MAG. URSULA ILLIBAUER

Vortrag „Allgemeine Informationen zur praktischen Anwendung der DSGVO“

Was ist neu? Das österreichische Datenschutzgesetz an sich war bislang schon sehr streng und ist jetzt an den digitalen Fortschritt bzw. an das digitale Zeitalter angepasst worden. 2016 ist die EU-DSGVO mit einer Übergangsfrist von zwei Jahren in Kraft getreten. Ab dem 25. Mai 2018 gibt es keine Nachlässe und keine Übergangsfristen mehr. Die EU-DSGVO ist eine Verordnung, dh. sie gilt prinzipiell unmittelbar in allen 28, bald 27 Mitgliedstaaten, aber es wäre nicht die EU, wenn es bei einzelnen Dingen nicht noch Spielräume für die Nationalstaaten gäbe. Das österreichische Datenschutzanpassungsgesetz 2018 - in Zukunft aber nur mehr DSG, Datenschutzgesetz – wird auch am 25. Mai 2018 in Kraft treten, wo u.a. das Datenschutzgeheimnis, die Bildverarbeitung (alte Bezeichnung: Videoüberwachung) und die Schulung von Mitarbeitern geregelt ist und wo auch nach wie vor das Grundrecht auf Datenschutz enthalten ist.

Wer ist betroffen? Datenverarbeitung zu privaten Zwecken, wie bspw. die private Social Media Nutzung (zB Facebook oder Twitter) oder die Anfertigung eines privaten Videos werden nicht von der DSGVO erfasst. Jedoch alles andere, was Sie in Ihrem beruflichen Leben mit personenbezogenen Daten machen, fällt unter die DSGVO.

Was heißt personenbezogen? Das ist alles, was nur in irgendeiner Art und Weise einen Bezug zu einer natürlichen Person herstellen kann. Name, Adresse, Telefonnummer sowie die Stimme und Bilder, aber auch IP-Adressen, Gesundheitsdaten und Gewerkschaftszugehörigkeit – die letzten beiden sind sogar sogenannte „sensible Daten“, bei welchen eine spezielle Grundlage zur Verarbeitung notwendig ist.

Welche Datenverarbeitungen sind erfasst? Einerseits die automatisierten Datenverarbeitungen, wenn Sie elektronisch Daten verarbeiten, speichern, weiterleiten etc. Andererseits aber auch, wenn Sie Daten in Papierform in einem sogenannten Dateisystem abspeichern. Der alte Papierordner kann eine systematisch geordnete Datei sein, der in irgendeiner Art und Weise alphabetisch oder chronologisch oder nach Fachgebiet abgelegt worden ist. Alles, was Sie nicht nach einem gewissen Prinzip geordnet in Papierform

ablegen und bspw. auf Ihrem chaotischen Schreibtisch einfach herumliegt, fällt nicht darunter. Allerdings all die Dinge, die Sie auch elektronisch erfasst haben, fallen sehr wohl wieder unter die DSGVO.

Wo sind sie erfasst? Der EU-Bezug muss bestehen. Alle Big-Player, die zwar einen Sitz außerhalb der EU haben, sich aber auf den europäischen Markt ausrichten oder Daten europäischer Staatsbürger verarbeiten, fallen trotzdem in die DSGVO hinein. Wir haben zum ersten Mal die Situation, dass eine Verordnung nicht nur wegen Big-Playern geschrieben worden, sondern tatsächlich auch auf diese anwendbar ist.

Ich kann Ihnen ein paar Begriffe leider nicht ersparen, merken Sie sich von nachstehender Tabelle bitte zumindest drei.

DSGVO	**DSG 2000**
personenbezogene Daten	personenbezogene Daten
besondere Kategorien von Daten	sensible Daten
verarbeiten	verwenden
Verantwortlicher	Auftraggeber
Auftragsverarbeiter	Dienstleister
Profiling	-
-	Übermitteln / Überlassen
Empfänger, Dritter	-
Pseudonymisierung	indirekt personenbezogene Daten
Dateisystem	-

Verantwortlicher ist derjenige, der die Entscheidung trifft, was mit den Daten passiert. Werden sie gespeichert, gelöscht, werden sie weitergeleitet, etc.? Verantwortlicher ist auch derjenige, der letztendlich die Haftung übernehmen muss und die entsprechende Strafe tragen wird.

Auftragsverarbeiter (alte Bezeichnung: Dienstleister) sind all jene, die Sie hinzuziehen, um Daten zu verarbeiten. Das sind Steuerberater, Buchhalter, Personalverrechner, IT-Dienstleister UND auch Sie, wenn Sie im Auftrag von einem Dritten Daten in irgendeiner Art und Weise verarbeiten. In diesem Fall sind Sie sowohl Verantwortlicher für Ihre eigenen Daten als auch Auftragsverarbeiter für Ihren jeweiligen Kunden.

Merken Sie sich bitte auch „**verarbeiten**". Das ist bearbeiten, ändern, korrigieren, speichern, löschen, etc. Die meisten von Ihnen werden mit Versicherungen zusammen arbeiten und die Daten der Versicherung weiterleiten.

Was Sie konkret einhalten müssen, um tatsächlich DSG-konform zu sein, finden Sie im **8-PUNKTE PLAN:**

1. GRUNDSÄTZE EINHALTEN

Diese Grundsätze sind nichts Neues und waren auch schon im DSG 2000 enthalten. Das sind Dinge, die Sie jetzt schon im Betrieb implementiert haben sollten.

Rechtmäßigkeit. Um Daten zu verarbeiten, brauchen Sie irgendeine Art von Rechtfertigungsgrund. Einerseits die Vertragserfüllung, da Sie Daten aufnehmen müssen, um den Vertrag mit dem Kunden abzuwickeln und die Versicherung vermitteln zu können oder andererseits die gesetzliche Grundlage, da Sie Daten Ihrer Mitarbeiter aufnehmen müssen, um sie an die Gebietskrankenkassa weiterzuleiten. Oder Sie haben sich eine Einwilligungserklärung (alte Bezeichnung: datenschutzrechtliche Zustimmung) eingeholt. Auch eine gesetzliche Grundlage ist eine mögliche rechtmäßige Grundlage um Daten zu verarbeiten.

Treu & Glauben oder Transparenz. Der Betroffene kennt sich aus, weiß was passiert, ist nicht verwirrt und hat eine Ahnung darüber was Sie mit Daten tun.

Richtigkeit. Daten müssen immer sachlich richtig und auf dem aktuellen Stand sein.

Speicherbegrenzung. Das Datenschutzgesetz oder die DSGVO sieht vor, dass Sie sich vorher überlegen müssen welche Aufbewahrungspflichten hinter den Daten bzw. Datensätzen stehen. Dh. Sie müssen sich auch überlegen ob Sie irgendwelche gesetzlichen Aufbewahrungspflichten haben z.B. aus der Bundesabgabenordnung (7 oder 10 Jahre?) oder aus dem Gewährleistungsrecht (2 oder 3 Jahre?) oder aus dem Schadenersatzrecht (3 oder 30 Jahre?). Wenn Sie Daten eines Kunden aufbewahren, weil Sie davon ausgehen, dass eventuell noch einmal ein Schaden auf Sie zukommen könnte, dann ist es in Ordnung wenn Sie diese Daten aufbewahren, aber bitte nur diese konkreten Daten und nicht das gesamte Kundenprofil, das Sie noch um den Kunden herum aufgebaut und gespeichert haben.

Zweckbindung. Sie dürfen Daten nur mit einem Zweck dahinter verarbeiten und müssen sich vorher überlegen, wofür Sie diesen Datensatz eigentlich brauchen. Das kann die Vertragserfüllung, die Tätigkeit mit der Versicherung, ein Werbezweck, eine Kundenbeziehung oder Ähnliches sein.

Datenminimierung. Die DSGVO schreibt vor, dass Sie nur so viele Daten sammeln dürfen, die Sie tatsächlich auch benötigen.

Integrität & Vertraulichkeit bedeutet, dass Sie die Daten so sicher wie es Ihnen möglich ist, verwahren. Datensicherheit spielt eine relevante Rolle bei der DSGVO.

Rechenschaft heißt für Sie als Verantwortlicher, dass Sie auch nachweisen können bzw. beweispflichtig sind, dass Sie diese Grundsätze auch tatsächlich erfüllt haben.

2. EINWILLIGUNGEN RICHTIG EINHOLEN

Einwilligungen müssen zum einen **freiwillig** und zum anderem für **einen bestimmten Fall** erteilt werden. Sie können sich keine Pauschaleinwilligung für alle möglichen Tätigkeiten einholen, sondern müssen konkret ausweisen, für welche Zwecke Sie diese Daten brauchen. Das muss sehr transparent erfolgen, weswegen Einwilligungserklärungen besser länger als knapper ausfallen sollten.

Der Kunde muss aktiv seinen Willen bekunden sein. Diese **Willensbekundung** kann zwar auch mündlich erteilt werden, aber schriftlich ist immer besser, da Sie dies im Einzelfall auch beweisen können.

Getrennt von anderen Sachverhalten bedeutet, dass Sie die Einwilligungserklärungen nirgends verstecken dürfen. Früher wurden diese in Allgemeinen Geschäftsbedingungen oder in Nutzungsbedingungen versteckt und waren aufgrund dieser Intransparenz auch früher schon nicht gültig. Sie müssen die Einwilligungserklärung entweder mit Fettdruck oder eigener Überschrift mit farblicher Markierung kennzeichnen oder Sie geben am Schluss Ihres Vertragskonvoluts den Hinweis, dass dies einerseits Vertrag und AGB sind, die hier akzeptiert werden, aber andererseits auch eine Einwilligungserklärung unterschrieben wird. Bitte achten Sie darauf, dass Sie das auch immer getrennt und transparent ausweisen. Der Kunde stimmt mit seiner Unterschrift nicht nur den AGB sondern auch den Datenschutzbestimmungen zu.

Prinzipiell ist eine Einwilligungserklärung **jederzeit widerrufbar** und daher eine sehr schwache Grundlage um Daten zu verarbeiten.

Formulierungsvorschläge für Einwilligungserklärungen finden Sie unter www.wko.at/datenschutz.

Sie werden keine großen Unterschiede zu den bereits existierenden geltenden Datenschutzrecht-Mustern bemerken, da die Wirtschaftskammer durchgesetzt hat, dass geltende gültige Datenschutzerklärungen auch nach in Geltung treten der DSGVO weiterhin gültig bleiben. Dh. wenn Sie die bisherigen (ohnehin schon sehr strengen) Bestimmungen eingehalten haben, erfüllen Sie gleichzeitig auch die Bestimmungen der DSGVO und können sich auch nach dem 25. Mai 2018 auf Ihre alten Einwilligungen stützen.

3. DATENSCHUTZBEAUFTRAGTEN BESTELLEN?

Es gibt für ganz bestimmte Branchen bzw. für sehr heikle Kerntätigkeiten eine Verpflichtung für die Bestellung eines Datenschutzbeauftragten. Der erste Entwurf, einen Datenschutzbeauftragten immer ab einer bestimmten Unternehmensgröße einzuführen, konnte abgewendet werden und geblieben ist die Verpflichtung für öffentliche Stellen und Behörden, aber auch für jene,

deren Kerntätigkeit eine besonders heikle Datenverarbeitung nach sich zieht. Darunter werden entweder systematisch umfangreich überwachende Tätigkeiten oder eine umfangreiche Datenverarbeitung sensibler Daten (z.B. Gesundheitsdaten) oder strafrechtlich relevanter Daten verstanden.

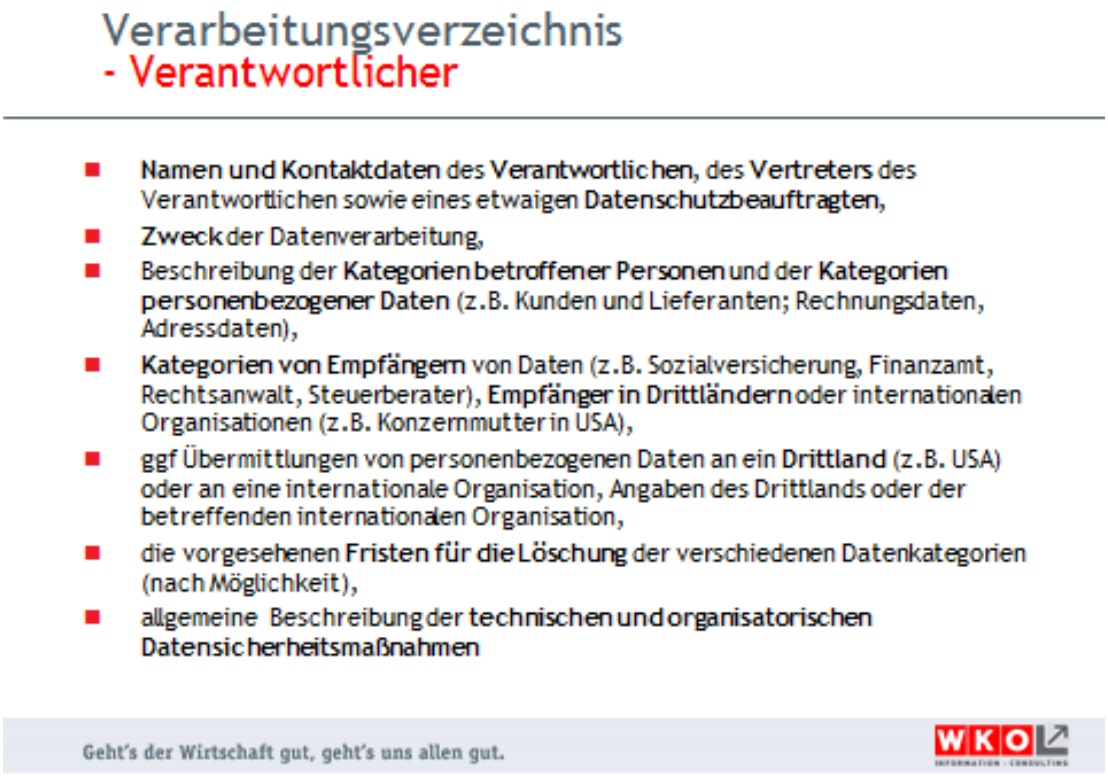
!Achtung bitte!: Diese drei Dinge müssen kumulativ entsprechend erfüllt sein. Dh. 1. muss die Kerntätigkeit auf diese besonders heikle Datenverarbeitung ausgerichtet sein und ist nicht etwas, das nebenher mitläuft. 2. muss es sich um eine umfangreiche Datenverarbeitung in Form einer hohen Anzahl an Betroffenen oder einer hohen Anzahl an Daten handeln. 3. muss es sich bei der umfangreichen Datenverarbeitung um die Verarbeitung sensibler Datensätze, strafrechtlich-relevanter Datensätze oder um eine systematische Überwachung handeln.

Ihre Hauptaufgabe besteht sicher nicht aus der Datenverarbeitung sensibler Daten, sondern wird wohl als Nebentätigkeit gesehen.

4. VERARBEITUNGSVERZEICHNIS ERSTELLEN!

Das Verarbeitungsverzeichnis ist wesentlich und hilft Ihnen gegenüber der Datenschutzbehörde. Wenn Sie das Verarbeitungsverzeichnis nicht vorweisen können, wird es sicher teuer. Das Verarbeitungsverzeichnis ist ein Kernpunkt des Datenschutzrechts und eine verpflichtende Vorschreibung der DSGVO. Es ist eine Aufzeichnung aller nur irgendwie denkbar datenschutzrelevanter Vorgänge im Betrieb. Dh. Sie protokollieren in schriftlicher oder elektronischer Form was Sie genau mit personenbezogenen Daten machen. Hierfür gibt es auch schon Muster auf www.wko.at/datenschutz.

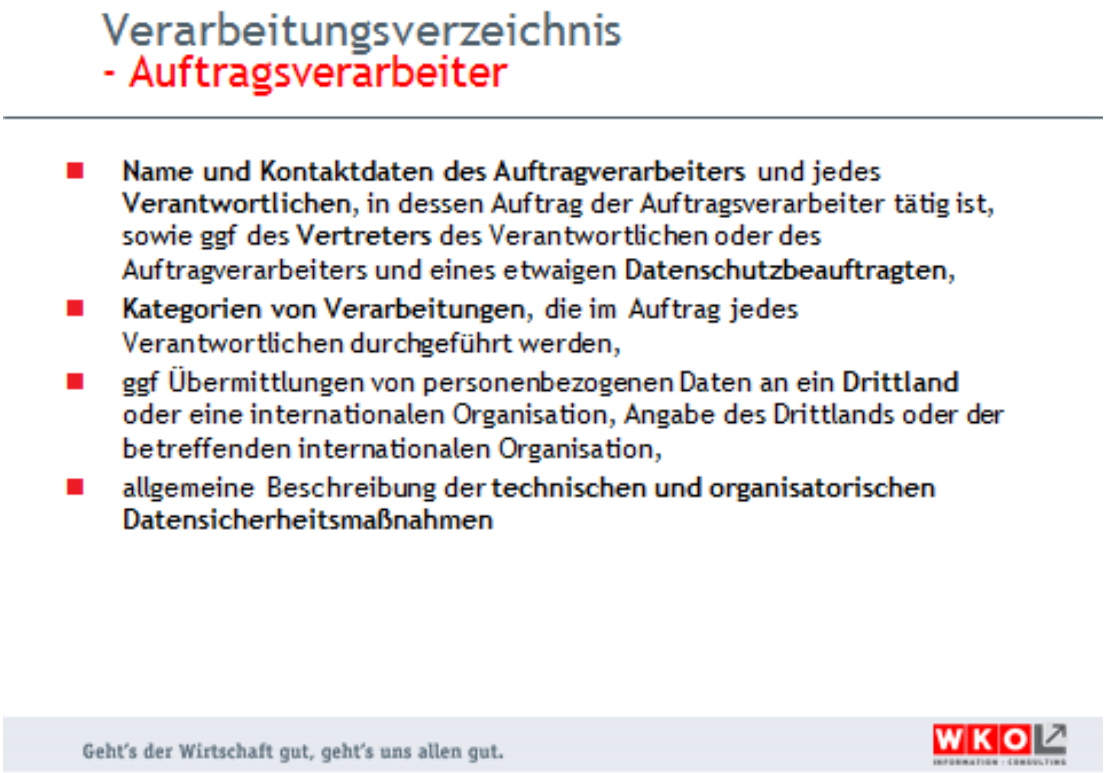
Das DVR, das Datenverarbeitungsregister bei der Datenschutzbehörde, ist mittlerweile exportierbar, sodass Sie Ihre Datenmeldungen aus dem Register „herausholen“ und für Ihre eigenen Aufzeichnungen verwenden können. Das Verarbeitungsverzeichnis ist zwar sehr arbeitsaufwendig, aber eines der wichtigsten Punkte aus der DSGVO und gegenüber der Behörde, damit Sie nicht (sofort) gestraft werden. Das Verzeichnis erfasst folgende Punkte:



Wenn Sie Daten an einen Dritten weitergeben, ob nun an Dienstleister, Vertragspartner oder Konzernunternehmen, müssen Sie das im Verzeichnis ausweisen. Wenn der Dienstleister, Ihr Auftragsverarbeiter, darüber hinaus noch außerhalb der EU ansässig ist, müssen Sie ebenfalls darauf verweisen, dass Sie hier Daten ins EU-Ausland schicken und auf welcher Grundlage Sie sich beziehen (zB USA: privacy shield?).

Im Verarbeitungsverzeichnis müssen weiters sowohl die Fristen für die Löschung der jeweiligen Daten als auch die technischen und organisatorischen Sicherheitsmaßnahmen angeführt werden.

Wenn Sie als Auftragsverarbeiter für Ihre Kunden oder für die Versicherung auftreten, müssen Sie ein zweites (drittes, viertes,…) Verarbeitungsverzeichnis jeweils für diese Kunden oder für die Versicherung, etc. führen und zwar eines, das das der Versicherung ergänzt. In diesem sind nur ergänzende Informationen anzuführen. Ich gehe davon aus, dass man ohnehin mit Ihnen Kontakt aufnehmen wird um eine gewisse Form abzustimmen.



Nachdem Sie in Ihrem Unternehmen wahrscheinlich mehr als ein Verarbeitungsverzeichnis führen werden müssen, stellen Sie bitte sicher, dass Sie dies auch organisatorisch im Betrieb entsprechend durchführen können.

5. RISIKEN ANALYSIEREN!

Ein weiterer sehr wichtiger Punkt der DSGVO ist die Stärkung der Selbstverantwortung im Unternehmen. Meldeverpflichtungen bei der Behörde werden bis auf zwei Fälle wegfallen, dh

- es gibt kein DVR-Nummern mehr,
- es gibt keine Meldeverpflichtung im Vornhinein mehr so wie wir es kannten.

Sie sind derjenige, der eine Selbstverantwortung im Betrieb trägt und das Risiko, das mit der Datenverarbeitung verbunden ist, einschätzen muss.

Wenn Sie zB im Rahmen eines Kundengesprächs Name, Adresse und Telefonnummer des Kunden aufnehmen und diese Daten elektronisch in Ihrer Kundendatenbank aufnehmen, ist das an sich eine normale, profane Datenverarbeitung und wohl nicht wirklich mit einem Risiko verbunden, da

man diese Daten üblicherweise auch im Telefonbuch findet oder der Kunde diese bspw. selbst über seine Webseite schon veröffentlicht hat. Wenn Sie aber darüber hinaus, wie es in Ihrem Fall möglicherweise passieren kann, umfangreich Gesundheitsdaten (Krankengeschichte, Röntgenbilder oder Ähnliches) vom Kunden miterfassen und zB an die Versicherung weiterschicken, kann eine sogenannte Datenschutzfolgenabschätzung nötig werden. Die Frage, die sich hier wieder stellt, ist – ist diese Datenverarbeitung „umfangreich“?

6. DATENSCHUTZFOLGENABSCHÄTZUNG ERSTELLEN?

Die Datenschutzfolgenabschätzung ist eine Art „worst-case-Szenario“. Sie müssen sich überlegen:

- Was mache ich mit den Daten?
- Warum mache ich das?
- Was sind die Risiken, die damit einhergehen?

und vor allem und das ist wesentlich

- Welche Sicherheitsmaßnahmen kann ich setzen, um diese Risiken einzuschränken bzw. entsprechend zu minimieren?
- Gibt es eine Verschlüsselungsmöglichkeit? Kann ich die Daten verschlüsselt abspeichern? Gibt es Pseudonymisierungsmöglichkeiten?

Wenn Sie diese Überlegungen mit-protokollieren, ist Ihre Datenschutzfolgen-abschätzung vollendet. Die Frage ist nun nur mehr, ob Sie allfällige Risiken entsprechend reduzieren bzw beseitigen konnten. Wenn das Risiko nach wie vor besteht und leider nur auf hoch eingeschätzt werden kann, müssen Sie die Datenschutzbehörde konsultieren. Das ist einer von zwei Fällen, in welchen Sie die Behörde kontaktieren müssen. Auf den zweiten Fall werde ich näher unter Punkt 8. „Datensicherheit einhalten“ eingehen. Die Datenschutzbehörde wird Ihnen in diesem Fall entweder eine Empfehlung abgeben oder Ihnen den Datenverarbeitungsvorgang untersagen, weil es einfach zu heikel und gefährlich ist und die Risiken für die betroffenen Personen zu hoch.

7. BETROFFENENRECHTE BEACHTEN!

Ich gehe davon aus, dass Sie die Betroffenenrechte bis auf das Recht auf Datenübertragbarkeit und das Recht auf Einschränkung bereits kennen.

Was hat sich nun geändert?

- der Inhalt (zB bei den Informationspflichten und Auskunftsrechten) ist wesentlich erweitert worden,
- die Frist ist von 8 Wochen auf 4 Wochen verkürzt worden.

Bitte versuchen Sie in Ihrem Betrieb einen systematisierten standardisierten Ablauf zu gewährleisten, um ggf. möglichst rasch auf Anfragen von Betroffenen reagieren zu können, sodass nicht der gesamte Betrieb still steht.

8. DATENSICHERHEIT EINHALTEN!

Der letzte und auch der wichtigste Punkt ist die Datensicherheit. Bitte vernachlässigen Sie das Thema nicht mehr, denn eine ruinierte Festplatte oder ein im Zug vergessener Computer können schnell einmal passieren, für Sie aber Einiges an Aufwand verursachen. Die DSGVO schreibt nicht konkret vor, was Sie tun müssen, aber sie weist aus, dass Sie als Unternehmer Ihr finanziell Möglichstes in Abstimmung mit den technischen Möglichkeiten am Markt tun müssen, um auch solche Datenlecks wie vorhin beschrieben zu vermeiden.

Und wenn dann doch einmal ein Datenleck passiert ist, obwohl Sie das Beste getan haben, und zB für die Kundendaten ein Risiko besteht, da deren Daten in irgendeiner Art und Weise abhandengekommen sind, müssen Sie den Vorfall – und das ist der 2. Fall – der Datenschutzbehörde melden. Unter der Bezeichnung „Data Breach Notification“ melden Sie der Datenschutzbehörde was passiert und wer betroffen ist. Das ist keine Selbstanzeige, sondern eine Information an die Datenschutzbehörde, die dann selber entscheidet, ob das eventuell ein Vorfall ist, bei welchem andere informiert werden müssen – wahrscheinlich eher nicht – oder ob hier eine individuelle Empfehlung ausreichend ist. Sollte das Risiko durch das entstandene Datenleck (z.B. der im Zug vergessene Laptop) sehr hoch sein, weil auf dem Laptop tatsächlich auch Gesundheitsdaten von betroffenen Personen abgespeichert wurden und diese nicht gesichert waren, dann sind Sie auch verpflichtet die betroffenen Kunden

darüber zu informieren. Wenn die Anzahl an betroffenen Kunden ebenfalls sehr hoch ist, müssen Sie im Einzelfall abwägen, ob Sie auf Ihrer Webseite über ein Datenleck informieren oder lieber eruieren wer die Kunden waren, um diese individuell darüber anzuschreiben.

Was ist nun zu tun?

- Schauen Sie sich einfach einmal an was Sie datenschutzrechtlich im Betrieb tun. Machen Sie einen Datencheck, eine IST-Stand-Analyse. Was tun wir überhaupt mit Daten?
- Wieviel Zeit und Budget haben Sie für die Adaptierung?
- Überlegen Sie sich wer in Zukunft für Datenschutz zuständig sein soll!
- Protokollieren Sie am besten gleich mit, da Sie diese Arbeit ohnehin für die Erstellung eines Datenverarbeitungsverzeichnis später brauchen werden.
- Überprüfen Sie auch Ihre veröffentlichten Informationen auf der eigenen Webseite, in E-Mails, in Vertragsmustern, etc.
- Schauen Sie sich Ihre Datensicherheitsmaßnahmen an und protokollieren Sie dies ebenfalls gleich mit.

Und warum das Ganze? U.a. auch wegen der sehr hohen Strafdrohung.

Die Höchststrafe beträgt 20 Millionen Euro oder 4 % des weltweiten Konzernumsatzes des vorangegangen Geschäftsjahres.
Datenschutzverletzungen werden in Zukunft finanziell schmerzen, es werden keine paar hundert sondern ein paar tausend Euro. Die Datenschutzbehörde ist auch angehalten abschreckende und wirksame Maßnahmen zu setzen.

Abschließend darf ich Ihnen noch die zwei wichtigsten Links vorstellen:

- www.wko.at/datenschutz

Auf dieser Webseite finden Sie Musterchecklisten, Informationsdokumente, zwei Online-Ratgeber, Musterdokumente und Vieles mehr. Bei einem der Onlineratgeber erhalten Sie eine auf Sie individuell zugeschnittene

Datenschutzerklärung, beim anderen können Sie auch einmal durchspielen, wie weit Sie im Unternehmen bereits in der DSGVO-Adaptierung sind.

- www.it-safe.at

Auf dieser Webseite können Sie einen Vergleich zu anderen österreichischen Unternehmen ziehen – tun Sie schon das Wesentlichste? Die Basics? Viel zu wenig? Ein Ampelsystem weist aus, wie sicher Sie in Ihrem Unternehmen da stehen.