Datenschutz-Grundverordnung

Die große Herausforderung für Finanz- und Versicherungsunternehmen sowie selbstständige Berater und Vermittler.
Eine Einführung.

Seit dem 24. Mai 2016 gilt die **Datenschutz-Grundverordnung**, allerdings mit einer zweijährigen Übergangsfrist. Mit dieser Verordnung werden die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen geregelt und **auf ein EU-weites Mindestniveau gebracht**.

Wer oder was ist betroffen?
„Wer" ist leicht erklärt. Jedes Unternehmen, egal ob klein oder groß, egal in welcher Branche tätig, das **personenbezogene Daten von EU-Bürgerinnen und Bürgern verarbeitet**. Allerdings stehen wohl die **Finanz- und Versicherungsbranchen unter besonderer „Aufsicht"**, da hier **sehr viele sensible Daten** (Finanz-, Bank-, Gesundheitsdaten etc.) vorliegen.

Das „was" ist viel schwieriger, da sehr umfangreich:
Viele denken bei DatenSCHUTZ, dass es um DatenSICHERHEIT gehe, also etwa dem (besseren) Schutz vor Datendiebstahl durch Hacker. Doch das ist nur ein kleiner (wenn auch sehr heikler) Bereich, um den Sie sich „dank" Datenschutz-Grundverordnung kümmern müssen.

Wer denkt schon an die Datenschutz-Grundverordnung, wenn er sein altes Faxgerät, seinen alten Kopierer oder Drucker entsorgt? Ist Ihnen bewusst, dass auf den darin verbauten Speichermedien unzählige Gigabyte an sensiblen Daten vorhanden sind, wie medizinische Befunde, Testamente, Passkopien, Anträge für Versicherungen, Passwörter oder Ähnliches?

Haben Sie von allen Datensätzen, die Sie besitzen, die **ausdrückliche Zustimmung**, dass Sie sie speichern dürfen? Wo dürfen Sie sie speichern (ist die Cloud sicher?) und wie lange? An wen unter welchen Bedingungen weitergeben?

Wie lösen Sie den „**Interessenskonflikt**" zwischen dem **Recht auf Vergessen** (einer Kundin/eines Kundens) und Ihrem berechtigten Wunsch, Unterlagen aufzuheben, um dann Jahre später in einem **Prozess beweisen zu können**, dass Sie die Beratung rechtskonform durchgeführt haben? Also die behauptete Fehlberatung nicht passiert ist?

Brauchen Sie einen Datenschutzverantwortlichen? Wie erfüllen Sie die Informations-, Dokumentations- und Schulungspflichten?

Was genau sind **personenbezogene bzw. sensible Daten** und wie ist damit umzugehen?

Diese Fragen sind nur die Spitze des Eisbergs und sollen ein wenig skizzieren, was alles unter Datenschutz zu verstehen ist und künftig durch die Datenschutz-Grundverordnung schärfer geregelt sein wird.

Da die nationalen Gesetzgeber auf sogenannte **Öffnungsklauseln** bestanden, ist noch nicht in allen Details klar, wie diese EU-Verordnung im österreichischen Datenschutzgesetz umgesetzt werden wird.

Sehr wohl klar ist jedoch:

- Die EU Datenschutz-Grundverordnung ist spätestens **ab 25. Mai 2018 anzuwenden**.
- **Gravierende Änderungen**: Es kommt zu Verschärfungen im Bereich des Datenschutzes und der Datensicherheit (verpflichtende angemessene Sicherheitsvorkehrungen, verpflichtende Meldung von Datenmissbräuchen und Sicherheitsverletzungen an die Aufsichtsbehörden, z.B. Datendiebstahl nach Hacker-Angriffen).
- **Stärkung der Rechte der Betroffenen** (u.a. unsere Kundinnen und Kunden und Mitarbeiterinnen und Mitarbeiter etc.) und strengere Vorgaben zur Datensicherheit. Recht auf Auskunft, Recht auf Vergessenwerden, Einwilligung gilt nur, wenn freiwillig, aktiv und eindeutig. Dazu kommt die Pflicht zur Berichtigung, Löschung und zur Einschränkung der Verarbeitung.
- **Strafen in Millionenhöhe**: Strafen bis zu 20 Millionen Euro bzw. 4 Prozent des Konzernumsatzes können verhängt werden.

- **Erhöhte Selbstverantwortung**: Künftig müssen Sie Ihre Datenanwendungen nicht mehr vorab von einer Datenschutz-Behörde prüfen und genehmigen lassen (keine DVR-Nummer mehr). Wenn aber etwas passiert (etwa durch Hacker-Angriff wurden Ihnen Kundendaten gestohlen), müssen Sie beweisen, dass Sie alles Denkmögliche getan haben, um das zu verhindern.

- Datenschutz wird eine **Compliance-Aufgabe**, mit der sich alle Abteilungen intensiv beschäftigen müssen. Besonders wohl die Rechts-, Organisations-, Prozess- und IT-Abteilungen.

- **Datenschutz-Folgenabschätzung, Verfahrensverzeichnis:**
  Dieser Punkt wird von Experten als die wichtigste Änderung eingestuft. Durch den Wegfall der Meldepflicht bei der Datenschutzbehörde liegt zukünftig die alleinige Verantwortung beim Auftraggeber und seinen Dienstleistern. Im Verfahrensverzeichnis beschreiben Sie Ihre Verarbeitungsvorgänge. In der Datenschutz-Folgenabschätzung beurteilen Sie die Notwendigkeit der Verarbeitungsvorgänge, deren Verhältnismäßigkeit, die damit verbundenen Risiken und geplante Abhilfe-Maßnahmen. Dieses Verzeichnis kann in elektronischer oder schriftlicher Form geführt werden und ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

- **Neue Dokumentationspflichten**, etwa das Führen eines Verzeichnisses von Verarbeitungstätigkeiten, Prüfpflichten für Verantwortliche.

- **Betriebliche Datenschutzbeauftragte** verpflichtend für große Unternehmen und jene, deren Kerngeschäft in der Verarbeitung personenbezogener Daten liegt.

- **Erfassungskette von Daten**: Was ist zu beachten, wenn Sie Daten weitergeben? Wie stellen Sie sicher, dass der Partner die Daten auch wieder verlässlich löscht?

  Wenn Sie Daten zur **Verarbeitung außer Haus geben** und diese von externen Dienstleistern erledigen lassen, so ist mit diesen Dienstleistern ein **schriftlicher Vertrag** mit zwingenden Mindestinhalten abzuschließen und die Einhaltung dieser Verpflichtungen vom Auftraggeber regelmäßig zu überwachen.

  ACHTUNG: **Unter „Verarbeiten" meint das Gesetz** nicht nur das Auswerten und Analysieren, sondern auch das bloße Speichern!

- **Nötige Anpassungen**: Verträge, allgemeine Geschäftsbedingungen und Websites müssen angepasst werden. Formulare, egal ob analog oder digital, müssen auf ihre Datenschutzhinweise, Belehrungen und Widerrufs-Möglichkeiten hin überprüft werden. In allgemein verständlicher Sprache (nicht in Juristen-Deutsch) ist dort zu erklären, welche Daten gespeichert werden, wie diese verarbeitet werden und an wen diese weitergegeben werden.

Zum Abschluss der Einführung in die Datenschutz-Grundverordnung **zwei Aspekte**, die besonders für die Finanz- und Versicherungsbranche typisch sind:

a) Besondere Risiken der Datenschutz-Grundverordnung (DSGVO) für die Finanz- und Versicherungsbranche

Dazu RA Mag. Stephan Novotny: „Die Finanz- und Versicherungsbranchen sind deswegen intensiv von der DSGVO betroffen, weil sie über eine **Vielzahl an sensiblen Daten** verfügen und andererseits die Aufsichtsbehörden ein strenges Auge auf diese Unternehmen werfen. Im Bereich der Personenversicherung verfügen Versicherungsunternehmen, aber auch Versicherungsvermittler wie Makler und Agenten über **Gesundheitsdaten**, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen, und aus denen Informationen über den Gesundheitszustand einer Person hervorgehen. In diesem Bereich ist daher von jedem Kunden, der beispielsweise vor Abschluss seines Versicherungsvertrages Gesundheitsfragen ausfüllt, eine **ausdrückliche Einwilligungserklärung einzuholen**. Besondere Einwilligungserklärungen sind auch für Kinder, die ebenfalls häufig zu Versicherungsnehmern zählen, vorgesehen. Betroffen sind aber naturgemäß auch alle Unternehmen, die ebenfalls Versicherungen vermitteln dürfen, wie Autohäuser (Kfz-Versicherungen), Banken, Reisebüros (Reiseversicherungen), Optiker (Brillenversicherung), der Elektronik(fach)handel (z.B. Handyversicherungen) etc."

b) Wer haftet in der Erfassungskette von Daten im Bereich der Finanz- und Versicherungswirtschaft?

Dazu RA Mag. Stephan Novotny: „Insbesondere im Bereich der Versicherungswirtschaft, aber auch im Bereich der Finanzdienstleistungsunternehmen, werden **Kundendaten vom Vermittler erfasst** und in der Folge an das Versicherungs- oder Wertpapierdienstleistungsunternehmen weitergegeben oder in dessen System eingespielt.

Dies betrifft insbesondere Versicherungsmakler. Hier **haften Makler** (vertraglich und deliktisch) **und Agent** (deliktisch) der Kundin/dem Kunden gegenüber für die weitere Verwendung der Kundendaten bei den Versicherungsunternehmen. Der Versicherungsmakler wird daher in seine Verträge mit den Versicherungsunternehmen ebenso wie die Versicherungsagenten in ihre Agenturverträge entsprechende Vertragsbestimmungen zur Absicherung, Übernahme der Haftung, Schad- und Klagloshaltung mit den Versicherungsunternehmen aufzunehmen haben.

Grundsätzlich reicht die **Erfassungskette lückenlos vom Ersterfasser** bis hin zum Letztanwender der Daten. Erstanwender sind dabei all jene, die die Daten vom Kunden erhalten: Versicherungsmakler, Versicherungsagenten, angestellter Außendienst, Vermögensberater, Banken etc. Bereits hier beginnt die Datenschutz-Grundverordnung zu greifen.

Da die Daten vom Vertrieb zur Versicherung zum Finanzdienstleister und umgekehrt hin und her gespielt werden bzw. von jedem abgerufen werden müssen, sind alle Datenanwender gleichermaßen betroffen. Es gibt keine Aufgabenteilung bzw. Arbeitsverteilung im Hinblick auf Datenschutz, allenfalls Zugriffsbeschränkungen für Einzelne in der Kette.

Unser Tipp: **Unternehmen können nicht früh genug** mit den erforderlichen Anpassungsmaßnahmen beginnen, um rechtzeitig bis 25. Mai 2018 für Big Data, Cloud Computing und (internationalen) Datenverkehr gewappnet zu sein und alle erforderlichen **Prozessschritte im Unternehmen implementiert** zu haben.

Für Experten gilt „die Vereinbarkeit zwischen fortschreitender Digitalisierung und massiv verstärktem Datenschutz hinsichtlich elektronischer Daten, die im Rahmen dieser Digitalisierung notwendigerweise vermehrt zu verwerten und zur verarbeiten sind, als **größte Herausforderung**.

Ihr Interesse vorausgesetzt, werden wir in den nächsten BAV-Newslettern einzelne Arbeitsschritte im Detail beschreiben, um Sie auf die Datenschutz-Grundverordnung vorzubereiten.

Quellen: B2B-Projekte Mag. Günter Wagner, Praxishandbuch „Das österreichische Versicherungsvermittlerrecht“, Kommentare von RA Mag. Stephan Novotny und Datenschutz-Experte Mag. Georg Markus Kainz