Weitere Urteile und Konkretisierungen zur DSGVO

Wann gilt Datenschutz bei Papierunterlagen? Abmahn-Briefe wegen fehlender SSL-Verschlüsselung zurecht?

Im vorigen BAV-Newsletter haben wir über erste Urteile und Konkretisierungen zur DSGVO berichtet. Einerseits hatte die Datenschutzbehörde eine **Whitelist** zur Klärung der Frage, wer eine **Datenschutz-Folgenabschätzung** machen muss und wer nicht, veröffentlicht.

Und dann hatten wir über ein **Urteil** der DSB informiert, das der Frage nachging, ob man als Unternehmen für die **Ausfolgung alter Daten** (etwa eines Kontoauszugs, kann aber ebenso eine Versicherungspolizze etc. sein) Geld verlangen dürfen.
Sollten Sie diese beiden – auch für Ihre tägliche Praxis – **nützlichen Informationen** übersehen haben, hier können Sie sie nachlesen …

Heute bringen wir **Teil 2** der losen Serie, die sich die Präzisierungen zum Thema DSGVO näher ansieht und für Sie praxisorientiert aufbereitet, damit Sie **am Letztstand bleiben** und Ihre praktische Umsetzung der DSGVO in Ihrem Unternehmen überprüfen und bei Bedarf adaptieren können.

a) EuGH-Urteil zu Datenschutz bei Papier-Unterlagen und Praxis-Tipp dazu

Heute informieren wir über ein **Urteil** des Europäischen Gerichtshofes, das **über den Anlass hinaus für jeden Bedeutung hat.** Nämlich dass die Datenschutzbestimmungen auch für Papierakten gelten.

Anlass war ein Verfahren in Finnland gegen die Zeugen Jehovas. Diese führen Haustürgespräche und fertigen davon Notizen an. Dabei werden etwa Name und Adresse, aber auch religiöse Überzeugung und Familienverhältnisse erfasst. Aus Sicht der Zeugen Jehovas würde das unter individuelle **Religionsausübung** fallen. Die Notizen seien rein persönlicher Natur argumentierte die Gegenseite, berichtete DER STANDARD über die Ausgangslage.

Der finnische Datenschutzbeauftragte dagegen verbot den Zeugen Jehovas, bei ihren Hausbesuchen **personenbezogene Daten** zu erheben und zu speichern. In der Folge wollte ein finnisches Gericht vom EuGH wissen, ob sich die Glaubensgemeinschaft an die EU-Datenschutzrichtlinie halten müsse.

EU-Richter bestätigen Datenschützer

Der Europäische Gerichtshof urteilte, dass sich die Zeugen Jehovas bei ihren Tür-zu-Tür-Besuchen **an die aktuell gültigen Datenschutzbestimmungen halten müssen.** Die Haustürgespräche seien keine ausschließlich persönliche oder familiäre Tätigkeit und fielen deshalb nicht unter die Ausnahmen der bis vor kurzem gültigen EU-Regeln, urteilten die Luxemburger Richter (Rechtssache C-25/17).

Aber: Die erhobenen Daten müssten so leicht auffindbar sein, dass man von einer Datei im Sinne der Datenschutzrichtlinie sprechen könne.

Und hier sind wir bei der allgemeinen Bedeutung des Urteils, über den Anlassfall hinaus. Denn viele denken bei der Befolgung der DSGVO nur an elektronische Datenverarbeitung, also digital gespeicherte Daten. Und vergessen auf die **„guten alten Papierakten".**

Der auf Versicherungs- und Datenschutzrecht spezialisierte **RA Mag. Stephan Novotny** hat diese Frage im aktualisierten Praxishandbuch **„Das österreichische Versicherungsvermittlerrecht**" (erhielt eine großes Sonderkapitel zur DSGVO-Umsetzung, alle Details hier…) bereits beantwortet:

*„Wenn die **Papierakten nach einem System aufbewahrt** werden, fallen sie auch unter die DSGVO. Kann ich etwa in einem Aktenschrank nach dem Namen suchen und die Akte finden, dann gilt die DSGVO. Mache ich mir Notizen auf einem Zettel und lege diesen in einer Schachtel unsystematisch ab, gilt hierfür die DSGVO nicht."*

Und zu diesem Themen-Kreis passt auch noch **folgender Praxis-Tipp,** der sich mit der Frage beschäftigt: „Gibt es eine gesetzliche Vorgabe für die **Archivierung von unterschriebenen Versicherungsanträgen** durch mich?"

Dazu **wieder Mag. Novotny:** *„Gesetzlich geregelt ist, dass Unterlagen zumindest für die Finanzbehörden 7 Jahre aufbewahrt werden müssen. Hierfür reicht aber eine elektronische Archivierung aus, sodass der Papierantrag grundsätzlich vernichtet werden kann/könnte. Außer es gibt eine anders lautende vertragliche Vereinbarung mit Versicherer, Kunden etc. Aber das wäre dann keine gesetzliche Regelung, sondern eine vertragliche Vereinbarung."*

Zusatzfragen: Wenn Ja, muss ich diese im Original archivieren? Oder kann ich alle Anträge vernichten, sobald ich diese an die Versicherung weitergeleitet habe? (Über das Programm der Versicherung habe ich ohnehin Zugriff auf die Anträge.)

Mag. Novotny: *„Nein, elektronische Archivierung reicht grundsätzlich. Aber ich würde aus Beweisgründen selbst eine elektronische Archivierung vornehmen und die Daten auch selbst bei mir speichern. In möglichen Streitfällen könnte drohen, dass die Versicherung die Anträge „ungern" herausgibt, auch wenn es sich um sogenannte gemeinsame Dokumente handelt. Auch können Server gehackt und Daten zerstört werden, wodurch eine zusätzliche Sicherung von Vorteil sein könnte."*

b) Auswirkungen der DSGVO auf IT

Dass die Datenschutz-Grundverordnung auch auf die verwendete Hard- und Software sowie IT-Technologie Auswirkungen hat, ist angesichts der ständig zunehmenden Gefahren aus dem Internet nur logisch. Immerhin können Hackerangriffe die Sicherheit der Daten Ihrer Kunden, Mitarbeiter, Projektpartner usw. gefährden.

Da Sie aber für die **Sicherheit der personenbezogenen Daten** verantwortlich sind, ist also eine EDV- und IT-Ausrüstung auf aktuellstem Stande dringend anzuraten. Konkret schreibt Ihnen die DSGVO „**geeignete technische und organisatorische Maßnahmen"** vor, um ein „angemessenes Schutzniveau" zu gewährleisten. Es wird bei der Beurteilung sicherlich berücksichtigt werden, ob es sich um einen Großkonzern (wird wohl mehr und umfassendere Vorkehrungen zu treffen haben) oder ein kleines EPU gehandelt hat. Aber keinesfalls darf man dieses Thema außer Acht lassen.

Und in „typische Fallen des Internets" sollte man auch nicht reintappen. Denn **rasch könnte ein Richter zur Ansicht gelangen,** dass man niemals so dumm hätte sein dürfen, auf den Link im nigerianischen Mail zu klicken, weil darin eine theoretische Millionen-Erbschaft versprochen wurde. Tatsächlich hat man damit dem Hacker Zugang zu allen Passwörtern etc. verschafft und somit die Datensicherheit gefährdet.
Um Sie **diesbezüglich vorzuwarnen und auf dieses Problem besonders zu sensibilisieren,** haben wir Ihnen im letzten BAV-Newsletter als Praxistipp die Watchlist Internet ans Herz gelegt, weil dort wöchentlich auf die aktuell im Netz kursierenden Fallen hingewiesen wird. **Zum Nachlesen** hier klicken…

Heute möchten wir zu diesem Themenkreis auf einen **aktuellen Anlassfall verweisen**, der unserer Ansicht nach wiederum über den Anlassfall hinaus für jedermann Auswirkungen hat. Es geht um das Thema:

Sichere Homepage, sicheres Formular. SSL-Verschlüsselung?

Der konkrete Anlassfall der in EDV-Fachmedien (u.a. Heise) heftig diskutiert wird, klingt wie eine „Räubergeschichte" und scheint auch „reine Geschäftemacherei". Dennoch zeigt der Fall berechtigte Probleme auf, auf die man vorbereitet sein sollte. Daher haben wir am Ende des Beitrags **Praxistipps** für Sie zusammengefasst.

Was ist der Anlass?
In Deutschland versendet ein (für so ein Vorgehen bereits bekannter) **Rechtsanwalt Abmahnbriefe und fordert Tausende Euro von Firmen.** Es gibt Schreiben mit Schadenersatzforderungen von EUR 8.500 und sogar EUR 12.500 für eine nicht vorhandene SSL-Verschlüsselung.
Der Anwalt argumentierte, dass sein **Kunde bei einem Händler ein Online-Formular ausgefüllt** habe. Erst im Nachhinein hätte sein Kunde gemerkt, dass die „Homepage ohne https als Transportverschlüsselung" die Formular-Daten versandt hätte. Und damit „lägen ganz erhebliche Verletzungen bei der Verarbeitung der Daten seines Mandaten" vor.

Und der Anwalt verweist im Schreiben auf **Artikel 82 der DSGVO,** worin tatsächlich davon die Rede ist, „dass jede Person, der wegen eines Verstoßes gegen die Vorschriften des Datenschutzes ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz zusteht". Im **„Erwägungsgrund 75"** werden dazu Beispiele wie etwa „finanzieller Verlust, Rufschädigung, Identitätsdiebstahl oder -betrug oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile" erwähnt.

Juristen bezweifeln aber, dass durch das bloße Behaupten eines Schadens Schadenersatz zugesprochen werde, noch dazu in dieser Höhe. Auch die **Fachgruppe Information und Consulting in der WKO** kam in ihrem Newsletter zu dieser Ansicht, denn „es muss ein konkreter Schaden entstanden (sein) und dargelegt werden".

Aber: Was können wir daraus lernen?

Kehren wir nun vom Anlassfall auf die übergeordnete Ebene zurück. **Wie kann man solche Schwierigkeiten vermeiden?**

Wenn Sie eine Website haben, dann speichert diese „ganz automatisch" viele Daten der Besucher. Zumeist in Form von Cookies. Das sind kleine Textdateien, die Name, IP-Adresse, besuchte Webseiten etc. speichern und damit helfen, den Besucher wiederzuerkennen und ihm z.B. individuelle Werbung anzubieten. Damit gelingt es großen Konzernen wie Amazon, Google, Facebook & Co, über die Jahre ein umfangreiches Bild einer Person und deren Vorlieben zu erstellen. Besonders bedenklich aus der Sicht der DSGVO ist es, diese personenbezogenen Daten, die sich in den Cookies verstecken, auf amerikanische Server zu übertragen, weil in den USA die Datenschutzbestimmungen für Europäer nicht die Anforderungen der DSGVO erfüllen. Wenn sich also Google nicht der europäischen DSGVO unterwirft, dann sollten Sie Web-Analyse-Tools wie etwa Google Analytics nicht verwenden.

Die DSGVO erwähnt explizit das Wort Cookies nicht.
Dazu sollte es bald nach dem 25.5.2018 eine ePrivacy-Verordnung geben, die die neuen Regeln für den Umgang der digitalen Medien und elektronischen Kommunikationsdienste mit der DSGVO festlegen soll. Leider warten wir noch immer darauf. Die Unternehmen versuchen daher, mit „irgendwelchen Hinweisen" auf die Nutzung der Cookies aufmerksam zu machen und sich damit abzusichern.

Doch von den Cookies abgesehen, speichert der Server, auf dem Ihre Homepage „liegt", Daten der Besucher ab. Besonders dann, wenn Sie ein **Feedback-Formular, Bestell-Formular etc**. nutzen, werden dort eingegebene Daten auf dem Server gespeichert und Ihnen z.B. per E-Mail zugesandt. Und genau auf diesen Punkt zielt das Abmahnschreiben ab!

Für viele EDV-Leute gilt die **SSL-/TLS-Verschlüsselung der Webseiten** – besonders dann, wenn dort Formulare verwendet werden – mittlerweile als **Stand der Technik.** Zwar gibt es dazu noch keine Vorgabe der DSB und kein Urteil eines Gerichts, das dies vorschreibt/bestätigt. Aber Vorsichtige sollten sich zu dieser Verschlüsselung entschließen, insbesonders dann, wenn personenbezogene Daten aus Formularen übermittelt werden.

Zur Technik selbst (Quelle: Datenschutzbeauftragter-info.de):
SSL steht für Secure Socket Layer und TLS steht für Transport Layer Security, das ist jeweils ein Protokoll, mit dem Daten **über eine verschlüsselte Verbindung** im Internet übertragen werden. Als Nutzer erkennen Sie eine verschlüsselte Verbindung daran, dass im Browser ein **kleines Schloss-Symbol** auftaucht, und daran, dass die Webadresse ein zusätzliches „s" hat. Also statt http steht **„https".** Bei beiden Protokollen handelt es sich um eine End-to-End-Verschlüsselung, d.h. dass die Informationen bereits vor dem Versenden verschlüsselt und erst beim Empfänger entschlüsselt werden.

Was sollten Sie also tun?

Das hängt natürlich von Ihrem Unternehmen selbst ab, wie auch die WKO Fachgruppe Information & Consulting zusammenfasste:

„Demnach sind

- *unter Berücksichtigung des **Stands der Technik** (was ist am Markt üblich?),*
- *der **Implementierungskosten** (was kann das Unternehmen finanziell leisten?) und*
- *der Art, des Umfangs, der Umstände und der Zwecke **der Verarbeitung** (wie riskant ist die Datenverarbeitung?) sowie*
- *der unterschiedlichen **Eintrittswahrscheinlichkeit** (wie wahrscheinlich ist der Fall eines Data Breaches?) und*
- ***Schwere des Risikos** (wie schlimm könnte ein Data Breach ausfallen?) für natürliche Personen*

***geeignete technische und organisatorische Maßnahmen** zu setzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.*

*Die konkret geeigneten Maßnahmen sind also je nach Unternehmen unterschiedlich und richten sich nach dem, was das Unternehmen tut, wie groß das Unternehmen ist, welche finanziellen Möglichkeiten es hat und so weiter. **SSL-Verschlüsselung** ist mittlerweile wohl als Stand der Technik anzusehen und deren überschaubare Kosten vertretbar, weshalb deren Verwendung auch mit Blick auf das gegenständliche Abmahnverfahren **unbedingt empfehlenswert** ist." So die WKO in ihrem entsprechenden Newsletter.*

Praxistipp:
Überlegen Sie, wozu Sie Ihre Homepage einsetzen.
Nutzen Sie sie „nur" dazu, um Informationen über Ihre Produkte und Dienstleistungen zu veröffentlichen? Dann bringt eine SSL-/TLS-Verschlüsselung keine Verbesserung für die Nutzer.

Oder bieten Sie dort auch **Kontakt- oder sogar Bestellmöglichkeiten** (Feedback-Formular, Anmeldungs-Formular, Bestellung etc.) an? Gibt es die Möglichkeit, unter (Blog-)Beiträgen eigene Kommentare zu hinterlassen? Etc.?
In diesen Fällen gibt es nach EDV-Experten nur **2 Möglichkeiten:**

- **Deaktivieren Sie solche Formulare** und stellen Sie auf **E-Mail** um:
  „Senden Sie uns Ihre Information, Bestellung per E-Mail an Firma@e-mail.at".
  Sendet der Benutzer ein E-Mail an Sie, dann liegt das Risiko der unsicheren Übertragung beim Sender und nicht mehr bei Ihnen.
- In allen anderen Fällen ist wohl die **Umstellung auf eine SSL-/TLS-Verschlüsselung** der Homepage zu empfehlen.

Recherche-Quellen: Mag. Günter Wagner, B2B-Projekte und RA Mag. Stephan Novotny (Spezialgebiet Versicherungen & Datenschutz-Grundverordnung), Praxishandbuch „Das österreichische Versicherungsvermittlerrecht" (erhielt kürzlich ein großes Sonderkapitel „praktische Umsetzung DSGVO, Details dazu hier …), Homepage Heise.de, Newsletter WKO Information & Consulting, Homepage Datenschutzbeauftragter-info.de