Datenschutz-Webinar vom 13. November 2017

Die gestellten Fragen und die Antworten der Expertin Frau Mag. Ursula Illibauer

Webinar-Rückblick: https://www.wko.at/branchen/industrie/datenschutz-webinar.html

1. **Wie hat der Mustertext für die Einwilligungserklärung für die Empfänger von Newslettern zu lauten?**
   Mustertext ist zu finden unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html
   „Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich … (die Datenarten genau aufzählen, z.B. „Name", „Adresse" etc.) zum Zweck der … (genaue Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte der Firma …") bei der Firma NN gespeichert werden. Diese Einwilligung kann jederzeit bei … (Angabe der entsprechenden Kontaktdaten) widerrufen werden."

2. **Sind Fotos ohne Namen ebenfalls betroffene Daten?**
   Ja, wenn eine Person erkennbar ist, ist das ein personenbezogener Datensatz und datenschutzrechtlich relevant. **ACHTUNG**: das ist auch urheberrechtlich relevant! Das Recht am eigenen Bild ist im Urheberrechtsgesetz verankert. Wenn Sie die Bilder von z.B. Mitarbeitern im Internet oder Intranet verwenden wollen, benötigen Sie die Einwilligung der Mitarbeiter.

3. **Wie sind denn Visitenkarten handzuhaben? Diese sind ja auch eine Sammlung personenbezogener Daten.**
   Sobald man eine organisierte und systematische Aufbewahrung hat, ist dem die Qualität als Dateisystem zuzusprechen und fällt damit in den Anwendungsbereich der DSGVO. Sie müssen alle Prinzipien einhalten. Wenn man die Visitenkarte persönlich erhalten hat, kann man wohl aber davon ausgehen, dass man damit die schlüssige Zustimmung des Betroffenen hat, die Daten abzuspeichern.

4. **Frage zur Definition von personenbezogenen Daten: Firmen, wie GesmbH usw., sind ja davon ausgenommen. Wie sieht es mit Ansprechpartnern bei einem solchen Unternehmen aus, z.B. Durchwahl, Firmen, E-Mail-Adresse. Fallen die mit rein oder nicht?**
   Die Daten juristischer Personen, wie GmbH und AG, würden nicht unter die DSGVO fallen, jedenfalls aber die Daten der dahinterstehenden natürlichen Personen, diese Daten sind also datenschutzrechtlich relevant. Bei den juristischen Personen ist noch nicht gänzlich klar, wie der österreichische Gesetzgeber das tatsächlich handhaben wird, da im nationalen Datenschutz-Anpassungsgesetz 2018 grundsätzlich auch juristische Personen angesprochen wurden. Das ist noch in Schwebe.

5. **Ein Datenschutzkoordinator ist nach Recherchen auch möglich. Es MUSS kein Datenschutzbeauftragter sein. Darf der Koordinator auch ein IT-Leiter sein?**
Das ist teilweise richtig. Wenn man einen Datenschutzbeauftragten zwingend bestellen muss, weil die Kerntätigkeit eine umfangreiche Datenverarbeitung von sensiblen, von strafrechtlich relevanten Daten oder eine systematische Überwachung nach sich zieht, muss man einen Datenschutzbeauftragten bestellen. Man kann aber zusätzlich auch einen Koordinator bestellen. Wenn man freiwillig einen Zuständigen im Betrieb für den Bereich „Datenschutz" bestellt, wird geraten, dass man ihn nur als Datenschutzkoordinator benennt. Auch der freiwillig bestellte Datenschutzbeauftragte hätte nämlich alle gesetzlichen Rechte und Pflichten eines solchen. Handelt es sich nur um einen Datenschutzkoordinator oder „eine spezifische Person, die für Datenschutz zuständig ist" (so könnte man ihn auch benennen), dann hat er einfach nur die Rechte, die ihm vom Unternehmen zugestanden werden. Es ist im Übrigen auch ratsam, eine Person zu benennen, die für datenschutzrechtliche Fragen verantwortlich und zuständig ist. Das ist aber natürlich dennoch eine freiwillige Entscheidung.

6. **Gibt es Einstufungen oder Beispiele für die Risikokategorien bei Folgeabschätzung?**
Die bis dato gültige Standard- und Musteranwendungsverordnung, in der die Ausnahmen von der Meldeverpflichtung bei der Datenschutzbehörde bzw. Datenverarbeitungsregister verankert waren, entfällt mit Mai 2018. Aber die Datenschutzbehörde hat für diese Fälle zugesichert, dass sie mittels Black- and White-Lists, also Positiv- und Negativlisten, bestimmte Fälle vorsehen wird, in denen ein hohes Datenschutzrisiko erreicht wird oder eben nicht. Diese Listen werden als Verordnung herausgegeben, in der festhalten wird, wann eine Datenschutzfolgenabschätzung eben aufgrund der Risikoabschätzung notwendig ist. Das heißt, es wird solche Abschätzungen direkt von der Datenschutzbehörde geben. Der Inhalt ist noch nicht bekannt. Die Datenschutzbehörde hat in Aussicht gestellt, dass diese Listen bis Ende dieses Jahres in Begutachtung gehen.

7. **Müssen kleine Unternehmen, die einem Konzern angehören, ein Verarbeitungsverzeichnis erstellen?**
Achtung: Verarbeitungsverzeichnisse müssen alle Unternehmen erstellen, da gibt es keine Ausnahmen. Die sogenannte KMU-Ausnahme gilt theoretisch nur für Unternehmen, die Daten gelegentlich verarbeiten. Man hat meistens z.B. eine Kundendatenbank oder Mitarbeiterdatenbank, damit ist der Tatbestand des gelegentlichen Verarbeitens nicht mehr erfüllt und die Ausnahme entfällt. Diese Ausnahme war eigentlich gut gemeint und als KMU-Ausnahme für Betriebe unter 250 Mitarbeiter gedacht, ist allerdings in der Umsetzung misslungen. Gehen Sie davon aus, jedenfalls ein Verarbeitungsverzeichnis zu brauchen.

8. **Wie ist der Widerspruch zwischen Mailprotokollierung und Löschung zu lösen?**
Man sollte alle datenschutzrelevanten Vorgänge im Unternehmen protokollieren. Man hat bei dieser Protokollierung keine weitere Datenbank zu befüllen. Man protokolliert nicht z.B. der Herr XY hat mir jenes E-Mail geschickt mit jenem Inhalt, sondern man protokolliert nach Kategorien und nicht die konkreten Fälle. Daher gibt es nicht wirklich einen Widerspruch. Bei gesetzlichen Aufbewahrungspflichten geht die gesetzliche Regelung dem individuellen Löschungsantrag vor.

9. **Private Mails sind nicht erlaubt, aber ich kann ja nicht ausschließen, dass trotzdem welche empfangen werden.**
Private E-Mails sind in Unternehmen oft nicht erlaubt, ausgenommen sind oft Notsituationen. Private E-Mails sind sofort an die private E-Mail-Adresse zu schicken oder sind zu löschen. **Achtung für Arbeitgeber:** Wenn private E-Mails von z.B. ehemaligen Mitarbeitern auftauchen, dann sollten diese nicht gelesen werden.

10. **Gibt es auch weiterhin eine Mitwirkungspflicht des Betroffenen bei Auskunftsbegehren und beginnt in diesem Fall die Frist wieder von vorne?**
Die Betroffenenrechte sind möglichst ohne Aufwand des jeweiligen Betroffenen abzuwickeln. Wenn man nicht feststellen kann, wer der Betroffene ist, z.B. wenn die Aufforderung von einer Phantasie-E-Mail-Adresse kam, dann sollte man nach einem Identitätsnachweis fragen, um feststellen zu können, ob denn das wirklich der Berechtigte selbst ist, der hier nachfragt. Die DSGVO konkretisiert diesen Fall nicht, es kann vermutet werden, dass die Frist erst mit der sicheren Feststellung der Identität zu laufen beginnt.

11. **Kann ich konzernübergreifende Vereinbarungen treffen, dass Daten zu bestimmten Zwecken ausgetauscht werden dürfen und dann ist das damit legitimiert?**
Man darf konzernübergreifende Vereinbarungen treffen. Diese Vereinbarung legitimiert aber nicht schlechthin. Man muss im Einzelfall beurteilen, ob die Verarbeitung im Konzern zulässig ist, also warum und wozu man die Daten in dieser Weise verarbeitet. Handelt es sich z.B. um ein zentral gelagertes Personalverwaltungssystem, könnte man argumentieren, dass das Interesse des Konzerns, dieses Verwaltungstool auch entsprechend ordentlich und zweckmäßig befüllen zu können, höherwertiger ist als das Interesse der Mitarbeiter an einer Nicht-Weitergabe der Daten. Man muss sich aber jede Vereinbarung einzeln ansehen. Wenn man aber z.B. nur eine Vereinbarung geschlossen hat, dass man alle Daten weltweit im Konzern austauschen darf ohne bestimmten Zweck, dann scheint dies nicht argumentierbar zu sein, weil die Rechtfertigungsgrundlage fehlt. Der Zweck muss ersichtlich sein. Binding Corporate Rules decken nur das Recht, Daten in ein Drittland zu schicken, ohne zusätzliche Erfordernisse. Das klärt die grundsätzliche Zulässigkeitsfrage der Datenverarbeitung noch nicht.

12. Gibt es Auflistungen, welche Security-Vorfälle gemeldet werden müssen?
Nein, aber es gibt Leitlinien von der sogenannten Art. 29-Gruppe. Das ist ein Beratungsgremium auf europäischer Ebene, welches aus Datenschutzexperten der Datenschutzbehörden der Mitgliedstaaten besteht. Diese Leitlinien geben Rahmenbedingungen vor, wann ein solcher Vorfall vorliegen könnte und wann nicht. Leider sind diese Leitlinien im konkreten Fall nicht genug aussagekräftig. Grundsätzlich kann sehr schnell ein Datenleck vorliegen und ist auch schnell mit einem Risiko für die betroffenen Personen, deren Daten verarbeitet wurden, verbunden. Wenn man Verschlüsselungssysteme oder Pseudonymisierungssysteme anwendet und somit das Risiko selbst im Fall eines Datenlecks stark minimiert, dann schaut es besser aus. Eine solche Liste wäre auch nicht aufschlussreich, da man nicht alle denkbaren Vorfälle berücksichtigen kann. Anwendungsbeispiele finden Sie aber z.B. unter www.it-safe.at. Gleichzeitig (und umso wichtiger) mit Tipps, wie man Vorfälle vermeiden kann.

13. Bedeutet die Deckelung mit max. 20 Mio. € auch wenn 4 % Umsatz mehr als 20 Mio. € ausmacht?
Wenn die 4 % Umsatz höher sind als die 20 Mio. €, dann wird der höhere Betrag schlagend werden und umgekehrt ebenso. Dies sind jedoch die Höchststrafen. Es gibt keine Mindeststrafen in der Verordnung und auch nicht im Datenschutzgesetz. Datenschutz wird aber „wichtiger genommen" und werden die Strafen sicher angesichts des tatsächlichen Vorfalles „angemessener weh tun" als bisher.

14. Datenschutzbeauftragter: Wer in einer Firma darf das ausüben, wie ist das geregelt, haftet der dann oder die Geschäftsführung weiterhin?
Datenschutzbeauftragter kann auch ein interner Mitarbeiter sein, prinzipiell auch ein Mitarbeiter der IT-Abteilung. Unklar ist, ob dies auch der Leiter der IT-Abteilung sein dürfte. In Deutschland war dies in der Vergangenheit nicht möglich, ob diese Sichtweise auch in Österreich geteilt wird ist, nicht klar, da in Österreich auch die Unternehmensstruktur eine andere ist als in Deutschland. Grundsätzlich sollte sich dieser Mitarbeiter im Datenschutz auskennen und sollte über entsprechendes Know-How verfügen. Er sollte auch eine gewisse Einflussnahme im Unternehmen haben, um Empfehlungen wirksam abgeben zu können und berichtet der höchsten Managementebene direkt.

Der Datenschutzbeauftragte kann aber auch ein externer Experte sein, z.B. ein Unternehmensberater, ein Rechtsanwalt oder ein IT-Dienstleister, mit dem ein entsprechender Auftragsverarbeitervertrag (früher: Dienstleistungsvertrag) geschlossen wird. Wichtig ist, dass dieser externe Beauftragte eine entsprechende Expertise hat.

Die Haftung (Strafe) geht nicht auf diesen Datenschutzbeauftragten über, er haftet nur im Ausmaß seiner Sorgfaltspflichten. Er ist lediglich beratend im Betrieb tätig, er

ist nicht derjenige, der die Entscheidungen trifft. Denjenigen, der die Entscheidungen trifft, den trifft auch die Strafe.

15. **Gibt es bereits Standardvertragsklauseln in der neuen DSGVO?**
Ja, es gibt bestehende Standardvertragsklauseln, die Muster der Europäischen Kommission sind bei der Datenschutzbehörde abrufbar, diese sind aber noch nicht an die neue DSGVO angepasst.

16. **Was mache ich mit Bewerbungsunterlagen? Darf ich diese jetzt nicht mehr in Evidenz nehmen bzw. wie lange darf ich diese in Evidenz nehmen? Ich möchte mir ja schließlich den "Pool" an potentiellen Mitarbeitern erhalten …**
Bewerberdaten kann man prinzipiell so lange in Evidenz halten, wie man sie braucht. Hier wird wohl die sechsmonatige Frist aus dem Gleichbehandlungsgesetz schlagend werden. Für den Fall eines Gleichbehandlungsprozesses sind sechs Monate zu berücksichtigen. Jede Aufbewahrungsfrist, die darüber hinausgeht, muss im Einzelfall argumentiert werden. Es kann z.B. eine Zustimmung des Bewerbers eingeholt werden. **Aber Achtung:** Schweigen gilt hier nicht als Zustimmung.

17. **Wie schaut es mit Speicherungen in Clouds aus?**
Speicherungen in Cloud-Systemen sind Auftragsverarbeitungen. Auftragsverarbeiter sind Dienstleister, denen Sie die Daten anvertrauen, die Daten für Sie hostet oder eben speichert oder damit eine gewisse Rechenleistung zur Verfügung stellt. Das heißt aber auch, man bleibt der Verantwortliche für die Daten, der Auftragsverarbeiter stellt nur eine entsprechende Dienstleistung zur Verfügung. Es ist zu beachten, dass dieser Auftragsverarbeiter Datensicherheitsmaßnahmen implementiert hat. Zertifizierungen, Gütezeichen oder -siegel können ein Hinweis dazu sein. Weiters ist ein schriftlicher Vertrag mit diesem Auftragsverarbeiter zu schließen, das sind z.B. Nutzungsbedingungen, die nun erweitert um die neuen datenschutzrechtlichen Notwendigkeiten werden. Viele große Anbieter stellen ihre Nutzungsbedingungen bereits auf die neue DSGVO um. Bei Zweifel sollte man im konkreten Anlassfall direkt nachfragen.

18. **Wenn kein Datenschutzbeauftragter notwendig ist und eine beliebige Person sich um den Datenschutz kümmert, unterliegt diese Person auch den Einschränkungen: weisungsungebunden, unbefangen, kein Abhängigkeitsverhältnis …? Oder darf das wirklich jeder prinzipiell geeignete Mitarbeiter machen?**
Wenn man einen Datenschutzkoordinator ernennt, setzt man selbst die Bedingungen und Vorgaben fest. Dieser Datenschutzkoordinator muss nicht alle Bestimmungen eines Datenschutzbeauftragten einhalten. Jedoch sollte diese Person ein gewisses datenschutzrechtliches Know-How haben.

19. **Inwieweit wirkt diese Verordnung rückwirkend? Muss ich beispielsweise meine E-Mails von vor 10 Jahren durcharbeiten?**
    Grundsätzlich sind auch diese Daten vom Datenschutz erfasst, wenn Sie die Daten auch nach dem 25. Mai 2018 in irgendeiner Art und Weise verarbeiten (speichern, bearbeiten, weiterleiten, löschen, …). Bevor man versucht, diese Datenverarbeitungen rechtskonform an die DSGVO anzupassen, sollte man sich überlegen, ob man diese Daten wirklich noch verwendet und braucht. Sollte diese Frage verneint werden, ist es besser, diese Daten auch zu löschen (schon nach geltendem Recht).

20. **Kann für Daten, die ich schon bisher verarbeitet habe, die Zustimmung/Einwilligung der Betroffenen angenommen werden? Oder muss ich für allen bisherigen Datenbestand neu eine Einwilligung einholen?**
    Wenn die Datenverarbeitung auf einer Zustimmung der Betroffenen basiert, d.h. Sie haben irgendwann eine Zustimmung eingeholt, dann ist davon auszugehen, dass diese auch DSGVO-konform ausgestaltet war (da auch jetzt sehr strenge Anforderungen an die Einwilligung bestehen) und diese fortgelten. Wenn Sie keine Zustimmung erhalten hatten und auch sonst keinen Rechtmäßigkeitsgrund für die Datenverarbeitung nachweisen können (überwiegendes berechtigtes Interesse, für die Vertragserfüllung notwendig, Gesetz schreibt die Datenverarbeitung vor, siehe auch: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html), dann müssen Sie eine Einwilligung nachträglich einholen. Im Übrigen wäre diese Datenverarbeitung leider aber dann auch schon nach geltendem Datenschutzrecht unzulässig.

Für weitere Fragen steht Ihnen die Bundessparte Industrie gerne zur Verfügung:

Mag. Hagen Pleile
Tel: 05 90 900 - 3214
E-Mail: hagen.pleile@wko.at

Die Informationsseite der Wirtschaftskammer Österreich mit allen Informationen, Mustern und Ansprechpartnern: www.wko.at/datenschutz