Rückschau auf ein Jahr mit der DSGVO.

Welche Gründe für Verfahren, welche Urteile gab es und was lernen wir daraus?

Rückblick: Was das neue Datenschutzrecht brachte.
Ausblick: Worauf sollte man achten, was ist noch zu tun?
Seit dem 25.5.2018 gilt die DSGVO. Wir machen nun einen ersten Rückblick auf die **Entscheidungen der Datenschutzbehörde DSB.** Worauf hat die Behörde in den letzten Monaten besonders „reagiert" und worauf sollte man **daher firmenintern besonderes Augenmerk legen?**

Fakt ist, dass die Umsetzung der DSGVO ganz allgemein **eine erhöhte Aufmerksamkeit** für den Datenschutz brachte. Und die **Beschwerden massiv gestiegen** sind, auch weil die Medien regelmäßig berichtet hatten.
Die Salzburger Nachrichten recherchierten, dass etwa eine Verzehnfachung stattgefunden habe. Gab es im **ganzen Jahr 2017 nur 156 Beschwerden,** so informierte die Behörde in Ihrem Datenschutzbericht 2018, dass es im Vorjahr bereits **1036 Beschwerdeverfahren** gegeben hatte (obwohl die DSGVO erst ab 25.5. Wirkung entfaltet hatte).

A) Worüber beschwerten sich die Konsumenten bei der Behörde?
Die Beschwerdeverfahren betrafen vornehmlich die Rechte auf Auskunft, Geheimhaltung, Widerspruch und Löschung. Was dabei zu beachten ist, wie ein Auskunfts- und Löschkonzept aussehen sollte, darüber haben wir bereits im April 2018 informiert (zum Nachlesen hier klicken…)

Häufige Frage dazu: **Müssen Sie immer die Daten löschen, nur weil ein Löschbegehren gestellt wird?** Nein, natürlich nicht. Aber es kommt darauf an, könnte die Antwort eines Juristen sein.

Grundsätzlich hat natürlich aufgrund der DSGVO **jede(r) das Recht** zu erfahren, welche Daten gespeichert wurden, und darf auch ein Löschbegehren stellen.
Ob Sie als Unternehmer jedoch die Daten wirklich löschen müssen, hängt davon ab, aus welchem Grund Sie die Daten gespeichert hatten.

- Hat sich jemand bei Ihnen für einen **kostenlosen Newsletter angemeldet**, kann er sich jederzeit davon wieder abmelden und kann die Löschung dieser Daten auch verlangen.

- Anderes Beispiel: Jemand hat sich eine kostenlose **App heruntergeladen** und in den AGBs (allgemeinen Geschäftsbedingungen) akzeptiert, dass das Unternehmen die Daten speichert. Dann haben Sie als Unternehmer ganz legal diese Daten gespeichert. Auch diese **Zustimmung kann wieder zurückgenommen** werden – und zwar jederzeit und kostenlos - und daher müssen Sie diese Daten löschen.

  Dazu die Leiterin der DSB **Mag.a Jelinek** in den Salzburger Nachrichten: *„Firmen müssen festlegen, wie lange welche Datensätze gespeichert werden. Daten sind unverzüglich zu löschen, wenn die Verarbeitung z.B. nicht mehr zweckmäßig oder gar unrechtmäßig ist, der Betroffene seine Zustimmung widerruft oder der Verarbeitung widerspricht."*

- Ganz anders sieht die Situation jedoch aus, **wenn eine Geschäftsbeziehung** eingegangen wurde. Der Kunde hat bei Ihnen etwas gekauft, gemietet, eine Leistung erhalten usw.
  Wenn in so einem Fall der Kunde die Löschung seiner Daten verlangt, können Sie ihm antworten, dass dies nicht (komplett) möglich ist, weil Sie etwa die Rechnungsdaten aufgrund steuerrechtlicher Vorgaben **mindestens 7 Jahre aufbewahren müssen.**
  Über ein **wichtiges Urteil zur Aufbewahrung von Daten** haben wir bereits im Dezember 2018 informiert. (zum Nachlesen hier klicken…)

Eine neue Entscheidung der DSB zur Behaltedauer bzw. Löschfrist gab es in den letzten Monaten. Eine **wichtige Klarstellung** zum Thema Datenspeicherung **von (Stellen-)Bewerbern:**

Konkret verlangte ein Bewerber nach einer erfolglosen Bewerbung von der betreffenden Firma die vollständige Löschung seiner personenbezogenen Daten. Die **Firma lehnte das ab und bekam von der Behörde Recht. Warum?**
Das **Gleichbehandlungsgesetz** sieht vor, dass sich Bewerber binnen 6 Monaten über eine erlittene Diskriminierung beschweren und Schadenersatz verlangen können. Um sich gegen einen solchen Vorwurf wehren zu können, brachte das Unternehmen vor, dass es die entsprechenden Unterlagen 6 Monate aufbewahren muss. Dieser Argumentation folgte die DSB **und wies die Beschwerde des Bewerbers ab.** Somit ist klargestellt, dass Bewerbungsunterlagen 6 Monate aufbewahrt werden dürfen.

Sie sehen also: **Eine „Zustimmung" ist die schwächste Basis für die Datenspeicherung,** weil sie jederzeit zurückgenommen werden kann. Sie sollten daher andere Gründe haben, um rechtssicher Daten speichern zu können.

B) Wie hat die Datenschutzbehörde bisher agiert? Häufigste Verfahrensgründe?

Grundsätzlich gilt in Österreich das – unter Juristen nicht unumstrittene – **Prinzip „Verwarnen statt strafen".** Das ist deshalb umstritten, weil renommierte Juristen darin eine Aufweichung der strengen Regelungen der DSGVO sehen und Österreich die DSGVO nicht EU-konform umsetzen würde.

2018 hat die Datenschutzbehörde in Wien nach Recherche der Salzburger Nachrichten **50 Verwaltungsverfahren** wegen Verletzungen der DSGVO eingeleitet.
Darin ging es hauptsächlich um **Bildverarbeitungen bzw. Videoüberwachungen**, die möglicherweise nicht den gesetzlichen Vorgaben entsprachen.

Was können wir daraus lernen? Bei einer Videoüberwachung ist zu beachten, dass diese grundsätzlich nicht den öffentlichen Raum oder Nachbargrundstücke erfassen darf und **deutlich gekennzeichnet** sein muss.
Die Mehrheit der bisherigen Verfahren vor der DSB betrafen diesen Themenkreis und führten zu Strafen von bis **zu EUR 5.300**. Heuer gab es auch schon eine **Strafe über EUR 10.000**. Das bewegt sich allerdings im europäischen Vergleich immer noch in „bescheidenem Rahmen".

Viele Fachjuristen erwarten aber bald ein **härteres Vorgehen der DSB und zwar im Verfahren gegen die Österreichische Post.** Zur Erinnerung: Die Post hat – wohl ohne Zustimmung der meisten Kunden – personenbezogene Daten mit angenommenen Eigenschaften wie politische Einstellung, Kaufverhalten, etc. angereichert und an politische Parteien, Firmen etc. verkauft. Da aber die **„politische Einstellung" zu den sensiblen Daten gehört**, die man nur mit **ausdrücklicher Zustimmung der Betroffenen speichern** darf, leitete die DSB ein **amtswegiges Prüfverfahren** ein. Mit dem Ergebnis, dass die Daten von der Post gelöscht werden müssen. Ausnahmen gäbe es nur dann, wenn tatsächlich eine Einwilligung der Kunden zur Verarbeitung vorliege.

Darüber hinaus stellte die Datenschutzbehörde weiters fest, dass die Datenschutz-Folgenabschätzung für diese Datenverarbeitung und der Eintrag in das interne **Verzeichnis der Verarbeitungstätigkeiten** mangelhaft seien.
Daher ordnete die Behörde an, die **Datenschutz-Folgenabschätzung zu wiederholen** und den Eintrag richtigzustellen.

Was können wir aus obigem Post-Fall lernen?
Die Datenschutzbehörde hat sich bei der Prüfung das Verfahrensverzeichnis näher angesehen und dort Fehler festgestellt. Und angeordnet, dass die Datenschutz-Folgenabschätzung zu wiederholen sei.

Wir haben über das **Verfahrensverzeichnis und Vorschläge, wie man es ausfüllen sollte,** bereits im Feber 2018 berichtet. Zum Nachlesen hier klicken…

Mit großer Wahrscheinlichkeit hat jeder vor dem 25.5.2018, also dem Inkrafttreten der DSGVO, sein Verfahrensverzeichnis erstellt.

C) Checken Sie: Stimmt Ihr Verfahrensverzeichnis noch?
Mehr als ein Jahr später wäre also ein in guter Zeitpunkt, sich das eigene Verfahrensverzeichnis neuerlich näher anzusehen.

- **Stimmen noch alle Daten** in diesem Formular oder haben sich Ansprechpartner, Adresse etc. geändert?
- Haben Sie **neue Datenverarbeitungen** eingeführt (etwa weil Sie nun einen Newsletter anbieten, bei dem personenbezogene Daten gespeichert werden)?
  In diesem Fall müssen Sie eine „neue Rubrik" dafür in Ihrem Verfahrensverzeichnis erstellen und mit allen relevanten Daten befüllen.
- Nutzen Sie **neue Dienstleister** (etwa weil Sie nun Ihren Newsletter über einen Online-Anbieter und dessen Server versenden oder eine Druckerei für Mailings einsetzen usw.). Falls ja, müssen Sie mit diesen Auftragsverarbeiter-Verträge abschließen und dies auch im Verfahrensverzeichnis dokumentieren.
- Haben sich Ihre **TOMs geändert** (etwa, weil Sie eine Sicherheitstüre eingebaut haben, neue Sicherheits-Elemente bei Hard- und Software eingeführt haben usw.)
  Auch in diesem Fall müssen Sie Ihr Verfahrensverzeichnis aktualisieren.

Der **zweite Kritikpunkt der Datenschutzbehörde** im Verfahren gegen die Post betraf die **Datenschutz-Folgenabschätzung.**
Auch diese findet sich im Verfahrensverzeichnis. Nämlich, ob Sie eine durchführen müssen oder nicht. **Was man darunter versteht und wann man eine solche Folgenabschätzung durchführen muss,** haben wir bereits im Dezember 2017 beschrieben. Zum Nachlesen hier klicken…

Rest-Europa legt die DSGVO wesentlich strenger aus: Krankenhaus zu EUR 400.000, Google zu EUR 50 Mio. verurteilt. Was können wir daraus lernen?

Während die Datenschutzbehörde **DSB in Österreich** bis dato nur Strafen in der Höhe von einigen Tausend Euro verhängte, erreichten die Strafen europaweit ganz andere Größenordnungen. Bekanntlich gilt die DSGVO europaweit.

Aufsehenerregend war z.B. eine enorme Strafe, die die Datenschutzbehörde über ein **Spital in Portugal** verhängt hatte. Die Firma musste beachtliche **EUR 400.000** bezahlen und die Strafe war nur deshalb „so" gering, weil man sich kooperativ gegenüber der Behörde zeigte und aktiv an der Behebung des Mangels gearbeitet wurde. Und diese Strafe musste tatsächlich bezahlt werden.

Die aktuell bekannte DSGVO-Höchststrafe – EUR 50 Mio. - sprach die französische Behörde gegenüber Google aus. Der Grund für die Bestrafung war, dass es **für Nutzer sehr kompliziert sei herauszufinden,** was Google über sie speichere, wofür und wie lange. Das Urteil ist allerdings noch nicht rechtskräftig, es wurde dagegen Einspruch erhoben und das Verfahren wird sicher einige Jahre dauern.

Die Salzburger Nachrichten (SN) berichteten, dass es auch immer wieder Beschwerden gäbe, dass die **großen Datenkraken** wie Google, Amazon, Facebook & Co **auf Anfragen der Kunden nicht reagieren** würden. Die SN machten daher den Selbstversuch und stellten fest: Es wird vorerst einmal gar nicht geantwortet. Das sei dort „leider die Normalität", die machen sich in der Regel nicht die Mühe, zu reagieren", wird Medienanwalt Stephan Kliemstein zitiert.

Die **Leiterin der Österreichischen Datenschutzbehörde, Mag.a Andrea Jelinek**, verweist aber darauf, dass sich Betroffene jederzeit beschweren können, und zwar bei der Datenschutzbehörde in Wien. „Die Behörde prüft jede Beschwerde und steigt dann - in der gebotenen Sachlichkeit - dem Säumigen auf die Zehen. Wobei auch Strafen verhängt werden können."

D) Was können wir aus dem obigen Urteil bzw. beschriebenen Problemen lernen?

a) **Keinesfalls** sollte man Auskunfts- bzw. Löschbegehren **ignorieren,** weil andernfalls eine Beschwerde bei der Datenschutzbehörde droht und diese dann das Nicht-Reagieren zum Anlass nimmt, eine Prüfung bei Ihnen durchzuführen.

b) Erarbeiten Sie ein **„Auskunfts- und Löschkonzept"** und **halten Sie sich daran.**
Wir haben schon im Vorjahr in der Vorbereitung auf die DSGVO auf die Wichtigkeit des **„Auskunfts- & Löschkonzeptes" verwiesen.**

Denn die Anfragen von Kunden (aber auch Nicht-Kunden) werden zunehmen. 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 Auskunft verlangt**, welche Daten von ihm gespeichert sind, diese korrigieren oder sogar löschen lassen möchte.

Weder dürfen solche Anfragen ignoriert werden, noch dürfen Daten in vorauseilendem 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.**

Obwohl wir uns erst **im nächsten Newsletter mit den schwierigen Themen IT-Sicherheit und TOMs beschäftigen** werden, auf die die Behörde ganz großen Wert legt, **schon heute einen wichtigen Tipp dazu, da er womöglich etwas Vorbereitungszeit benötigt:**

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 (mit-)schuld sind am Datenverlust, wegen des dann unsicher gewordenen Betriebs-Systems.

Quellen: Homepage der Datenschutzbehörde, DER STANDARD, Salzburger Nachrichten

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