erteilen, wenn von dem Recht Gebrauch gemacht wird" so wird aus dem Urteil im STANDARD zitiert.

Und weiter: **Alle Kontoauszüge zu verlangen sei nicht exzessiv!**

Der **Argumentation der Bank,** dass personelle Ressourcen und damit Kosten entstehen würden, **folgte die Behörde nicht.** Die Bank muss also kostenlos Auskunft erteilen und auch historische Kontoauszüge zur Verfügung stellen.

Da uns der Bescheid nicht im Wortlaut vorliegt, können wir nur mutmaßen, ob neben dem Recht auf Auskunft nicht auch das **Recht auf Übertragbarkeit** bei der Urteilsfindung eine Rolle spielte. Da über das letztgenannte Recht erst ganz selten zu lesen war, möchten wir dieses in Erinnerung rufen, denn es könnte etwa bei uns dann eine Rolle spielen, **wenn eine Kundin/ein Kunde seine Versicherung wechselt.**

**Zur Erinnerung:** Die DSGVO brachte bzw. verschärfte die Rechte der Betroffenen.
Es gibt das Recht auf Information (beim Erheben der Daten), auf Auskunft, auf Berichtigung, auf Löschen und des Vergessenwerdens. Weiters ein Recht auf Einschränkung der Verarbeitung (wenn sich das Löschen nicht sofort umsetzen lässt) und ein **Recht auf Datenübertragbarkeit** (etwa, um Daten von einer Versicherung zu einer anderen mitzunehmen).
**Details zu den Betroffenenrechten** können Sie hier nachlesen.

Im **nächsten BAV-Newsletter** berichten wir dann über ein Urteil, das klarstellt, ob/wann die DSGVO auch für Papier-Unterlagen gilt und ein Urteil zur Speicherdauer bei Telekoms und Co und möglichen weiteren Klarstellungen! Ich prognostiziere: Die Arbeit wird uns nicht ausgehen!

Recherche-Quellen: Mag. Günter Wagner, B2B-Projekte und RA Mag. Stephan Novotny (Spezialgebiet Versicherungen & Datenschutz-Grundverordnung), Praxishandbuch „Das österreichische Versicherungsvermittlerrecht" (wurde gerade auf Stand 2018 aktualisiert, Details dazu hier…), Der Standard, Homepage der Datenschutzbehörde.