Datenschutz-Folgenabschätzung

Ihr Einstieg in die Datenschutz-Grundverordnung (DSGVo).

Im vorigen BAV-Newsletter haben wir eine grobe Zusammenfassung gegeben, was alles unter den Problemkreis Datenschutz-Grundverordnung fällt. Hier zum Nachlesen… . Heute möchten wir Ihnen weitere Informationen dazu übermitteln.

Bitte beachten Sie, dass wir hier **keine allgemein gültigen Empfehlungen** geben können. Einerseits ist bei einer Reihe von wichtigen Fragen noch nicht klar, wie das von der österreichischen Aufsicht (Datenschutzbehörde) gesehen werden wird. Auch die Frage, wie umfassend kontrolliert werden wird, lässt sich noch nicht vorhersagen. Immerhin hat Österreich laut heutiger Anfrage bei der WKO 535.612 Unternehmen, in denen es die Umsetzung zu kontrollieren gilt.

Vorhersehbar ist aber, dass die **Finanz- und Versicherungsbranche besonders stark** im „Visier der Aufsichtsbehörden" sein wird, weil diese Branchen über viele **sensible Daten** von Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeiter verfügen (Einkommens-, Steuer-, Gesundheitsdaten).

Daher: Nicht auf die leichte Schulter nehmen und nicht einfach zuwarten: Die **Strafandrohungen** sind für viele existenzbedrohend: Bis zu EUR 20 Mio. oder 4 % des Konzernumsatzes können als Strafe verhängt werden.

Wir setzen daher unsere **Serie zur DSGVo** fort und versuchen, **ein paar Fragen,** die sich bei näherer Betrachtung des Themas stellen, grob zu beantworten, um weiteres Problembewusstsein für das Thema zu schaffen und eventuell Hilfe bei der Umsetzung zu bieten.

Wer ist von DSGVo betroffen?
Jedes Unternehmen, egal ob groß oder klein, sobald **personenbezogene Daten** (elektronisch) verarbeitet werden. Wichtig: Unter **„Verarbeiten" versteht der Gesetzgeber laut Mag. Kainz** nicht nur das Auswerten und Analysieren („Profiling"), sondern es reicht schon, **wenn man die Daten einfach nur speichert.**

Georg Markus Kainz, führender Datenschützer Österreichs, meinte kürzlich, dass „die wahrscheinlich **wichtigste Änderung der neuen DSGVo-Regelung**" darin besteht, dass man künftig „die Verantwortung für die Einschätzung und Bewertung des eigenen Datenbestandes selbst zu tragen habe. Er meinte damit **all jene Daten, die von Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeiter** im Rahmen der eigenen Geschäftstätigkeit entstehen, und deren Verarbeitung.

Bis dato musste man seine „Datenanwendungen" der Datenschutzbehörde melden. Diese **Meldepflicht** und die verpflichtende Eintragung ins Datenverarbeitungsregister fallen weg.
Diese „Erleichterung" führt aber dazu, dass Sie (und Ihre genutzten) Dienstleister zukünftig die **alleinige Verantwortung** für die Daten haben. Daher ist ein **wichtiger Aspekt** der DSGVo die sichere Aufbewahrung der Daten. Wir haben in den letzten BAV-Newslettern mehrmals **„Sicherheits-Tipps" für Software und Hardware** geliefert, die helfen sollen, Hacker-Angriffe und damit verbundene Datendiebstähle zu vermeiden. Etwa:

„WannaCry": Existenzbedrohende Millionenstrafen bei Datendiebstahl! Teil 1 finden Sie hier …, Teil 2 hier … Oder: Praxistipps: Wie vor Datenverlust schützen? Zum Nachlesen hier klicken…

Risikoabschätzung, wie geht das?
Sie müssen künftig „die sachliche Anwendbarkeit und das mit der Verarbeitung der Daten verbundene Risiko" eigenständig einschätzen. Und die daraus abgeleiteten Entscheidungen und ergriffenen Maßnahmen dokumentieren.

Viele erinnert diese Vorgehensweise an die ISO 9001-Zertifizierungen, die vor etwa 15 Jahren in aller Munde waren. Damit möchte man das Qualitätsmanagement in Unternehmen steigern, indem man sich alle Vorgänge eines Unternehmens genau ansieht und diese dokumentiert. Kritiker meinten damals, dass nur durch das bloße Aufschreiben der Vorgänge noch keine Qualitäts-verbesserung passieren würde.

Aber sie übersahen, dass durch das vorherige Betrachten der Vorgänge und Überlegen („Ist das gut so, gehört das so, sollte man das nicht ändern?) Fehler gefunden und dadurch die Qualität gesteigert werden konnte. Und ähnlich ist es nun mit der DSGVo.

Daher sollte Ihr Einstieg in die DSGVo mit der **Datenschutz-Folgenabschätzung** beginnen. Darin beschreiben Sie **Ihre Verarbeitungsvorgänge**, deren Notwendigkeit, die Verhältnismäßigkeit, damit verbundene Risiken und geplante Abhilfemaßnahmen, so Mag. Kainz.

Das Ziel ist also die **„systematische Vorab-Bewertung der Risiken",** die Ihre Daten-Verarbeitung mit sich bringt, und das Festlegen und Dokumentieren, welche Strategien Sie verfolgen, um diese Risiken zu verhindern oder zu minimieren.

Die WKO hat dazu eine Checkliste „Ablaufplan zur Datenschutz-Folgenabschätzung" erstellt und darin wichtige Fragen aufgeworfen, die Sie sich stellen sollten**. Die Checkliste können Sie hier als PDF herunterladen …**

Darin finden sich einige wichtige Begriffe, die Mag. Kainz wie folgt erläutert:

„Personenbezogen sind Daten, die sich auf eine bestimmte oder bestimmbare, natürliche Person beziehen. Ob eine Person aufgrund der Daten bestimmbar ist, muss objektiv beurteilt werden, sodass nicht nur auf die rechtlichen und tatsächlichen Möglichkeiten des Verantwortlichen, sondern auf die Möglichkeiten Dritter abzustellen ist."

Mag. Kainz bezieht sich hier auf die Gefahr, die sich durch das **konsequente Daten-Sammeln („Big Data")** und die modernen technischen Möglichkeiten ergibt. Je mehr Daten gesammelt werden, umso leichter fällt es, einen Personenbezug herzustellen. Ein Beispiel zum besseren Verständnis: Bei einem **„Experiment"** gelang es – mit lediglich geringen technischen Fähigkeiten und Mitteln - aus hunderten Millionen anonymisierter Telefondaten Großbritanniens die Nummer und damit Aufenthaltsort und Aktivitäten eines Einzelnen herauszufinden. Also einen „Personenbezug" herzustellen. Stellen Sie sich also die – berechtigte – Aufregung vor, wenn etwa aus anonymisierten Kundendaten eines Versicherers (die gehackt und gestohlen wurden) herausgefunden würde, dass Herr XY an einer bestimmten Erkrankung leidet …

Bei den personenbezogenen Daten **ist zwischen „sensiblen Daten" und den „restlichen Daten" zu unterscheiden**. Die sensiblen Daten sind eine Untergruppe der personenbezogenen Daten, die ganz besondere Konsequenzen bei der Risikoanalyse und der Verarbeitung verlangen.

Die **normalen personenbezogenen Daten** verwenden wir regelmäßig bei unserer Arbeit. Dazu gehören zum Beispiel Name, Adresse, Geburtsdatum, Bank- oder Kommunikationsdaten, wie die Telefonnummer und die E-Mail-Adresse. Hier ist schon ein ordentliches Maß an **Schutz zu gewährleisten,** damit diese Daten nicht in fremde Hände fallen, und Hacker keinesfalls auf Shopping-Tour gehen oder sonstigen Missbrauch begehen können.

Die **sensiblen Daten** sind eine **besondere Kategorie** unter den personenbezogenen Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hergeleitet werden können.

Auch die **genetischen Daten, alle biometrischen Daten**, die zur eindeutigen Identifizierung einer natürlichen Person verwendet werden können, aber auch die **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung zählen zu den sensiblen Daten. Also fallen zum Beispiel die Bilder für die Gesichts-Erkennung, der Fingerabdruck oder Iris-Scan genauso unter die sensiblen Daten wie auch die Krankengeschichte.

Fallen „solche Daten" bei Ihrer Tätigkeit an, dann müssen Sie sich in einem zweiten Schritt weitere Fragen stellen. Etwa:

- Wann und wie lange darf ich diese Daten speichern, verarbeiten? An wen darf ich sie weitergeben und unter welchen Bedingungen? Dazu müssen Sie ein **Verarbeitungstätigkeiten-Verzeichnis** erstellen.
- Wie schaut eine rechtswirksame **Einwilligungserklärung** aus? Muss ich für Daten, die ich in der Vergangenheit gesammelt habe, neuerlich eine Einwilligung einholen? Oder nur für neue Daten?
- Brauche ich einen **Datenschutzverantwortlichen?**

- Werden die datenschutzrechtlichen **Prinzipien** eingehalten?
- **Was tun, wenn Daten – etwa durch Hacker-Angriff – verloren gingen?**

Mit diesen Fragen beschäftigen wir uns in den nächsten BAV-Newslettern im Frühjahr 2018!

Zusammenfassung: Das Wesentlichste von Schritt 1:

- **Betroffen von der DSGVo ist jede (elektronische) Verarbeitung von personenbezogenen Daten.**
- **Unter „Verarbeiten"** versteht der Gesetzgeber nicht nur das Auswerten und Analysieren, sondern bereits das bloße **Speichern der Daten.**
- **Datenschutz-Folgenabschätzung:** Darin analysieren Sie, wo welche Daten anfallen. Klären vorab Risiken, die sich aus Ihrer Datenverarbeitung ergeben können und welche Strategien Sie verfolgen, um diese Risiken zu minimieren bzw. zu verhindern. Das alles müssen Sie dokumentieren.

Quellen: B2B-Projekte Mag. Günter Wagner, Praxishandbuch „Das österreichische Versicherungsvermittlerrecht", Kommentare von Rechtsanwalt Mag. Stephan Novotny und Datenschutz-Experte Mag. Georg Markus Kainz, Checkliste der WKO zur DSGVo