Wr. Neustadt am 22.08.2018

HIS-1808003

Wenn Datenschutz zur Pflicht wird!

Die **VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES** vom 27. April 2016 ist zum **Schutz natürlicher Personen** bei der **Verarbeitung personenbezogener Daten** und dem **freien Verkehr solcher Daten** gedacht. Dabei handelt es sich um ein **Grundrecht gem. Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union** sowie **Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union** (AEUV).

Der folgende Beitrag soll einen **ersten Einblick in den Zweck der Richtlinie** einschließlich einiger **Vorgaben** dieser aber auch der **damit verbunden Maßnahmen und Sanktionen** geben.

Aufgrund der **Komplexität des Themas** und der **vielen unterschiedlichen Auslegungen der rechtlichen Bestimmungen** wird hiermit **kein Anspruch auf Vollständigkeit** erhoben. Es soll vielmehr ein **Bewusstsein in Bezug auf Datenschutz** und den **Umgang damit geschaffen werden**.

Was ist der Zweck der Richtlinie?

Laut Erwägungsgrund 3 der VERORDNUNG (EU) 2016/679 sollen damit die **Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung** sowie die **Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten** erreicht werden.

Die **Verarbeitung personenbezogener Daten** sollte **im Dienste der Menschheit** stehen. Das **Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht**; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. (Auszug aus Erwägungsgrund 4 der VERORDNUNG (EU) 2016/679)

Im Erwägungsgrund 71 der VERORDNUNG (EU) 2016/679 ist festgehalten, dass die **betroffene Person das Recht haben sollte**, **keiner Entscheidung** — was eine Maßnahme einschließen kann — **zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden**, die **ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder** sie **in ähnlicher Weise erheblich beeinträchtigt**, **wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen**.

Was ist eine Verletzung des Schutzes personenbezogener Daten?

In den Begriffsbestimmungen des Artikels 4 Punkt 12 der VERORDNUNG (EU) 2016/679 ist die „**Verletzung des Schutzes personenbezogener Daten**“ als **eine Verletzung der Sicherheit** definiert, die - ob unbeabsichtigt oder unrechtmäßig - zur **Vernichtung**, zum **Verlust**, zur **Veränderung** oder zur **unbefugten Offenlegung** von beziehungsweise zum

unbefugten Zugang zu **personenbezogenen Daten führt**, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Wer ist für die Überprüfung der Einhaltung der Vorschriften zuständig?

Im Artikel 51 Abs. (1) der VERORDNUNG (EU) 2016/679 ist festgehalten, dass jeder Mitgliedstaat vorzusehen hat, dass eine oder mehrere **unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig** ist/sind, damit die **Grundrechte und Grundfreiheiten natürlicher Personen** bei der Verarbeitung **geschützt werden** und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde").

Weiters sind diese **Aufsichtsbehörden befugt, Verstöße** den **Justizbehörden** zur **Kenntnis zu bringen** und gegebenenfalls die **Einleitung eines gerichtlichen Verfahrens** zu betreiben oder sich sonst **daran zu beteiligen**, **um die Bestimmungen** der VERORDNUNG (EU) 2016/679 **durchzusetzen**.

Welche Befugnisse haben die Aufsichtsbehörden?

Gemäß Artikel 58 der VERORDNUNG (EU) 2016/679 (Auszug davon) haben diese Aufsichtsbehörden über **Untersuchungsbefugnisse** zu verfügen die es ihr gestatten,

*a) den **Verantwortlichen, den Auftragsverarbeiter** und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters **anzuweisen**, alle **Informationen bereitzustellen**, die **für die Erfüllung ihrer Aufgaben erforderlich** sind,*
*b) **Untersuchungen in Form von Datenschutzüberprüfungen** durchzuführen,*
*c) eine **Überprüfung** der nach Artikel 42 Absatz 7 **erteilten Zertifizierungen** durchzuführen,*
*d) den **Verantwortlichen** oder den **Auftragsverarbeiter** auf einen vermeintlichen **Verstoß** gegen diese Verordnung **hinzuweisen**,*
*e) von dem **Verantwortlichen** und dem **Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen,** die zur Erfüllung ihrer Aufgaben notwendig sind, **zu erhalten**,*
*f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats **Zugang zu den Geschäftsräumen**, einschließlich aller Datenverarbeitungsanlagen und -geräte, des **Verantwortlichen** und des **Auftragsverarbeiters zu erhalten**.*

und über **Abhilfebefugnisse** zu verfügen die es ihr gestatten,

*a) einen **Verantwortlichen** oder einen **Auftragsverarbeiter** zu **warnen**, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,*
*b) einen **Verantwortlichen** oder einen **Auftragsverarbeiter** zu **verwarnen**, wenn er mit Verarbeitungsvorgängen **gegen diese Verordnung verstoßen hat**,*
*c) den **Verantwortlichen** oder den **Auftragsverarbeiter anzuweisen**, den Anträgen der **betroffenen Person** auf Ausübung der ihr nach dieser Verordnung **zustehenden Rechte zu entsprechen**, 4.5.2016 L 119/69 Amtsblatt der Europäischen Union DE*
*d) den **Verantwortlichen** oder den **Auftragsverarbeiter anzuweisen**, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums **in Einklang mit dieser Verordnung zu bringen**,*
*e) den **Verantwortlichen anzuweisen**, die von einer Verletzung des Schutzes personenbezogener Daten **betroffenen Person entsprechend zu benachrichtigen**,*
*f) eine **vorübergehende** oder **endgültige Beschränkung der Verarbeitung**, **einschließlich** eines **Verbots**, zu verhängen,*
*g) die **Berichtigung oder Löschung** von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen **anzuordnen**,*
*h) eine **Zertifizierung zu widerrufen** oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,*
*i) eine **Geldbuße gemäß Artikel 83 zu verhängen**, **zusätzlich** zu **oder anstelle** von in diesem **Absatz genannten Maßnahmen**, je nach den Umständen des Einzelfalls,*
*j) die **Aussetzung der Übermittlung von Daten** an einen Empfänger in einem Drittland oder an eine internationale Organisation **anzuordnen**.*

sowie über **Genehmigungsbefugnisse und beratenden** Befugnisse zu verfügen die es ihr gestatten,

*a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den **Verantwortlichen zu beraten**,*
*b) zu **allen Fragen**, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, **von sich aus oder auf Anfrage Stellungnahmen** an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats **an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten**,*
*c) die **Verarbeitung gemäß Artikel 36 Absatz 5 zu** genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,*
*d) eine **Stellungnahme abzugeben** und **Entwürfe von Verhaltensregeln** gemäß Artikel 40 Absatz 5 zu **billigen**,*
*e) **Zertifizierungsstellen** gemäß Artikel 43 zu **akkreditieren**,*
*f) im Einklang mit Artikel 42 Absatz 5 **Zertifizierungen zu erteilen** und Kriterien für die Zertifizierung zu billigen,*
*g) **Standarddatenschutzklauseln** nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d **festzulegen**,*
*h) **Vertragsklauseln** gemäß Artikel 46 Absatz 3 Buchstabe a zu **genehmigen**,*
*i) **Verwaltungsvereinbarungen** gemäß Artikel 46 Absatz 3 Buchstabe b zu **genehmigen***
*j) **verbindliche interne Vorschriften** gemäß Artikel 47 zu **genehmigen**.*

Weiters sind diese **Aufsichtsbehörden befugt Verstöße** den **Justizbehörden** zur **Kenntnis zu bringen** und gegebenenfalls die **Einleitung eines gerichtlichen Verfahrens** zu betreiben oder sich sonst **daran zu beteiligen**, **um die Bestimmungen** der VERORDNUNG (EU) 2016/679 **durchzusetzen**.

Wie ist die Haftung geregelt?

Die **Vorgaben** des Artikels 82 der VERORDNUNG (EU) 2016/679 zu **Haftung und Recht auf Schadenersatz** sehen vor, dass jede Person, der wegen eines Verstoßes gegen diese Verordnung ein **materieller** oder **immaterieller Schaden** entstanden ist, **Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter** hat.

Ein **Auftragsverarbeiter haftet** für den durch eine Verarbeitung **verursachten Schaden** nur dann, wenn er seinen **speziell den Auftragsverarbeitern auferlegten Pflichten aus der Verordnung (EU) 2016/679 nicht nachgekommen ist** oder **unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen** oder **entgegen diese Anweisungen gehandelt hat**.

Der Verantwortliche oder der Auftragsverarbeiter wird **von der Haftung** gemäß Artikel 82 Absatz 2 der VERORDNUNG (EU) 2016/679 **befreit**, wenn er **nachweist**, dass er in **keinerlei Hinsicht für den Umstand**, durch den der **Schaden eingetreten** ist, **verantwortlich** ist. Im österreichischen Datenschutzgesetz ist im § 29 Folgendes zu lesen:

> *(1) Jede Person, der wegen eines **Verstoßes gegen die DSGVO** oder **gegen § 1 oder Artikel 2 1. Hauptstück** ein **materieller oder immaterieller Schaden** entstanden ist, hat **Anspruch auf Schadenersatz gegen** den **Verantwortlichen** oder gegen den **Auftragsverarbeiter** nach Art. 82 DSGVO. **Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts.***

Welche Maßnahmen und/oder Strafen sind vorgesehen?

Besonderes Augenmerk ist auf den Artikel 83 der VERORDNUNG (EU) 2016/679 in Bezug auf die **Verhängung von Geldbußen** zu legen. Diese sehen vor, dass jede Aufsichtsbehörde sicherstellt, dass die **Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.**

Im **Erwägungsgrund 148** der VERORDNUNG (EU) 2016/679 ist Folgendes zu lesen:

> *Im Interesse einer konsequenteren **Durchsetzung der Vorschriften** dieser Verordnung sollten **bei Verstößen** gegen diese Verordnung **zusätzlich zu** den **geeigneten Maßnahmen**, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, **oder** **an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen** verhängt werden. Im Falle eines **geringfügigeren Verstoßes** oder falls **voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken** würde, **kann anstelle einer Geldbuße eine Verwarnung erteilt werden**. Folgendem sollte **jedoch***

***gebührend Rechnung getragen** werden: der **Art**, **Schwere** und **Dauer des Verstoßes**, dem **vorsätzlichen Charakter** des Verstoßes, den Maßnahmen **zur Minderung des entstandenen Schadens**, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der **Art und Weise**, wie der **Verstoß der Aufsichtsbehörde bekannt wurde**, der **Einhaltung der** gegen den Verantwortlichen oder Auftragsverarbeiter **angeordneten Maßnahmen**, der **Einhaltung von Verhaltensregeln** und **jedem anderen erschwerenden oder mildernden Umstand**. Für die **Verhängung von Sanktionen einschließlich Geldbußen** sollte es **angemessene Verfahrensgarantien** geben, die den **allgemeinen Grundsätzen des Unionsrechts** und der **Charta**, einschließlich des Rechts auf **wirksamen Rechtsschutz** und ein **faires Verfahren**, entsprechen.*

Im Artikel 82 der VERORDNUNG (EU) 2016/679 (Auszug davon) sind **Haftung und Recht auf Schadenersatz wir folgt geregelt:**

*(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat **Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter**.*

*(2) **Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.** Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.*

Geldbußen werden je nach den Umständen des Einzelfalls **zusätzlich zu oder anstelle von Maßnahmen** nach Artikel 58 Absatz 2 Buchstaben a bis h und i der VERORDNUNG (EU) 2016/679 **verhängt** und sehen gemäß Artikel 83 folgende Höhen vor:

*(4) Bei **Verstößen gegen die folgenden Bestimmungen** werden im Einklang mit Absatz 2 **Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*

- *a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;*
- *b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;*
- *c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4. 4.5.2016 L 119/82 Amtsblatt der Europäischen Union DE*

*(5) Bei **Verstößen gegen die folgenden Bestimmungen** werden im Einklang mit Absatz 2 **Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*

- *a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;*
- *b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;*
- *c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;*
- *d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;*
- *e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.*

*(6) Bei **Nichtbefolgung einer Anweisung der Aufsichtsbehörde** gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels **Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.*

Die **allgemeinen Bedingungen für die Verhängung von Geldbußen** sind im **österreichischen Datenschutzgesetz** (DSG) wie folgt geregelt (Auszug DSG):

*§ 30. (1) Die **Datenschutzbehörde kann Geldbußen gegen eine juristische Person verhängen**, wenn Verstöße gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben und eine Führungsposition innerhalb der juristischen Person aufgrund*

1. *der Befugnis zur Vertretung der juristischen Person,*
2. *der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder*
3. *einer Kontrollbefugnis innerhalb der juristischen Person*

innehaben.

(2) ***Juristische Personen können wegen Verstößen*** *gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück auch* ***verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle*** *durch eine in Abs. 1 genannte Person die* ***Begehung dieser Verstöße*** *durch eine* ***für die juristische Person tätige Person*** *ermöglicht hat, sofern die* ***Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet****.*

(3) Die ***Datenschutzbehörde*** *hat von der Bestrafung eines* ***Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991*** *– VStG, BGBl. Nr. 52/1991,* ***abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.***

Nicht zu unterschätzten sind die **besonderen Strafbestimmungen im österreichischen Datenschutzgesetz,** welche wie folgt lauten (Auszug DSG):

Verwaltungsstrafbestimmungen

§ 62. (1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine ***Verwaltungsübertretung****, die mit* ***Geldstrafe bis zu 50 000 Euro*** *zu ahnden ist, wer*

1. *sich* ***vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft*** *oder einen* ***erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält****,*
2. ***Daten vorsätzlich in Verletzung des Datengeheimnisses*** *(§ 6)* ***übermittelt****, insbesondere Daten, die ihm gemäß §§ 7 oder 8 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,*
3. ***sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten*** *gemäß § 10* ***verschafft****,*
4. *eine* ***Bildverarbeitung entgegen den Bestimmungen*** *des 3. Abschnittes des 1. Hauptstücks betreibt* ***oder***
5. *die* ***Einschau*** *gemäß § 22 Abs. 2* ***verweigert****.*

(2) ***Der Versuch ist strafbar****.*

(3) ***Gegen juristische Personen*** *können bei Verwaltungsübertretung nach Abs. 1 und 2* ***Geldbußen*** *nach Maßgabe des § 30 verhängt werden.*

Datenverarbeitung in Gewinn- oder Schädigungsabsicht

§ 63. Wer mit dem ***Vorsatz****,* ***sich oder einen Dritten dadurch unrechtmäßig zu bereichern****, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen,* ***personenbezogene Daten****, die ihm* ***ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut*** *oder* ***zugänglich geworden sind*** *oder die er* ***sich widerrechtlich verschafft hat****,* ***selbst benützt****,* ***einem anderen zugänglich macht oder veröffentlicht****, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht* ***ist****,* ***vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen****.*

Wichtig und zu beachten – Sanktionen und Maßnahmen!

Sanktionen gemäß Artikel 84 der VERORDNUNG (EU) 2016/679 **müssen wirksam**, **verhältnismäßig** und **abschreckend sein**.

Mit dem **Datenschutz-Deregulierungs-Gesetz 2018** hat der Nationalrat folgende Änderung des Datenschutzgesetzes (DSG) beschlossen:

„Verwarnung durch die Datenschutzbehörde

§ 11. Die **Datenschutzbehörde** wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur **Anwendung** bringen, dass die **Verhältnismäßigkeit gewahrt** wird. Insbesondere bei **erstmaligen Verstößen** wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere **durch Verwarnen Gebrauch** machen."

In **Expertenkreisen ist jedoch fraglich**, ob dieser **Beschluss im Einklang mit dem Europarecht** steht, da mit dem **Beitritt Österreichs zur Europäischen Union Kompetenzen an diese abgegeben** wurden (**Subsidiaritätsprinzip**) und die **VERORDNUNG** (EU) 2016/679 **direkt wirkt**, anders als bei einer Richtlinie der EU (welche in nationales Recht übergeleitet werden muss).

Es kann somit dazu kommen, dass die **gut gemeinte Reglung des § 11 DSG als nicht europarechtskonform angesehen** wird und **Bescheide der Datenschutzbehörde mit**

Strafen und/oder Maßnahmen vor dem Verwaltungsgerichtshof landen und dieser im Zuge eines **Vorabentscheidungsverfahrens den Europäischen Gerichtshof** anruft (bzw. anrufen muss), um diese Frage zu klären.

Wie hoch soll/muss der Aufwand für die Umsetzung des Datenschutzes im Unternehmen sein?

Auszug aus Artikel 24 der VERORDNUNG (EU) 2016/679:

> „(1) Der **Verantwortliche setzt unter Berücksichtigung** der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere der Risiken** für die **Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen** um, um **sicherzustellen** und den **Nachweis dafür erbringen zu können**, dass die **Verarbeitung gemäß dieser Verordnung erfolgt**. Diese **Maßnahmen** werden **erforderlichenfalls überprüft** und **aktualisiert**."

Auszug aus Artikel 25 der VERORDNUNG (EU) 2016/679:

> „(1) Unter **Berücksichtigung des Stands der Technik**, der **Implementierungskosten** und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der **unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen** trifft der **Verantwortliche** sowohl zum **Zeitpunkt der Festlegung der Mittel für die Verarbeitung** als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** — wie z. B. Pseudonymisierung — trifft, **die dafür ausgelegt sind**, die **Datenschutzgrundsätze** wie etwa Datenminimierung **wirksam umzusetzen** und die **notwendigen Garantien in die Verarbeitung aufzunehmen**, um den **Anforderungen dieser Verordnung zu genügen** und die **Rechte der betroffenen Personen zu schützen**."
>
> „(2) Der **Verantwortliche trifft geeignete technische und organisatorische Maßnahmen**, die **sicherstellen**, dass **durch Voreinstellung** grundsätzlich **nur personenbezogene Daten**, deren **Verarbeitung** für **den jeweiligen bestimmten Verarbeitungszweck** erforderlich ist, **verarbeitet werden**. Diese Verpflicht**ung gilt für die Menge der erhobenen personenbezogenen Daten**, den **Umfang ihrer Verarbeitung**, ihre **Speicherfrist** und ihre **Zugänglichkeit**. Solche **Maßnahmen müssen insbesondere sicherstellen**, dass **personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden**."

Was bedeutet dies nun für die tägliche Arbeit?

Das kommt drauf an! Soll heißen, dass die Auswirkungen der doch sehr unglücklich formulierten Verordnung nicht vorhersehbar sind.

Manche neigen dazu, dies als gelernter Österreich „**locker und entspannt**" **zu sehen**, andere wiederum dürften hier über „**das Ziel hinausschießen**" und eine **zu strenge Auslegung vornehmen**.

Die „**Wahrheit**" wird wohl **irgendwo dazwischen** liegen, wobei **zu beachten** ist, dass es sich hier **um ein Grundrecht handelt** und die Einhaltung solcher von der Europäischen Union innerhalb der EU sehr ernst genommen wird.

Eine **entscheidende Rolle** werden die **Aufsichtsbehörden** einnehmen, denn diese sind mit dem **Vollzug des Datenschutzes** betraut. In diesem Zusammenhang wird auch **die Zukunft zeigen**, ob und **wie intensiv die Aufsichtsbehörden angerufen** werden, sei es von betroffenen Personen laut DSGVO-Wording oder durch deren Vertreter (Datenschützer, Rechtsanwälte usw.) und **wie mit den gewonnen Erkenntnissen umgegangen** wird.

Es wäre sehr **wünschenswert**, wenn solche **Erkenntnisse zur Verbesserung des Datenschutzes verwendet** würden **und nicht zum Aufbau eines Geschäftsmodelles** zur **Erlangung möglichst hoher Schadenersatzzahlungen**.

Natürlich ist an dieser Stelle anzumerken, dass **bewusste bzw. schwere Verstöße** gegen den Datenschutz **geahndet werden** müssen und **verursachte Schäden wiedergutzumachen** sind.

Der **Datenschutz bzw. die Umsetzung** dessen ist **keine neue Reglung**. Diese **gibt es schon sehr lange**, nur haben sich nicht alle in der **Intensität damit beschäftigt** wie dies nun **durch die DSGVO ausgelöst** wurde. **Viele Vorgaben** sind in **Österreich** nicht neu und schon **lange geltendes Recht**.

Auf **keinen Fall zu unterschätzten** sind die **Sanktionen und Strafen**, die Aufsichtsbehörden verhängen können, denn diese können nicht nur **finanziell schmerzhaft** sein, sondern sie können auch zur **Untersagung der Datenverarbeitung** führen. Dies würde im **Zeitalter der Digitalisierung** wohl einer, wenn **auch (nur) temporären, „Schließung des Betriebes“** gleichkommen. Was es für **Auswirkungen** haben kann, wenn ein **Kunde einen Auftrag erteilen möchte** (bzw. eine **Beratung wünscht**) und **Sie dann KEINE Daten verarbeiten dürfen,** kann **jeder selbst für sein Unternehmen abschätzen**.

Bei Personen, die beispielsweise als **Datenschutzbeauftragte für einen Verantwortlichen** tätig sind, kann es dennoch passieren, dass sich **im Falle einer Bestrafung des Verantwortlichen** dieser **beim Datenschutzbeauftragten regressieren** wird. Dies kann durch eine **Schadenersatzforderung** in der **Höhe der bezahlten Strafe** sowie etwaiger anderer **Vermögensschäden** (Verfahrenskosten, Betriebsausfallskosten usw.) passieren. Nicht zu vergessen ist, dass sich der **Geschäftsführer/-leiter unter Umständen verpflichtet** sieht, eine **solche Forderung geltend zu machen**, um nicht selbst in die Haftung zu kommen.

Der **Abschluss einer Versicherung für Strafen** wird als **sittenwidrig** angesehen, zumindest **wenn es sich um Vorsatzdelikte handelt**. **Versicherbar** sind hingegen **Schadenersatzforderungen**, die ein („bestrafter“) Verantwortlicher beispielsweise beim Datenschutzbeauftragten gelten macht – zum Bespiel im Rahmen der **D&O-Versicherung** oder einer **Haftpflichtversicherung für Datenschutzbeauftragte**.

Was sagt die zuständige EU-Kommissarin Věra Jourová dazu?

„Selbst ich könnte die Regeln der DSGVO umsetzen", wird Věra Jourová, die Hüterin des europäischen Datenschutzes, in einem Interview mit der Zeit Online zitiert (https://www.zeit.de/digital/datenschutz/2018-05/vera-jourova-eu-kommissarin-datenschutz-grundverordnung-dsgvo/seite-2).

Besonders interessant ist **folgender Passus** im Interview:

> **ZEIT ONLINE:** Die großen Konzerne können einfach einen Anwalt anrufen, um die DSGVO umzusetzen. Aber kleinere Betreiber, gerade Blogger und Vereine, haben oft nicht das Geld und wissen nicht, wie sie alle Kriterien umsetzen sollen.
>
> **Jourová:** Die sollen mir eine E-Mail schicken.
>
> **ZEIT ONLINE:** Wir werden das genauso veröffentlichen.
>
> **Jourová:** Ja, ja. Machen Sie das. Ich werde ihnen raten, dass sie sich auf ihren gesunden Menschenverstand verlassen sollen.

Wenn Sie nun dem Vorschlag der **EU-Kommissarin** folgen und eine **E-Mail an sie** senden möchten, teilen wir gerne die entsprechende **E-Mail-Adresse** mit: vera-jourova-contact@ec.europa.eu.

Haben Sie keine Scheu und teilen Sie den für die DSGVO zuständigen Personen Ihre Erfahrungen mit den neuen Datenschutzbestimmungen mit.

Conclusio!

Lassen Sie sich nicht durch verschiedene Berichte und Meldungen aus der Ruhe bringen, machen Sie Ihre Hausaufgaben und wenn die Behörde klingelt, ist es allemal ratsam, mit dieser zu kooperieren, um mögliche Verbesserungspotentiale optimal umzusetzen.

Mit freundlichen Grüßen,

René Hompasz
Höher Insurance Services GmbH

Zum Autor:

René Hompasz ist Geschäftsführender Gesellschafter der Höher Insurance Services GmbH (diese ist seit mehr als 20 Jahren im Bereich der Vermögensschaden-Haftpflichtversicherung tätig), ist seit 1994 in der Finanz- und Versicherungsbranche, hat den Lehrberuf Versicherungskaufmann erfolgreich abgeschlossen, war im Back Office einer österreichischen Versicherungsgesellschaft tätig, wechselte nach einigen Jahren in den Vertrieb und begann im Anschluss daran seine selbständige Tätigkeit als Versicherungsmakler, wobei das Dienstleistungsangebot sukzessive um die Gewerbliche Vermögensberatung, die Wertpapierberatung als Wertpapierdienstleistungsunternehmen sowie die Unternehmensberatung erweitert wurde. Zudem ist er allgemein beeideter und gerichtlich zertifizierter Sachverständiger für das Versicherungswesen.