DR. ROLAND WEINRAUCH

Vortrag „Die Datenschutzgrundverordnung aus Sicht des Versicherungsmaklers“

Die Idee ist, das 8-Punkte-Programm der DSGVO, das Frau Mag. Illibauer Ihnen bereits vorgestellt hat, nochmals aus dem Blickwinkel eines Versicherungsmaklers durchzugehen.

Man muss vielleicht voranstellen, dass wir es hier mit einer europäischen Regulierung zu tun haben, die unmittelbar auf Österreich wirkt, aber letztlich ist es europäisches Recht. Das bedeutet zum einen, dass gesetzliche Bestimmungen oft mit Gesetzesbegriffen übersetzt worden sind, die in der deutschen Sprache neu sind und uns als solche unbekannt und letztlich in der Verwaltungspraxis erst ihre Auslegung finden müssen. Dh. wir sind in einer Situation, wo man diese zum Teil unbestimmten Begriffe erst mit Inhalten befüllen muss. Zum anderen ist es ein Paradigmenwechsel. Der typische Österreicher bevorzugt es, sich sagen zu lassen, was er genau tun soll und ist sozusagen sehr „behördentauglich“. Das Ganze wird jetzt aber durch die Verordnung umgedreht und wir müssen nun selbst bestimmen was wir im regulativen Rahmen zu tun haben.

Warum sind wir nun hier?

Wenn wir ehrlich sind, bringt die DSGVO bzw. ein Großteil davon grundsätzlich nichts Neues (wenn auch in anderer Ausprägung), aber die Maximalstrafen - bis zu 20 Millionen Euro bzw. 4 % des Jahresumsatzes – führen dazu, dass wir uns nun ernsthaft mit dem Thema auseinandersetzen müssen.

Gilt die Verordnung für jeden Versicherungsmakler, unabhängig von seiner Rechtsform, unabhängig von seiner Größe?

Die Bestimmungen werden für jeden Versicherungsmakler relevant sein, egal ob Sie keinen Mitarbeiter, 5 Mitarbeiter oder 100 Mitarbeiter haben. Sie sind letztlich genauso betroffen wie eine Bank, eine Versicherung oder Facebook, da die gleichen Regeln für jedes Einzelunternehmen sowie für große Konzerne gelten.

Warum sind wir alle davon betroffen?

Das Arbeiten mit personenbezogenen Daten schafft die Grundlage hierfür. Egal ob Sie mit solchen Daten elektronisch oder in Papierform arbeiten und egal welche Verarbeitungstätigkeit (erheben, speichern, etc.) Sie verrichten, sobald ein gewisses System (Archiv, Computerdateien, Ablagesystem in Ordnern, etc.) dahinter ist, sind Sie in diesem Datenschutzthema drinnen.

Zusammenfassend bedeutet das: es gilt für jeden von Ihnen, weil jeder ganz sicher personenbezogene Daten verarbeiteten wird und es gilt sofort, nämlich ab dem 26. Mai 2018, und es wird hier grundsätzlich auch kein Pardon geben, weil die Behörde sich darauf stützen wird, dass Sie zwei Jahre lang Zeit gehabt haben.

Personenbezogene Daten können alles Mögliche sein, was zur Identifizierbarkeit der Person führt. Ein ganz interessanter rechtlicher Nebenaspekt ergibt sich zudem aus dem Umsetzungsgesetz. Wenn man in Österreich eine Verfassungsbestimmung ändern möchte, braucht man eine Zweitdrittelmehrheit im Parlament. Nachdem hier einige Verfassungsbestimmungen in der bisherigen Datenschutzgesetzgebung enthalten waren und man sich politisch nicht einigen konnte, ist einiges im Gesetz übrig geblieben. Vor allem ist das Grundrecht übrig geblieben, dass als Jedermannsrecht ausgestaltet ist und sich daher die Frage ergibt, ob jetzt nur personenbezogene Daten von natürlichen Personen betroffen sind, was Verordnungsinhalt ist und wovon wir alle ausgehen, oder – und das ist durchaus noch etwas unklar – auch personenbezogene Daten von juristischen Personen betroffen sind. Wir gehen davon aus, dass hoffentlich der neue Gesetzgeber noch vor dem 25. Mai 2018 für Klarheit sorgen wird, weil es schon wichtig zu wissen ist, ob ich Unternehmensdaten einer GmbH und Daten einer natürlichen Person gleich behandeln muss. Sie müssen sich überlegen, ob Sie bei der Datenverarbeitung mit personenbezogenen Daten überhaupt eine Unterscheidung treffen möchten.

Wie Sie sehen, ist sogar in der gesetzlichen Umsetzung und auch in einigen anderen Punkten, wo uns die Behörde noch Antworten schuldet, vieles im Moment noch eher unklar.

Klar ist aber die neue Rechtsdefinition des Verantwortlichen, den primären Adressaten der Bestimmungen. Das kann eine natürliche oder juristische Person

sein, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verantwortlicher - wie kann man sich das vorstellen?

Der primäre Adressat aus Sicht der Verordnung ist das Unternehmen als solches, dh. Sie als Unternehmer egal in welcher Rechtsform. Sie sind der Adressat und somit der Verantwortliche, der letztendlich dafür Sorge tragen muss, dass diese Regelungen eingehalten werden.

Wer wird gestraft werden - das Unternehmen oder der Geschäftsführer?

Der eine oder andere wird Geschäftsführer einer GmbH sein und vielleicht sogar noch Fremdgeschäftsführer (nicht die eigenen Anteile verwaltend) und hier müsste man sich überlegen, wer hier Strafadressat sein soll. Meiner Meinung nach ist es so, dass sowohl das Unternehmen als auch der Geschäftsführer Strafadressat sein kann. Nachdem die Umsetzungsgesetz-gebung in Österreich ein Doppelbestrafungsverbot vorsieht, wird wohl primär das Unternehmen der Strafadressat sein. Aus meiner Sicht ist es aber im Umkehrschluss möglich zu sagen, dass, wenn das Unternehmen nicht bestraft wird, der Geschäftsführer bestraft wird.

Was ist das Unangenehme an den Strafen?

Es sind die Maximalstrafen, die man in absurder Höhe vorgesehen hat. Vielleicht nicht in absurder Höhe im Sinne von Facebook oder Google, aber im Sinne eines Ein-Personen-Unternehmens, eines Versicherungsmaklers. Der Behörde wurde ein hoher Ermessensspielraum eingeräumt und macht diese die Bestrafung anhand eines sehr kurz gehaltenen Kriterienkatalogs fest.

Wie erreichen wir das Ziel NICHT bestraft zu werden?

Die Behörde hat und ich zitiere hier das Umsetzungsgesetz § 22 *„umfassende Rechte erhalten … sich bei Ihnen Dinge anzuschauen“*. Die Datenschutzbehörde kann

- vom Verantwortlichen alle notwendigen Aufklärungen verlangen.
- Einschau in die Datenverarbeitungen halten und diesbzgl. Unterlagen begehren.

- nach Verständigung des Verantwortlichen und des Inhabers der Räumlichkeiten, die Räume in welchen Datenverarbeitungen vorgenommen werden, betreten.
- Datenverarbeitungsanlagen in Betrieb setzen und die zu überprüfendenden Arbeiten durchführen.
- Kopien von Datenträgern, in dem von der Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß, herstellen.

Wenn Sie der Behörde den Zutritt verwehren, kann Sie diese bestrafen.

Was ist unser Problem?

Es gibt unterschiedliche Betroffenenrechte, wie das Recht auf Löschung, das Recht auf Auskunft, das Recht auf Berichtigung etc., mit denen man umgehen muss. Vor dem Hintergrund der Betroffenenrechte werden Sie auch Korrespondenzen mit Betroffenen führen, die Ihnen vielleicht auch nicht wohl gesinnt sein könnten und Sie gegenüber der Datenschutzbehörde anzeigen oder anschwärzen.

Ich glaube nicht, dass die Behörde uns ab morgen flächendeckend überprüft, weil sie das aus budgetären Gründen auch nicht schaffen wird, aber ich mutmaße natürlich nur und gleichzeitig sind wir nicht davor gefeit überprüft zu werden. Es muss daher eine logische Konsequenz sein sich einerseits zu überlegen, was man bei einer Überprüfung seitens der Behörde alles parat haben sollte, damit Sie idealer Weise nicht bestraft sondern nur ermahnt werden. Andererseits sollte man ein System schaffen, dass mit Betroffenenrechten möglichst gut umgehen kann, damit einen möglichst wenig oft die Behörde besuchen kommt.

Vertragserfüllung oder Einwilligung?

Jede Datenverarbeitung ist grundsätzlich unrechtmäßig, wenn nicht irgendein Rechtfertigungsgrund vorliegt. Die zwei wesentlichen Ausnahmen, die für Sie eine Rolle spielen, sind zum einen die Vertragserfüllungsausnahme und zum anderen die Ausnahme rund um die Einwilligung. Sie dürfen Daten verarbeiten, wenn derjenige, dessen Daten hier betroffen sind, dazu seine Einwilligung erteilt.

Sie dürfen aber auch ohne Einwilligung Daten verarbeiten wenn es für die Vertragserfüllung erforderlich ist.

Im Sinne der Rechtskonformitäten-Grenze besteht die Grenze dieser Datenverarbeitung jedoch darin, sich im Rahmen des Vertragserfüllungs-zweckes zu bewegen. Dh. Sie dürfen Daten, die Sie für die Vermittlung des Versicherungsproduktes für sich in die Verarbeitung genommen haben, verarbeiten solange Sie dem Zweck der Vermittlung dieses Produktes dienen. Sie dürfen aber bspw. dem Kunden ohne Einwilligung keinen Newsletter schicken, da der Newsletter nichts mit der Vertragserfüllung zu tun hat. Wo genau sich noch die Grenze der Vertragserfüllung befindet und wohin bzw. wie weit das noch führen kann, wird ein Argumentationsthema sein, dass man auch mit der Behörde durchorganisieren muss. Von der Vermittlerperspektive aus wird man sehr oft, sehr gut in dieser Vertragserfüllung unterwegs sein.

Die zweite Möglichkeit ist die Einwilligung. Was spricht dafür und was dagegen? Sie könnten bspw. ein System hinterlegen, dass automatisch zu Beginn immer eine Einwilligung einholt. Wenn Sie sich nun eine solche Einwilligung eingeholt haben, laufen Sie aber Gefahr, dass Sie den Zweck, wofür Sie diese Daten verwenden wollen, zu eng definieren, da Sie vielleicht noch gar nicht ersehen können wo die Reise hingehen wird. Eine rechtsrichtige Einwilligungserklärung sich einzuholen ist sehr schwierig, weil sehr hart definiert ist, was die Einwilligung alles können muss, damit sie funktioniert.

Meiner Meinung nach spricht sehr vieles gegen eine Einwilligung und insoweit es Ihnen möglich ist, macht eine auf Vertragserfüllung basierte Datenverarbeitung wohl vieles leichter. Außer Sie arbeiten mit sensiblen Daten. Hierzu müssen Sie sich eine Einwilligung holen, da Vertragserfüllung allein als Rechtfertigungsgrund nicht ausreicht.

<u>Was sind sensible Daten?</u>

Sensible Daten sind Daten aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen. Dazu gehören auch genetische und biometrische Daten sowie Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung.

Abgesehen von den Gesundheitsdaten werden unter Umständen auch Daten zur Religionszugehörigkeit für Sie eine Rolle spielen, sofern Sie Mitarbeiter haben, bei denen im Rahmen Lohnverrechnung aufgrund der Feiertags-regelungen das Religionsbekenntnis abgefragt wird. Von diesen Mitarbeitern werden Sie beispielsweise Einwilligungen benötigen sowie auch bei Gesundheitsdaten.

Dh. in einer ersten Prüfung sollten Sie sich in einer Status-Quo-Analyse überlegen, welche Daten Sie verarbeiten und für welche Sie eine Einwilligung brauchen und für welche nicht. Sie müssen eine rechtssichere Einwilligungserklärung als Formblatt haben, dass Sie als Formblatt verwenden, um keine Fehler zu machen und um letztlich auch einen Standard im Unternehmen zu setzen. Auf der Webseite der WKÖ stehen bereits einige Musterformblätter zur Verfügung mit denen man arbeiten kann, um rechtssicher unterwegs zu sein. Letztlich wird man die Verwaltungspraxis abwarten müssen, um zu sehen, welche Arten von Erklärungen von der Behörde als ausreichend rechtskonform anerkannt werden.

Was ist mit Verarbeitungsverzeichnis gemeint?

Die Kernverpflichtung wird die Erstellung eines Verarbeitungsverzeichnisses nach Artikel 30 sein. Das Verzeichnis muss eine Schriftform haben, egal ob elektronisch oder in Papierform. Aus diesem Verzeichnis muss hervorgehen, welche Daten Sie in welcher Form im Unternehmen verarbeiten.

Unter Zuhilfenahme von Mustersheets von EDV-Dienstleistungsunternehmen werden Sie nicht herumkommen sich für Ihr Unternehmen folgende Fragen zu stellen:

- Wer verarbeitet im Unternehmen welche Daten?
- Welche Daten gehen wohin?

Für einen Dritten muss anhand Ihrer Aufstellung nachvollziehbar sein, wie die Datenverarbeitung in Ihrem Unternehmen funktioniert. Wenn man es runterbricht, ist das der Kern des Verzeichnisses und Sie werden bei dieser Aufstellung sehr viele Grundsätze des Datenschutzrechtes wieder finden, da Sie sich - vor allem vor dem Hintergrund des Grundsatzes der Datenminimierung und des Grundsatzes der Datensicherheit – immer wieder überlegen müssen:

- soll wirklich jeder Mitarbeiter über diese Daten verfügen
- wie lange soll der Mitarbeiter über diese Daten verfügen
- wer soll wo und wie welche Daten abspeichern
- wie sicher werden diese Daten abgespeichert etc.

Dh. im Zuge der Verzeichniserstellung werden sich sukzessiv viele Fragen klären. und ob Sie das alleine schaffen oder eine externe Hilfestellung in Anspruch nehmen bleibt Ihnen überlassen. Ich glaube die Kammer gewährt Zuschüsse für Coachings und man kann sich zum Teil auch die Kosten ersetzen lassen. Es kostet viel Zeit sich diesem Thema zu widmen, weil vielen Unternehmen gar wissen welche Abteilung von welcher Abteilung welche Daten erhält und wie das miteinander verschachtelt ist. Aber Erstellung eines solchen Verzeichnisses ist eine Rechtspflicht, um die Sie nicht herumkommen werden.

Warum müssen Sie ein Verarbeitungsverzeichnis machen?

Unabhängig von der Mitarbeiteranzahl sind Sie aufgrund der permanenten Verarbeitung von Daten verpflichtet ein Verarbeitungsverzeichnis zu führen.

Wenn Sie bei einer Überprüfung seitens der Behörde ein solches Verzeichnis nicht vorweisen können, wird es wohl nicht bei einer Ermahnung bleiben, da das Verzeichnis eben eine Kernverpflichtung ist. Man muss sich dem Thema daher auch mit der gebotenen Sorgfalt eines Unternehmers stellen und Sie werden viel Zeit und Kraft investieren müssen, aber über das Verzeichnis wird sich dann auch vieles für Sie klären.

Wann muss ich eine Meldung bei der Behörde machen?

Sie müssen eine Meldung immer dann machen, wenn Sie personenbezogene Daten „verlieren“ oder Gefahr für diese Daten besteht. Je nach Ausmaß müssen Sie nur die Behörde oder auch die Betroffenen verständigen.

Wenn Sie bspw. tausende Kundendaten auf einem Datenstick verlieren, weil bspw. einer Ihrer Mitarbeiter den besagten Stick in der S-Bahn verloren hat, werden Sie als Unternehmer entscheiden müssen, ob Sie die tausenden Betroffenen informieren oder nicht. Wenn Sie sich aber entscheiden keine Meldung zu machen, müssen Sie sich auf jeden Fall Ihre Argumentation gegenüber der Behörde überlegen und auch wie Sie bei den Mitarbeitern das

Bewusstsein schaffen mit Daten ab sofort anders umzugehen und Sie bei Datenverlust immer zu informieren.

Sie werden sich auch überlegen müssen, ob Sie nicht z.B. Ihren EDV-Techniker damit beauftragen alle Geräte auch von extern deaktivieren, um ggf. alle Daten löschen zu können. Das könnten bspw. Voreinstellungen auf Handys oder Notebooks sein. Rund um diese Data-Breach Thematik sollten Sie sich überlegen wie Sie und Ihre Mitarbeiter mit einem solchen Fall umgehen. Sollten Sie sich dafür entscheiden bei einem Datenverlust keine Meldung zu machen und die Behörde überprüft Sie, sind Sie der Behörde jedenfalls eine Erklärung schuldig.

Müssen Sie einen Datenschutzbeauftragten bestellen?

Grundsätzlich müssen Sie keinen Datenschutzbeauftragten bestellen, da eine Verpflichtung nur dann besteht, wenn Ihre Kerntätigkeit aus einer umfangreichen und systematischen Überwachung von Betroffenen besteht oder Ihr primäres Aufgabengebiet in der Verarbeitung von sensiblen Daten liegt. Das wird wohl beides bei Ihnen weniger der Fall sein, deswegen wird man in 99 Prozent der Fälle davon ausgehen dürfen, dass Sie keinen Datenschutzbeauftragten brauchen.

Falls Sie sich trotzdem die Frage stellen, ob es Sinn machen würde jemanden für die Compliance einzusetzen, warne ich nur davor den Datenschutz-beauftragten als denjenigen zu sehen, der nach § 9 2 VSTG die Verwaltungs-strafen ausfasst. Aber letztlich wird der Datenschutzbeauftragte nicht als Strafadressat sondern als informierender Berater sowie kontrollierender weisungsunabhängiger Experte im Unternehmen gesehen, der für die datenschutzkonforme Verarbeitung von Daten Sorge tragen soll. Die Frage, die Sie sich als Versicherungsmakler stellen müssen, ist, ob Sie freiwillig einen Datenschutzbeauftragten bestellen.

Ähnliches gilt auch für die Datenschutzfolgenabschätzung. Auch hier ist mit sehr hoher Wahrscheinlichkeit davon auszugehen, dass keine Datenverarbeitung mit hohem Risiko zu Recht und Freiheiten von Betroffenen platzgreifend sein werden.

Diese Überlegungen werden Sie auch beim Löschungsthema zu treffen haben, v.a. im Hinblick auf die Frage: wie lange kann ich die Daten doch noch speichern, obwohl ich zur Löschung aufgefordert wurde?

Was sind aus meiner Sicht die wesentlichen To Do's, denen man sich vor dem 26. Mai 2018 stellen muss?

1. Sie müssen ein **Verarbeitungsverzeichnis erstellen**. Am besten schaffen Sie sich zu allererst einen Überblick über das, was Sie tun und über den Status Quo in Ihrem Unternehmen. Im Rahmen dieser Beschäftigung wird sich sehr viel an Nebel lichten.
2. Sie werden sich in einem zweiten Schritt überlegen müssen, ob Sie das **alleine oder** nur mit einer **Expertenhilfe** schaffen.

3. Wenn Sie dann das Verarbeitungsverzeichnis erstellt haben, müssen Sie sich noch überlegen, ob Sie sich einen **Datenschutzbeauftragten engagieren oder nicht**.

4. Weiters werden Sie sich überlegen müssen, welche vorliegenden **Musterdokumente** Sie **verwenden oder** ob Sie **selber** Dokumente **erstellen**. Wenn die Behörde bei Ihnen vorbeikommt, wird sie sich Ihre Vorgänge und Prozesse und Dokumente, die Sie dazu hinterlegt haben, näher anschauen sowie welche Mitarbeiter dafür verantwortlich sind.
   Dh. Sie werden die Mitarbeiter entsprechend schulen müssen, um der Behörde auch zu zeigen, dass Sie das Thema mit ihnen durchgegangen sind. Auf der Webseite der WKÖ gibt es dazu auch schon Mustervorlagen für Schulungen von Mitarbeitern.

5. Dahinter steht das große Thema der IT-Sicherheit. Sie werden sich gemeinsam mit einem EDV-Dienstleistungsanbieter überlegen müssen, wie Sie **Datensicherheit schaffen**. Zum einen wird die gebotene Datensicherheit abhängig sein von den Arten der Daten sowie von der Art der Datenverarbeitung. Zum anderen aber auch vom Datenmüll. Ist mein Papiermüll für jeden Nachbarn einsichtig, weil der sich bspw. Versicherungsverträge und Gesundheitsdaten aus dem Mistkübel holen kann oder habe ich ein besonderes Service der Entsorgung dahinterstehen?

6. Sie werden sich im Rahmen der Verzeichniserstellung auch überlegen müssen:

    - **Wie lange** ist es legitim und sinnvoll, **Daten** zu **verarbeiten**?
    - **Wie lange** ist es legitim und sinnvoll, insbesondere personenbezogene **Daten** zu **speichern**?
    - **Welche Rechtspflichten** gehen damit einher?
    - **Welche Rechtfertigungsgründe** stehen dafür?

Ich denke man muss die Kirche im Dorf lassen und darf sich nicht zu Tode fürchten, aber es ist ein Thema, dem man sich einfach stellen muss und das man nicht länger ignorieren kann. Sie sollten mit der entsprechenden Eigenressource und den gebotenen Mitteln für sich, Ihr Unternehmen und Ihre Mitarbeiter einen Modus finden, wie Sie damit am besten umgehen. Es ist sicher keine einfache Aufgabe das notwendige Maß zu finden, aber wenn sich die ersten Nebel einmal gelichtet haben, werden Sie mit einem sinnvollen Aufwand ein möglichst rechtskonformes Ergebnis erzielen können.