10 Schritte zur Datenschutz-Compliance

Fit für den 25.5.2018

Die EU-Datenschutz-Grundverordnung (DSGVO) ist zwar bereits seit 24. Mai 2016 in Geltung, wird aber faktisch erst zwei Jahre nach diesem Datum anwendbar. Über diesen Zeitpunkt hinaus ist keine weitere „Gnadenfrist“ mehr vorgesehen. Höchste Zeit also, die Neuerungen im Datenschutzrecht in die eigene Datenschutz-Compliance zu integrieren!

Foto: freepik.com

Künftig werden die Unternehmen für die Einhaltung der Pflichten aus der DSGVO, insbesondere für deren Umsetzung in ihren Organisationen verstärkt Eigenverantwortung übernehmen müssen. Um diese Eigenverantwortung durchzusetzen und der DSGVO entsprechend normatives Gewicht zu verleihen, enthält die DSGVO schwerwiegende Sanktionen: Es drohen Geldstrafen von bis zu 20 Millionen Euro oder bis zu 4 % des globalen Konzernumsatzes, je nachdem, welcher der Beträge höher ist (Art 83 Abs 4 DSGVO).

Diese Strafbestimmungen sind ohne weitere „Schonfrist" ab 25.5.2018 voll anwendbar.

Was ist neu im Datenschutzrecht?

Folgende Neuerungen kommen auf Verantwortliche und Auftragsverarbeiter zu:

- Erweiterte und neue Betroffenenrechte
- Verpflichtung zum Datenschutz durch Technik („Privacy by Design and by Default")
- Gemeinsame Verantwortliche („joint controllers")
- Dienstleisterverträge
- Verfahrensverzeichnis statt Datenverarbeitungsregister
- Informationspflicht beim Datenmissbrauch
- Die Datenschutzfolgenabschätzung
- Der Datenschutzbeauftragte
- Regelung des internationalen Datenverkehrs
- Strafen

1. BETROFFENENRECHTE

Hinsichtlich der Betroffenenrechte stehen deutlich aufwändigere Informationspflichten als bisher gegenüber den Betroffenen ins Haus. Dies gilt sowohl schon bei der Datenerhebung als auch beim Erhalt oder der Weitergabe von Daten. Das Recht auf Auskunft, Richtigstellung und Löschung umfasst künftig auch die Auskunft über die Speicherdauer und muss binnen eines Monats umgesetzt werden.

Zudem wurde ein Recht auf Vergessen niedergeschrieben sowie die Verpflichtung all jene, denen Daten weiterübermittelt wurden, über die Richtigstellung, Löschung oder Einschränkung der Datenverarbeitung zu informieren.

Das Recht auf „Datenmobilität" wird wohl einen erheblichen Investitionsbedarf nach sich ziehen. Denn die Betroffenen erhalten das Recht, ihre Daten vom Auftraggeber herauszuverlangen und zwar in einer strukturierten Form und einem üblichen maschinenlesbaren Format. Soweit dies technisch möglich ist, kann der Betroffene auch verlangen, dass der Auftraggeber diese Daten direkt an einen anderen Auftraggeber überträgt.

2. DATENSCHUTZ DURCH TECHNIK (ART 25 DSGVO)

Die Verpflichtung zum Datenschutz durch Technik umfasst im Wesentlichen zwei Gruppen von (technischen und organisatorischen) Maßnahmen: Privacy by Design (Gestaltung der Datenverarbeitung) und Privacy by Default (Datenschutzrechtliche Voreinstellung).

Durch Privacy by Design soll sichergestellt werden (durch technische und organisatorische Maßnahmen), dass nur so viele Daten verarbeitet werden, wie für die Zweckerreichung erforderlich sind. Dazu sollen Verantwortliche „interne Strategien und Maßnahmen" festlegen: z.B. Minimierung der Verarbeitung personenbezogener Daten, Pseudonymisierung personenbezogener Daten, Transparenz bezüglich Funktion und Verarbeitung personenbezogener Daten u.a.

Diese Verpflichtung besteht sowohl im Zeitpunkt, in dem die Mittel für die Datenverarbeitung festgelegt werden, als auch während der Datenverwendung selbst. Sie unterliegt jedoch einer Verhältnismäßigkeitsabwägung, wobei auch die Implementierungskosten eine maßgebliche Rolle spielen.

Die Pflicht zu datenschutzfreundlichen Voreinstellungen (Privacy by Default) umfasst 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.

Die Verpflichtung zur Privacy by Default sieht keine Verhältnismäßigkeitsprüfung vor, ist also unabhängig von den Kosten, Risiken oder anderen Faktoren umzusetzen.

Da die Pflicht zu datenschutzfreundlichen Voreinstellungen unbeschränkt auch für bestehende Systeme gilt, ist zu empfehlen, so früh als möglich zu prüfen, was diese Pflicht für die eigenen Produkte und Dienstleistungen bedeutet:

- Umsetzung (Versehen der Anwendungen mit datenschutzfreundlichen Voreinstellungen) im Zuge laufender Updates
- Vereinbarungen mit Zulieferern treffen (möglichst frühzeitig)

Zum Nachweis der Erfüllung des Datenschutzes durch Technik sind Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen vorgesehen (Art 42f DSGVO).

3. SOLIDARHAFTUNG DER GEMEINSAMEN VERANTWORTLICHEN

Wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und Mittel der Datenverarbeitung festlegen (gemeinsame Verantwortliche), trifft sie die Verpflichtung, die Umstände ihrer Zusammenarbeit in transparenter Art und Weise vertraglich festzulegen. Dabei müssen insbesondere die Umstände der Zusammenarbeit hinsichtlich der Betroffenenrechte und der Informationspflichten geregelt werden.

4. DIENSTLEISTUNGS-VERTRAGSMANAGEMENT

Wie schon bisher regelt auch die DSGVO die Zusammenarbeit mit Dienstleistern. Auch künftig muss zwischen dem Auftraggeber und dem Dienstleister ein Dienstleistervertrag geschlossen werden. In Anbetracht der drohenden Strafen von bis zu 10 Millionen Euro oder bis zu 2 % des konzernweiten Jahresumsatzes ist es angezeigt, dass Auftraggeber hinkünftig ein genaues Dienstleister-Vertragsmanagement betreiben.

5. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Das bisherige Datenverarbeitungsregister wird durch ein „Verfahrensverzeichnis“ (Art 30 DSGVO) ersetzt. Das Führen des Verfahrensverzeichnisses trifft nicht nur Auftraggeber sondern auch Dienstleister.

Das Verfahrensverzeichnis hat (wie bisher schon das Datenverarbeitungsregister) folgende Informationen zu enthalten:

- die eigenen Kontaktdaten
- die Zwecke der Datenverwendung
- eine Beschreibung der in der Datenanwendung enthaltenen Datenkategorien
- eine Beschreibung der in der Datenanwendung enthaltenen Empfängerkategorien
- Datentransfers in Drittstaaten (separat ausgewiesen)
- NEU: die geplante Speicherdauer (wenn möglich)
- eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

Diese Vorschriften gelten nicht für Unternehmen mit weniger als 250 Mitarbeitern, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt und die Datenverarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besonders sensibler Daten (Daten zu rassischer oder ethnischer Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Verarbeitung genetischer oder biometrischer Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung) oder über strafrechtliche Verurteilungen und Strafdaten einschließt.

6. INFORMATIONSPFLICHTEN BEIM DATENMISSBRAUCH (ART 33, 34 DSVGO)

„Data Breaches“ – also der Verlust der vollständigen Kontrolle über die Daten bzw. was mit diesen Daten passiert – sind bei Verletzungen des Schutzes von personenbezogenen Daten der Aufsichtsbehörde unverzüglich (möglichst binnen 72 Stunden) nach Bekanntwerden der Verletzung zu melden.

Wenn die Verletzung ein hohes Risiko für die persönlichen Freiheiten und Rechte der betroffenen natürlichen Personen zur Folge hat – z.B. einen physischen, materiellen oder immateriellen Schaden – so sind auch die Betroffenen vom Auftraggeber unverzüglich von der Verletzung zu verständigen.

7. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Mit Art 35 DSGVO wurde eine völlig neue Verpflichtung zur Abschätzung der möglichen Folgen einer Datenverarbeitung eingeführt. Die Datenschutz-Folgenabschätzung („Data Protection Impact Assessment) ist insbesondere dann durchzuführen, wenn bei der Datenverarbeitung neue Technologien verwendet werden und diese im Hinblick auf ihre Art, Anwendungsbereich, Kontext und Zwecke möglicherweise ein hohes Risiko für die Privatsphäre der Betroffenen zur Folge haben. Dies ist etwa der Fall bei systematischer und extensiver Auswertung von persönlichen Aspekten (insb. durch Profiling), bei der Verarbeitung von sensiblen Daten oder bei der Verarbeitung von strafrechtlich relevanten Daten. Auch erfasst ist die „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“ (lit c).

Beachtlich ist, dass die Verpflichtung zur Datenschutz-Folgenabschätzung unabhängig von der Unternehmensgröße (keine Ausnahmen für KMU) ist und sich nur aus dem Inhalt der Verarbeitung ergibt.

Die Folgenabschätzung umfasst insbesondere eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck, eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen. Diese inkludieren 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 wird.

Das Ergebnis der Datenschutz-Folgenabschätzung kann zudem eine Konsultation mit der Datenschutzbehörde erforderlich machen (Art 35 Abs 2 DSGVO), nämlich wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein

hohes Risiko zur Folge hätte, soferne der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Kommt die Aufsichtsbehörde zur Auffassung, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen entsprechende schriftliche Empfehlungen (Weisungen). Somit kann sie ihre Befugnisse (Untersuchungsbefugnisse, Abhilfebefugnisse, Genehmigungsbefugnisse und Beratungsbefugnisse) entsprechend ausüben.

8. DER DATENSCHUTZBEAUFTRAGTE (ART 37 DSGVO)

Neu ist auch die Verpflichtung einen Datenschutzbeauftragten einzusetzen, der über besondere Fähigkeiten und Kenntnisse auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis verfügt.

Ein Datenschutzbeauftragter ist dann erforderlich, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird (Ausnahme: Gerichte, die im Rahmen ihrer justiziellen Tätigkeit handeln), 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 die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten (sensible Daten) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und besondere Straftaten besteht.

Diese Pflicht zur Bestellung eines Datenschutzbeauftragten trifft sowohl Auftraggeber als auch Dienstleister.

Die Aufgaben des Datenschutzbeauftragten umfassen insbesondere

- die Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer datenschutzrechtlichen Pflichten
- die Überwachung der Einhaltung der datenschutzrechtlichen Bestimmungen sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- die Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- die Zusammenarbeit mit der Aufsichtsbehörde sowie
- die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation und gegebenenfalls Beratung zu allen sonstigen Fragen.

9. INTERNATIONALER DATENVERKEHR (ART 44FF DSGVO)

Vor dem Hintergrund der Notwendigkeit des „Flusses personenbezogener Daten aus Drittländern“ für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit (EG 101) wurden die Regelungen für den internationalen Datenverkehr inhaltlich etwas erweitert und formal erleichtert.

Erhalten bleibt aber der Grundsatz, dass ein Datentransfer in Drittstaaten außerhalb der EU grundsätzlich verboten ist, soweit nicht eines der Datentransferinstrumente greift. Es besteht jedoch die Möglichkeit, dass die Europäische Kommission feststellt, dass ein Drittstaat ein angemessenes Datenschutzniveau bietet – dann bedarf eine Datenübermittlung keiner weiteren besonderen Genehmigung.

10. STRAFEN

Die Datenschutz-Grundverordnung sieht die Verhängung von Geldbußen von bis zu 20 Millionen Euro oder 4 % des konzernweiten Umsatzes vor, je nachdem, welcher Betrag höher ist. Diese Geldbuße ist von der Aufsichtsbehörde zu verhängen oder zumindest die Verhängung von Geldbußen „in die Wege“ zu leiten, sodass die Geldbußen dann „von den zuständigen nationalen Gerichten verhängt“ werden.

Verfassungsrechtliche Gründe sprechen eher gegen ein Verfahren im Verwaltungs(straf)-rechtsweg, zumal bereits die Höhe der drohenden Geldbußen indiziert, dass die derart strafbewährten Datenschutzbestimmungen in zum „typischen Kernbereich strafbarer Handlungen“ und damit in die Kompetenz der Strafgerichtsbarkeit gehören.

Wie der österreichische Gesetzgeber diese Bestimmung umsetzen wird, ist derzeit noch unklar. Klar ist lediglich, dass er dies effektiv und unter Beachtung des österreichischen Verfassungsrechts bis längstens 25.5.2018 tun muss. ■

Rechtsanwalt
Mag. ANDREAS BAUER
ist Teammitglied in der LGP-Praxis für öffentliches Wirtschaftsrecht. Sein fachlicher Schwerpunkt liegt in den Bereichen Datenschutzrecht, Gewerberecht, Industrie- und Betriebsanlagenrecht, Bau- und Immobilienrecht, Raumordnungsrecht, Infrastrukturrecht, Umwelt und Technikrecht, Verwaltungsstrafrecht sowie Europa- und Verfassungsrecht.

Foto: Raphael Schwarz