DSGVO: Urteil zur maximalen Speicherdauer

Was bedeutet das Urteil für die Praxis? Was kann/sollte man tun?

Vorgestern schlagzeilte DER STANDARD **„Bislang vier Strafen wegen DSGVO-Verstößen seit Mai.** 59 Prozent aller heimischen Unternehmen sollen immer noch bei der Umsetzung hinterherhinken."

Wer nur die Überschrift las, hat sich wohl entspannt in den Sessel zurückfallen lassen und sich bestätigt gefühlt, das Thema zu ignorieren. Motto: Steht sich doch nicht dafür, dass ich mich mit dem Thema weiterhin beschäftige. Diese Einschätzung wird auch dadurch bestärkt, dass Österreich in seiner **nationalen Umsetzung** der DSGVO die Strafdrohungen merklich entschärft hat (wir erinnern uns an das Motto: „Mahnen statt strafen"). Zwar halten namhafte Juristen diese Vorgehensweise für bedenklich/unzulässig und ein **EU-Verfahren steht im Raum.** Was aber durch die langsam mahlenden (EU-)Mühlen noch ein wenig dauern wird.

Also zurücklehnen? Nein, keinesfalls.
Vergessen Sie nicht, die DSGVO ist das erste EU-GESETZ überhaupt. Bisherige EU-Vorgaben waren EU-RICHTLINIEN, bei denen der EU-Gesetzgeber eine Mindestvorgabe definiert. In solchen Fällen kann der nationale Gesetzgeber die Umsetzung landesspezifisch gestalten, solang er nicht die Mindestvorgaben verletzt.
Die DSGVO dagegen ist – nach einer 2-jährigen Übergangsfrist bis 25.5.2018 – sofort und **unverändert in allen EU-Ländern anzuwenden.** Und dort findet sich nichts von einem Ansatz „Mahnen statt strafen", sondern das genaue Gegenteil. Es wurden ganz bewusst **horrende Strafen von bis zu EUR 20 Mio. oder 4 % des Konzernumsatzes definiert,** um die Ernsthaftigkeit des Anliegens und die Wichtigkeit des Datenschutzes zu unterstreichen**.** Selbst wenn nur niedrigere Strafen zur Anwendung kämen, wäre dies für den Großteil der österreichischen Firmen durchaus **existenzbedrohend.**

Vergessen Sie weiters nicht, dass **die Finanz- und Versicherungsbranche** sehr **viele personenbezogene und auch so manche heikle, sensible Daten der Kunden** abspeichert (Gesundheitsdaten!). Es ist also nur eine Frage der Zeit, bis die Datenschutzbehörde DSB hier **Detail-Prüfungen vor Ort vornehmen wird** – auch wenn sich vielleicht noch kein Kunde beschwert hat.

Doch warum gab es in den ersten 6 Monaten erst so wenige (und noch dazu so geringe) Strafen?
Die geringe Höhe ist rasch erklärt. Es wurden bisher keine großen Verfahren wegen gravierender Verfehlungen beendet und die Bestraften haben aktiv mit der Behörde kooperiert, was sich positiv auf die Strafhöhe auswirkte. Daher wurden lediglich Strafen von EUR 300 bis EUR 4.800 verhängt. Die bisher abgewickelten Verfahren haben sich hauptsächlich mit dem Themenkreis „unzulässige Videoüberwachung" beschäftigt und dieses Vergehen wurde „human bestraft".

Bevor wir auf ein sehr **interessantes Urteil zur Begrenzung der Speicherdauer** eingehen, noch ein paar weitere Fakten zu den Verfahren bei der DSB.

Die DSGVO ist nun seit 6 Monaten in Kraft. Die **DSB hat in dieser Zeit rund 900 Beschwerden** erhalten (Quelle: DER STANDARD) und muss nun diese Verstöße überprüfen. Da es im gesamten Jahr 2017 laut Andrea Jelinek, Leiterin der Datenschutzbehörde, nur 530 Meldungen potenzieller Verstöße gegeben hat (laut TREND-Bericht) bedeutet das immerhin eine gute **Verdreifachung** der Beschwerden. Dass es nicht viel mehr sind, liegt auch daran, dass die Regierung im Begleitgesetz zur DSGVO verhindert hat, dass private Datenschutzorganisationen für Dritte Schadenersatz bei etwaigen Verstößen vor Gericht einklagen können. Viele sehen das als **Maßnahme gegen den Noyb-Verein,** den der österreichische **Datenschützer Max Schrems** gegründet hat (noyb steht für none of your business, auf Deutsch „Das geht Sie nichts an" – gemeint sind natürlich die persönlichen Daten). Daher konzentriert sich **Noyb jetzt auf die großen Datenkraken** und hat Beschwerden gegen Google (max. Strafhöhe EUR 3,7 Mrd.), Instagram (EUR 1,3 Mrd.), WhatsApp (EUR 1,3 Mrd.) und Facebook (EUR 1,3 Mrd.) eingebracht. **Details** dazu unter www.noyb.eu. Klar ist, JEDES Urteil wird neue Klarstellungen bringen, die auch die Klein- und Mittelbetriebe berücksichtigen müssen.

Sehr bedenklich ist auch der zweite Teil der Überschrift des STANDARDS, **wonach 59 %** der österreichischen Unternehmer die DSGVO noch **nicht (vollständig) umgesetzt hätten** (das teilte kürzlich der Gläubigerschutzverband KSV1870 in einer Aussendung mit).

Fakt ist, dass vieles nach wie vor nicht ganz klar ist, trotzdem die DSGVO seit 25.5.18 gilt. Das aber als Ausrede herzunehmen, um nicht oder nur im geringen Maße die DSGVO umzusetzen, ist unserer Ansicht nach **grob fahrlässig**. Denken Sie nur an die Möglichkeit, dass ein **unzufriedener Kunde** eine (berechtigte oder auch nicht berechtigte) Beschwerde bei der DSB einbringen kann und diese dann die Beschwerde als Anlass nimmt, um Sie zu überprüfen!

Und die noch bestehenden Unklarheiten werden in den nächsten Monaten und Jahren durch sukzessive Klarstellungen der Datenschutzbehörde DSB (was ist erlaubt, wie hat Umsetzung auszusehen, was geht keinesfalls etc.) oder durch Gerichtsurteile beseitigt werden.
Daher werden wir Sie, **werte Leserin, werter Leser auch in den nächsten Monaten** immer wieder auf derartige Klärungen hinweisen, damit Sie überprüfen können, ob dieses Urteil, diese DSB-Entscheidung auch für Ihr Unternehmen zutrifft und Sie womöglich Ihr Vorgehen ändern müssen.

Urteil der DSB zur maximalen Speicherdauer von personenbezogenen Daten

Vor wenigen Wochen wurde eine Entscheidung der DSB bekannt, von der man nur hoffen kann, dass sie nicht als künftige Handlungsanleitung („Blaupause") für andere Unternehmen herangezogen wird, weil es nämlich dann **keine Chance** gäbe, um sich nach einigen Jahren gegen behauptete Vorwürfe wehren und **freibeweisen zu können.**

Worum ging es in dem Verfahren?
Eine einstige Kundin einer Telekom-Firma verlangte Auskunft, welche Daten von ihr nach ihrer Kündigung noch gespeichert seien. Dadurch erfuhr sie, dass die Firma neben Name, Adresse, SIM-Daten u.a. auch Geburtsdatum, Pass- und Kontodaten etc. nach wie vor gespeichert hat. Daraufhin brachte sie eine Beschwerde bei der Datenschutzbehörde ein.
Und das Ergebnis der Prüfung ist nun die **erste Entscheidung der DSB zur Dauer der Datenspeicherung,** seitdem die DSGVO in Kraft getreten ist.
Zwar nimmt die Behörde auf die speziellen Bestimmungen des **Telekommunikationsgesetzes** (TKG) Bezug, verweist aber ausdrücklich auch auf die DSGVO und das dort definierte Prinzip der **Speicherbegrenzung.** Und kommt zum Schluss, dass die Datenverarbeitung (und damit die Speicherung) rechtswidrig seien. Ein Urteil, das für unsere Branche **große Probleme verursachen könnte, wenn es 1:1 angewendet würde.**

Konkret steht im Urteil, das Sie hier herunterladen und nachlesen können wie folgt:
„Wenn sich die Beschwerdegegnerin (Anmerkung Redaktion: also die Telekom-Firma) bei der Speicherung von Stammdaten auf die zehnjährige Frist des § 207 Abs. 2 BAO beruft (Anmerkung: BAO ist die Bundesabgabenordnung und regelt u.a. die Verjährung von Abgaben), so verkennt sie, dass hierbei lediglich eine Verjährungsfrist, jedoch keine konkrete Verpflichtung zur Aufbewahrung von Daten normiert wird. Eine gesetzliche Verpflichtung, Stammdaten über die Frist nach § 97 Abs. 2 TKG 2003 aufzubewahren, kann aus § 207 Abs. 2 BAO nicht abgeleitet werden. Auch der Verfassungsgerichtshof geht in seiner jüngeren Rechtsprechung davon aus, dass die weitere Aufbewahrung von Daten durch ein sich konkret abzeichnendes Verfahren gerechtfertigt sein muss. Die bloße Möglichkeit, dass ein Verfahren eingeleitet wird, reicht hingegen nicht aus (siehe dazu das Erkenntnis vom 12. Dezember 2017, GZ E3249/2016)."
Es ist schwer abzuschätzen, ob die DSB eine andere Entscheidung getroffen hätte, wenn sich die Telekom-Firma nicht ausdrücklich auf die 10-jährige Frist des §207 BAO berufen hätte.

Denn an anderer Stelle des Urteils steht:
„Anders verhält es sich mit § 132 Abs. 1 BAO, welcher eine Aufbewahrungspflicht von Büchern und Aufzeichnungen für sieben Jahren normiert und somit auch den datenschutzrechtlichen Vorgaben des Art. 5 Abs. 1 lit. e DSGVO bzw. von § 97 Abs. 2 TKG 2003 entspricht. Die Beschwerdegegnerin ist daher befugt, Stammdaten gemäß § 132 Abs. 1 BAO für die Dauer von sieben Jahren aufzubewahren."
Diese Passage im Urteil bedeutet, dass Sie personenbezogene Daten u.a. **für Steuerzwecke 7 Jahre aufbewahren** dürfen, weil Sie die Daten (für Kontrollen) aufbewahren MÜSSEN.

Beweisnotstand nach 7 Jahren?
Speziell für unsere Branche ergibt sich das **Problem, dass Prozesse erst viele Jahre später eintreten.** Denken Sie an die letzten 10 Jahre, wo zahlreiche (etwa über schlechte Performance) verärgerte Kunden zu Recht oder Unrecht Jahre später eine **unvollständige/falsche Beratung behaupteten und Klagen einbrachten.** Und sich für die „beteiligten Firmen" daher die Notwendigkeit des Freibeweisens stellte und künftig weiter stellen wird.
Denn: **Wie soll man Beweise für ein korrektes Arbeiten vorlegen**, wenn man alle personenbezogenen Daten (etwa das Beratungsprotokoll) nach Ablauf der gesetzlich vorgesehenen Aufbewahrungspflicht – also der 7 Jahre – löschen muss?

Sollte also obiges Urteil der Datenschutzbehörde als Blaupause für weitere Verfahren dienen, dann drohen große Probleme für die Vermittler, aber auch Banken, Versicherungen, Wertpapierfirmen etc.

Wir haben daher Mag. Stephan Novotny, Rechtsanwalt mit Spezialisierung auf Versicherungsrecht und DSGVO um seine Einschätzung gebeten.

„Nach Studium der Entscheidung, angeführten Gesetzesstellen und zitierten Judikatur des Verfassungsgerichtshofes ist eine gewisse Tendenz erkennbar, dass Daten nur so lange aufbewahrt werden dürfen, als es dazu eine gesetzliche Verpflichtung gibt.

1. Im gegenständlichen Fall geht es allerdings um bestimmte im TKG 2003 schon angeführte Aufbewahrungsfristen für Stamm- und Verkehrsdaten, *die von der Telekom Gesellschaft nicht eingehalten wurden, insbesondere im Hinblick auf die Verkehrsdaten (sechs statt drei Monate). Ob die Begründung der Entscheidung dann auch für die Versicherungswirtschaft so ausfallen würde, dass personenbezogene Daten nicht länger als in der BAO vorgesehen aufbewahrt werden dürfen, ist die Frage. Die Begründung, dass sie* nur bei anhängigen oder drohenden Verfahren länger aufbewahrt werden dürfen, *als in der Vorschrift zur Aufbewahrungspflicht vorgesehen, ist zumindest „interessant", falls sie auch für die 30-jährige Frist für Schadenersatzansprüche gegen Versicherungsvermittler verwendet werden sollte.*

2. In der zitierten Entscheidung des Verfassungsgerichtshofes *ging es um die Aufbewahrung von personenbezogenen Daten bei einem Finanzamt und die Abwägung zwischen Überwiegen des öffentlichen Interesses an der Aufbewahrung der Akten gegenüber dem Löschungsinteresse der Beschwerdeführerin. Auch hier war die Möglichkeit, dass die Beschwerdeführerin weitere Anträge und Klagen gegen das Finanzamt einbringt, nicht ausreichend, um die Daten weiterhin (also länger) aufbewahren zu dürfen.*

3. Soweit mir ersichtlich liegt NOCH KEINE Entscheidung über personenbezogene Daten von Versicherungskunden vor. *Auch Judikatur seitens der DSB habe ich dazu keine gefunden. Es gilt daher noch abzuwarten.*

Wenn das obige Urteil als „Blaupause" für alle Branchen und Unternehmen verwendet werden sollte, dann ist anzunehmen, dass die oftmals im Verfahrensverzeichnis definierte 30-jährige Speicherfrist nicht erlaubt sein wird. *Was sehr unbefriedigend wäre, weil sich der Versicherungsvermittler im Einzelfall dann nicht freibeweisen kann, weil er nicht mehr über bestimmte Daten verfügt, die er dazu allenfalls braucht.*

Zwar glaube ich nicht, dass dieses Urteil 1:1 auf unsere Branche angewandt *werden wird (denn Spätschäden treten oft erst nach vielen Jahren auf), aber mit Sicherheit kann man das erst dann feststellen, wenn weitere Urteile (Datenschutzbehörde und/oder Gerichte) zu diesem Themenkreis gefällt werden. Wahrscheinlich gilt es im Einzelfall abzuwägen: Das Interesse des Einzelnen (auf Löschen) gegenüber den berechtigten Interessen des Versicherungsvermittlers/Versicherers, sich z.B. in Fällen, in denen er wegen falscher Beratung in Anspruch genommen wird, freibeweisen zu können."*

Wie soll man sich also verhalten? Ein paar praktische Überlegungen:

a) So lange es keine weiteren Urteile gibt, die ausdrücklich die Löschpflicht nach 7 Jahren auch für die Finanz- und Versicherungsbranche festlegen, sollte man sich weiterhin für drohende Prozesse rüsten und **alles dokumentieren und speichern. (Vielleicht nützt Ihnen das kostenlose Tool, das wir Ihnen im Punkt 2 dieses Newsletters vorstellen.)**

b) **Aufgrund der IDD** sind Sie verpflichtet, die **Beratung zu dokumentieren.** Dies sollten Sie daher unbedingt tun (auch um beweisen zu können, dass Sie innerhalb des Zielmarktes vermittelt haben etc.) und danach abspeichern, um sich künftig freibeweisen zu können.

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

Häufige Frage dazu: 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: *„Ich würde aus Beweisgründen selbst eine elektronische Archivierung vornehmen und die Daten auch selbst bei mir speichern. Zwar handelt es sich um sogenannte „gemeinsame Dokumente", in möglichen Streitfällen könnte drohen, dass die Dokumente nicht auffindbar sind."*

c) **Holen Sie sich vom Kunden** – z.B. im Zuge des Ausfüllens des Beratungsprotokolls – die **Zustimmung** zur Speicherung bis zum Ablauf der absoluten Verjährungsfrist ein. Am besten in jene Passagen einarbeiten, die das Speichern der personenbezogenen Daten betreffen und unterschreiben lassen.

d) Füllen Sie das **Verfahrensverzeichnis korrekt** aus und definieren Sie für jede Datenkategorie, wie lange sie diese speichern und warum. Es ist anzunehmen, dass die DSB sich bei Prüfungen bzw. Rechtsstreitereien dieses Verzeichnis genau ansehen und die dortigen Begründungen prüfen wird.

e) Auch eine vorbildliche Umsetzung der DSGVO z.B. in Form eines genau beschriebenen und in der Praxis eingehaltenen Prozesses für **Auskunfts- und Löschbegehren** sollte Punkte bei der Prüfung bringen. In einem **Lösch-Konzept** könnten Sie z.B. definieren, welche Daten Sie im Falle eines Löschwunsches löschen können (z.B. die Telefonnummer etc.) und welche nicht (z.B. alle steuerrelevanten Daten).
Wie oben geschrieben: Wahrscheinlich werden in den nächsten Monaten weitere Urteile - auch zu diesem Problemkreis- Klarheit bringen. Wir halten Sie weiter topaktuell informiert.

Quellen: Mag. Stephan Novotny (Fachanwalt für Versicherungsrecht und DSGVO, Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche, Der Standard, DER TREND