MME

eHealth

Auswirkungen der neuen EU-Datenschutz-Grundverordnung auf Schweizer Datenverarbeiter

23. März 2017

Dr. Martin Eckert
martin.eckert@mme.ch

Ausgangslage: DSGVO

Die neue Datenschutzgrundverordnung („DSGVO“) ist am 24. Mai 2016 in Kraft getreten. Sie gilt einheitlich für alle EU-Länder und verschärft das Schutzniveau der bisherigen der in der EU geltenden nationalen Datenschutzgesetze.

Nach einer Übergangsfrist von zwei Jahren wird die neue Verordnung ab 25. Mai 2018 für alle Mitgliedsstaaten verbindlich.

Der schweizerische Gesetzgeber zieht nach. Der Entwurf zum neuen Datenschutzgesetz (VE DSG) ist in der Vernehmlassung.

Was gilt für CH-Unternehmen?

Die neue Datenschutzgrundverordnung gilt nicht nur in der EU, sondern hat extraterritoriale Wirkung (Niederlassungsprinzip und Marktortprinzip).

- **Niederlassungsprinzip**: Die DSGVO gilt zunächst nach Art. 3 Abs. 1 (DSGVO) für jegliche Datenverarbeitung im Rahmen von Aktivitäten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union. Entscheidend ist hier der Ort der Niederlassung, nicht der Ort der Datenverarbeitung.

Art. 3 – EU-DSGVO – Räumlicher Anwendungsbereich

1. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

Was gilt für CH-Unternehmen?

- CH-Unternehmen muss einen **Vertreter in der EU** benennen (Art. 27 Abs. 1 DSGVO).
- **Marktortprinzip**: (Art. 3 Abs. 2 DSGVO). DSGVO gilt auch für Unternehmen oder Auftragsverarbeiter mit Niederlassung ausserhalb der EU, also auch Unternehmen in der Schweiz, wenn Daten von Personen, die sich in der Union befinden, verarbeitet werden.
- Extraterritoriale Anwendung: Gilt zum einen für Datenverarbeitung, falls z.B. Kunden in der EU Waren oder Dienstleistungen angeboten werden (eine Zahlung ist hierbei unerheblich), aber auch für Datenverarbeitungen und Anwendungen, die bloss der Beobachtung von betroffenen Personen in der EU dienen.

DSGVO: besondere Daten

Die Verarbeitung folgender Daten ist gem. Art. 9 DSGVO untersagt (mit Ausnahmenkatalog):

- Daten aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen
- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben
- Sexuelle Orientierung

Spezielle Regeln:

- Kinder (16 Jahre; Zustimmung)
- Profiling
- Daten über strafrechtliche Verurteilung

Was ist neu?

Die DSGVO führt zahlreiche neue Pflichten für Unternehmen ein:

- Meldepflichten bei Datenschutzverletzungen (möglichst binnen 72 Stunden) an die zuständige Aufsichtsbehörde (Art. 33 DSGVO); damit wird das Risiko von Reputationsschäden signifikant erhöht; Benachrichtigung der betroffenen Personen bei hohem Risiko von Persönlichkeitsverletzungen

Art.33 – EU-DSGVO – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.
2. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.
3. Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:
a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
4. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
5. Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

Was ist neu?

- Benennung eines internen oder externen Datenschutzbeauftragter (Art. 37 DSGVO) mit Dokumentations- und Nachweispflichten

Art.37 – EU-DSGVO – Benennung eines Datenschutzbeauftragten

1. Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
2. Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.
3. Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.
4. In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.
5. Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
6. Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
7. Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Was ist neu?

- Datenschutz durch Technikgestaltung (Privacy by Design; Art. 25 Abs. 1 DSGVO) und datenschutz-freundliche Voreinstellungen (Privacy by Default; Art. 25 Abs. 2 DSGVO)

Art.25 – EU-DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

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 Verpflichtung 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 ist neu?

- Big Data: Pflicht zur vorgängigen Durchführung einer Datenschutz-Folgenabschätzung (Data Protection Impact Assessment; Art. 35 DSGVO)

Art.35 – EU-DSGVO – Datenschutz-Folgenabschätzung

1. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.
2. Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.
3. Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:
a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;
4. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.
5. Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlichb ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.
6. Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.
7. Die Folgenabschätzung enthält zumindest Folgendes:
a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen
8. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.
9. Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.
10. Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.
11. Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Was ist neu?

- Koppelungsverbot bei Einwilligung (Art. 7 Abs. 4 DSGVO)

Art. 7 – EU-DSGVO – Einwilligung

4. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, **ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.**

Was ist neu?

- Ausbau der Rechte der betroffenen Personen (Kunden)
  - Recht auf Transparenz
  - Informationspflichten der Verantwortlichen
  - Auskunftsrecht
  - Recht auf Berichtigung und Löschung
  - Recht auf Einschränkung der Verarbeitung
  - Recht auf Datenübertragbarkeit
  - Widerspruchsrecht (gegen Profiling; automatisierte Entscheidfindung)

Was ist neu?

- Auslagerung von der Datenverarbeitung (Auftragsverarbeitung) nur auf der Grundlage eines Vertrages (Standardvertragsklauseln) bei hinreichenden Garantien des Auftragsverarbeiters (z.B. Datenschutzsiegel; Art. 28 Abs. 1 DSGVO)

Art.28 – EU-DSGVO – Auftragsverarbeiter

1. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Was ist neu?

- Keine Unter-Auftragsverarbeitung (Sub-Sub-Akkordanten) ohne schriftliche Genehmigung des Verantwortlichen (Art. 28 Abs. 2 DSGVO)

Art.28 – EU-DSGVO – Auftragsverarbeiter

2. Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Was ist neu?

- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Art.20 – EU-DSGVO – Recht auf Datenübertragbarkeit

1. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

2. Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

3. Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

4. Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Was ist neu?

Die EU meint es ernst:

Die zivilrechtliche Haftung wird verschärft, insbesondere für Auftragsdatenverarbeiter.

Es werden harte Strafen eingeführt. Unternehmen müssen mit Bussgeldern bis zu 4% ihres globalen Jahresumsatzes rechnen, natürliche Personen mit Geldbussen von bis zu 20 Mio. EUR.

Es gibt auch positive Neuerungen:

- Erleichterter Datenschutz im Konzern mit einem gemeinsamen Datenschutzbeauftragen für die Unternehmensgruppe (Art. 37 Abs. 2 DSGVO) und „Verbindlichen internen Datenschutzvorschriften“ (**Binding corporate rules**: Art. 47 DSGVO)
- Private Datenschutzzertifizierung (**Datenschutzsiegel** und Datenschutzprüfzeichen; Art. 42 DSGVO)
- **Einheitlichkeit** des Datenschutzes in der EU: Vorrang der DSGVO vor Rechtsvorschriften der Mitgliedsstaaten; Sicherstellung der einheitlichen Anwendung der DSGVO durch den Europäischen Datenschutzausschuss
- **Recht auf Vergessenwerden** (Art. 17 DSGVO)

Was gilt es vorzukehren?

Massnahme 1 (sofort):

- Der Datenschutz gehört auf die Agenda des **Verwaltungsrates**.

- Datenschutz ist ein Compliance-Thema das im Unternehmen angemessen adressiert und dokumentiert werden muss (risikobasierter Ansatz).

Was gilt es vorzukehren?

Massnahme 2 (2017):

- Wir empfehlen bereits heute die Bezeichnung eines externen oder internen **Datenschutzbeauftragten**.
- Dieser Datenschutzbeauftragte sollte eine Prüfung der möglichen Relevanz der neuen EU DSGVO für das eigene Unternehmen durchführen (Risikoprüfung).
- Notwendig ist insbesondere eine Analyse, ob und in welchem Umfang personenbezogene Daten gesammelt und verarbeitet werden, um EU Bürgern Waren oder Dienstleistungen anzubieten oder um deren Verhalten zu beobachten.

Was gilt es vorzukehren?

Massnahme 3 (2017):

- Nicht im Sinne des vorauseilenden Gehorsams, sondern im Sinn von vorausschauendem Handeln sollten sich CH-Unternehmen schon heute darauf einstellen, dass der neue Datenschutzstandard der EU auch in der Schweiz in die Gesetzgebung einfliessen wird. Durch die extraterritoriale Anwendung der EU DSGVO wird dies bei globalen Unternehmen eine Implementierung von Massnahmen in vielen Drittstaaten erfordern.

Welche Privaten Organisationen sind verpflichtet einen Datenschutzbeauftragten zu benennen?

- Organisationen, deren Kerntätigkeit die systematische Überwachung von Personen umfasst (bspw. Google, verhaltensorientierte Internetwerbung, Geolokalisierungsdienste, Überwachung von Besucherverhalten, gewisse Fälle von Direktmarketing, ad tracking, personalisierte Werbung, Kunden oder Patientenprofile, je nach Produkten kommen auch Versicherungen oder Banken in Frage; zusammenfassend, sämtliche überwachende Tätigkeiten)

Welche Privaten Organisationen sind verpflichtet einen Datenschutzbeauftragten zu benennen?

- Organisationen, deren Kerntätigkeit die Verarbeitung spezifischer Datenkategorien (z.B. Gesundheit oder Religion) umfasst (bspw. Spitäler, Pharmakonzerne, gewisse Forschungsinstitute, Laboratorien, Marktforschungsunternehmen, welche personenbezogene Daten verarbeiten wie bspw. politische Einstellungen)

Keinen Datenschutzbeauftragten müssen Unternehmen benennen, wenn deren Datenverarbeitung nicht Teil ihrer Kerntätigkeit ist. In diesem Fall müssen Unternehmen jedoch beweisen können, dass diese Verarbeitungen nicht zu ihrer Kerntätigkeit gehören.

Was sind die Aufgaben eines Datenschutzbeauftragten?

- Beratung bei der Einhaltung der EU-DSGVO sowie die Durchführung von Schulungen und internen Audits
- Kontaktperson sowohl für die Aufsichtsbehörde als auch für die betreffenden Mitarbeiter
- Führung - ausgenommen bei gewissen (kleinen) Unternehmen - ein Verzeichnis aller Datenverarbeitungstätigkeiten und hält darin alle Organisationsabläufe fest, welche die Verarbeitung von personenbezogenen Daten betreffen. Dieses Verzeichnis enthält u.a. den Zweck und die Voraussetzungen der Verarbeitung und wird der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt.

Wen kann man als Datenschutzbeauftragten benennen?

- keine spezifischen Anforderungen.
- Der Beauftragte sollte ein Experte im Bereich Datenschutz sein. Dementsprechend sollte der Datenschutzbeauftragte solide Erfahrung im Bereich Datenschutz, Datensicherheit und Geschäftsprozesse haben und darüber hinaus gut über die relevanten Aspekte der Organisation informiert sein.
- **Interne Lösung**, sofern kein Interessenskonflikt (Governance). Beispielsweise kann ein Datenverantwortlicher nicht als Datenschutzbeauftragter benannt werden, der bereits für viele Datenverarbeitungsvorgänge verantwortlich ist.

Wen kann man als Datenschutzbeauftragten benennen?

- Externer Datenschutzbeauftragter: Nach der neuen Verordnung dürfen auch externe Datenschutzbeauftragte benannt werden. Dies ist eine prüfenswerte Lösung für KMUs und Organisationen mit wenig Datenschutz-Know-how. Diese Aufgabe kann von Datenschutz-Rechtsanwälten oder Spezialisten erfüllt werden.

Exkurs: ePrivacy Verordnung

- Am 10. Januar 2017: Offizieller Vorschlag der Europäischen Kommission für die neue ePrivacy Verordnung
- Inkrafttreten: Zusammen mit DSGVO im Mai 2018
- Im Gegensatz zur alten ePrivacy-Richtlinie: Unmittelbare Anwendbarkeit in allen Mitgliedstaaten bzw. Vorrang gegenüber nationalen Gesetzen

- Verschärfung Datenschutz für Websitebetreiber

Vorschlag ePrivacy Verordnung

- **Grundprinzip: Opt-in**

- **Ungenügend:**
- Allein der Besuch einer Website durch den Endverbraucher stellt noch keine Einwilligung in eine gesonderte Datenverarbeitung dar
- Heute gebräuchliche Banner unzulässig: „Mit dem Besuch dieser Website akzeptieren sie (konkludent) die Verwendung von Cookies“ oder „Wir benutzen Cookies“ und einem OK-Button
- Allein der Hinweis, dass der betroffene Nutzer im Browser bestimmte Datenschutzeinstellungen vornehmen kann, genügt nicht

Vorschlag ePrivacy Verordnung

- **Ausreichend:**
- Beim ersten Aufruf der Website, noch vor der ersten Platzierung eines einwilligungsbedürftigen Cookies, muss ein Hinweis auf deren Verwendung dargestellt werden, bei dem der Nutzer die Wahl hat, dem zuzustimmen oder es abzulehnen
- Die Darstellung kann durch ein Banner oder ein Hinweisfenster erfolgen, das nicht übersehen werden kann
- Der Nutzer muss zur Zustimmung unzweideutig selbst auf „Zustimmen“ klicken (sog. «Opt-in»)
- Ohne Zustimmung dürfen, dürfen keine einwilligungsbedürftigen Cookies eingesetzt werden

Vorschlag ePrivacy Verordnung

- Websitebetreiber muss den Nutzern eine Option zum späteren Widerruf der Einwilligung, anbieten (sog. «Opt-out»)
- Websitebetreiber sollten auch die Browsereinstellung „Do Not Track“ von jedem Nutzer abfragen. Ist „Do Not Track“ aktiviert, so hat dies als Nichteinwilligung des Nutzers zu gelten

Vorschlag ePrivacy Verordnung: Fazit

- Nicht unerheblicher Aufwand zur Anpassung der Websites
- Website-Monitoring: Sehr genaues Abwägen, welche Datenerhebungen einer Nutzereinwilligung bedürfen, wird nötig

Fragen?

Dr. Martin Eckert
Legal Partner

martin.eckert@mme.ch
T +41 44 254 99 66
Zurich | Zug

- Breite Erfahrung bei der umfassenden Beratung von international orientierten Technologie- und Handelsunternehmen (inklusive M&A)
- Fachliche Schwerpunkte: IT-, IP-, Datenschutz- und Technologierecht, Telekommunikationssektor und Hightechbranchen (u.a. Medizinaltechnik)
- Anerkannter Experte in zahlreichen grossen und komplexen IT Outsourcing–Projekten von Banken und Versicherungen (vgl. Legal 500)
- Führt wirtschaftsrechtliche Prozesse (Handelsgerichtsprozesse und Schiedsverfahren)
- Ehemaliger Obergerichtssekretär am Handelsgericht Zürich
- Verwaltungsratstätigkeit (Bank, IT, Medizinaltechnik); Dozententätigkeit an der HWZ Hochschule for Wirtschaft Zürich (CAS Digital Risk Management)
- Akkreditierter Datenschutzgutachter bei ePrivacyseal GmbH
- Treasurer World IT Lawyers; ehem. Richter an der Eidg. Rekurskommission für Geistiges Eigentum

LEGAL500.COM
MME – Legal | Tax | Compliance regularly advises on IT law and data protection and is particularly experienced in IT outsourcing projects in the banking sector. Martin Eckert's 'legal and negotiation skills are superb'.

WHOSWHOLEGAL.COM
At MME Martin Eckert is 'top notch'. As former judge at the Swiss Federal Appeal Commission for Intellectual Property, he has a 'wealth of knowledge' and is respected in the field.

MME

Office Zurich
Kreuzstrasse 42
P.O. Box 1412
CH-8032 Zurich
T +41 44 254 99 66
F +41 44 254 99 60

Office Zug
Gubelstrasse 11
P.O. Box 7613
CH-6302 Zug
T +41 41 726 99 66
F +41 41 726 99 60

www.mme.ch
office@mme.ch