EU-Datenschutz-Grundverordnung
Überblick für Ingenieurinnen und Ingenieure

Berlin, 27.03.2018
Rechtsanwalt Karsten U. Bartels LL.M., HK2 Rechtsanwälte

Die folgende Darstellung gibt einen Überblick über die Anforderungen der **Datenschutz-Grundverordnung**[1] (DSGVO). Die Verordnung ist am 25. Mai 2016 in Kraft getreten und gilt nach einer Übergangsfrist von zwei Jahren ab dem 25. Mai 2018 unmittelbar und verbindlich.

Die neuen Regelungen weichen mitunter stark von den bekannten Anforderungen ab, so dass sich vor allem Geschäftsführer, Abteilungsleiter und Datenschutzbeauftragte mit den Grundlagen und Besonderheiten der DSGVO vertraut machen sollten. Die gilt unabhängig von der Größe des **Ingenieurbüros**. Eine Kleinst- oder Kleinunternehmerausnahmeregelung gibt es nicht.

1. Anwendungsbereich der DSGVO

Die DSGVO gilt in allen Mitgliedstaaten der Europäischen Union direkt und löst die bisherigen datenschutzrechtlichen Regelungen, wie in Deutschland das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze, ab. Die nationalen Gesetzgeber haben jedoch aufgrund sogenannter Öffnungsklauseln in bestimmten Bereichen einen gesetzgeberischen Spielraum. Deutschland hat von diesem durch ein **neues Bundesdatenschutzgesetz** (BDSG-neu) Gebrauch gemacht. Im BDSG-neu wird z. B. der Beschäftigtendatenschutz geregelt. Neue Landesdatenschutzgesetze sind zu erwarten, aber derzeit noch nicht von allen Bundesländern verabschiedet.

Der Anwendungsbereich der DSGVO führt zu einer weitreichenden Geltung des Datenschutzrechts, da sich die Verordnung an **alle Verarbeiter personenbezogener Daten von Bürgern der Europäischen Union** richtet. Das bedeutet, dass auch ausländische Unternehmen, die EU-Bürger bewerben, die Regelungen der DSGVO einzuhalten haben.

Eine Verarbeitung personenbezogener Daten ohne Rechtsgrundlage ist nach den Vorschriften der DSGVO verboten (sog. **Generalverbot mit Erlaubnisvorbehalt**). Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine gesetzliche Regelung die Verarbeitung erlaubt, diese gesetzlich vorschreibt oder eine ausdrückliche Einwilligung der betroffenen Personen vorliegt. Zudem können Betriebsvereinbarungen als Rechtsgrundlage dienen. **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das sind neben Namen, Anschriften und E-Mail-Adressen auch Telefondurchwahlnummern, ggf. Fotos, IP-Adressen, Angaben über Nutzungsverhalten, persönliche Eigenschaften und vieles andere mehr. Liegen besondere Kategorien von personenbezogenen Daten nach Art. 9 DSGVO (sog. sensible Daten) vor, sind die datenschutzrechtlichen Anforderungen nochmals gesteigert. Eine **Datenverarbeitung** im Sinne der DSGVO ist jede Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung von personenbezogenen Daten.

Die DSGVO gilt allerdings nicht für anonyme Daten. Bei diesen handelt es sich nicht um personenbezogene Daten im Sinne der Verordnung.

1 eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

2. Gesetzliche Änderungen und Prinzipien der Datenverarbeitung

Ausgangspunkt für die Datenverarbeitung sind die von der Verordnung aufgestellten Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO). Danach müssen personenbezogene Daten

- **rechtmäßig** und für die betroffene Person nachvollziehbar verarbeitet werden;
- für festgelegte, eindeutige und **legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**„Datenminimierung“**);
- **sachlich richtig** und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist und
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete **technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit“).

Besonderes Augenmerk ist dabei zudem auf die neu geschaffene **Rechenschaftspflicht** in Art. 5 Abs. 2 DSGVO zu legen, die Verantwortliche verpflichtet, detailliert nachzuweisen, ob und inwiefern sie die oben genannten Grundsätze der Datenverarbeitung einhalten.

Eine Konkretisierung der dargelegten Grundsätze erfolgt zudem im Rahmen von Art. 25 DSGVO, der die Grundsätze von **privacy by default** und **privacy by design** regelt. Privacy by default bedeutet im Wesentlichen, dass im Falle von Datenverarbeitungsprozessen datenschutzfreundliche Voreinstellung zugunsten der Betroffenen getroffen werden muss. Privacy by design erfordert, dass die Datenschutzprinzipien der DSGVO bereits bei der Gestaltung des Datenverarbeitungsprozesses mitberücksichtigt werden sollen.

3. Betroffenenrechte (Artt. 15 ff. DSGVO)

Die Rechte der Betroffenen sind signifikant ausgeweitet worden. So haben Betroffene beispielsweise das Recht, über den Datenverarbeitungsprozess informiert zu werden, auf die verarbeiteten Daten zugreifen zu können, fehlerhafte Daten berichtigen sowie personenbezogene Daten löschen zu lassen. Außerdem besteht ein erweitertes **Recht des Widerspruchs gegen die Datenverarbeitung**. Auf das Widerspruchsrecht ist spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich, verständlich und getrennt von weiteren Informationen hinzuweisen.

4. Meldepflichten (Artt. 33, 34 DSGVO)

Neu ist die Meldepflicht bei Verletzung des Schutzes personenbezogener Daten, soweit damit ein Risiko für die Rechte der Betroffenen verbunden ist. Dies kann bei einem Hacker-Angriff, aber auch bereits bei Verlust eines Datenträgers vorliegen. In einem solchen Fall soll binnen **72 Stunden** eine Meldung des Vorfalls an die zuständige **Aufsichtsbehörde** erfolgen. Bei voraussichtlich hohen Risiken sind zudem die betroffenen Personen selbst zu informieren.

5. Datenschutzbeauftragter

Weiterhin wurde auch der Kreis der zur Bestellung eines **Datenschutzbeauftragten** (DSB) verpflichteten Unternehmen erweitert. Insbesondere Art. 38 des BDSG-neu regelt die Pflicht für Unternehmen, einen Datenschutzbeauftragten zu benennen, soweit sie in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Ein DSB kann intern oder extern benannt werden. Geschäftsführer und IT-Leiter kommen als DSB nicht in Betracht.

Hilfestellung zur Ermittlung: nach herrschender Meinung kommt es nur auf die Anzahl der Mitarbeiter (**Kopfzahl**) an, nicht auf die Arbeitszeit oder Vollzeitäquivalente. Auch geringfügig Beschäftigte zählen danach als ganze Person. „Automatisierte Verarbeitung“ liegt vor, wenn IT verwendet wird, z. B. PCs, Smartphones, Scanner, Kopierer etc. „Ständig“ bedeutet, dass die betreffende Person in Ausübung ihrer Tätigkeit immer wieder mit der automatisierten Verarbeitung personenbezogener Daten befasst ist.

Diese Anforderungen dürften regelmäßig auf ein Ingenieurbüro mit mehr als neun Mitarbeitern zutreffen. Ergänzend verlangt Art. 37 DSGVO, dass Unternehmen unabhängig von der Anzahl ihrer Angestellten einen DSB zu benennen haben, wenn der Tätigkeit des Unternehmens im Kern die Verarbeitung besonders sensibler Daten oder eine systematischer Überwachung Betroffener zugrunde liegt.

6. Datenschutzerklärung (Artt. 13, 14 DSGVO)

Bisherige Datenschutzerklärungen sind anzupassen und zusätzliche sind zu verwenden: Denn nach Artt. 13 und 14 DSGVO sind künftig sämtliche Betroffene darüber zu informieren, wie mit ihren personenbezogenen Daten umgegangen wird. Dazu gehören z. B. **Kunden, Dienstleister, Mitarbeiter**. Neu ist, dass nicht nur die Zwecke der Datenverarbeitung zu nennen sind, sondern auch die der Datenverarbeitung zugrunde liegende **Rechtsgrundlage** anzugeben ist. Die Datenschutzerklärung muss in allgemeinverständlicher Sprache und transparent formuliert sowie jederzeit abrufbar sein. Der Betroffene muss zum Zeitpunkt der Erhebung der Daten informiert werden.

Auch die Datenschutzerklärungen auf Websites sind entsprechend anzupassen. Sollte es dabei zum Beispiel zum Einsatz von Tracking Tools wie Google Analytics kommen oder liegt ein Formular für Kontaktdaten vor, so ist über die Umstände der Datenverarbeitung zu informieren.

7. Auftragsverarbeitung (Art. 28 DSGVO)

Auch unter der DSGVO ist es für den Verantwortlichen möglich, Daten im Auftrag verarbeiten zu lassen. Eine solche Konstellation liegt vor, wenn Daten ohne Einwilligung der Betroffenen an **Dritter außerhalb des Unternehmens** gegeben werden. Dies kann beispielsweise geschehen, wenn in einem Unternehmen Daten auf **externen Cloud-Speichern** abgelegt werden (z. B. AWS oder Microsoft Azure). Damit die Verarbeitung personenbezogener Daten im Auftrag gesetzlich zulässig ist, ist eine den Anforderungen von Art. 28 DSGVO genügende **Auftragsverarbeitungs-Vereinbarung** zu schließen. Diese sollte Regelungen zu Gegenstand und Dauer der Vereinbarung, Art und Zweck der Verarbeitung und personenbezogener Daten, Rechten und Pflichten des Auftraggebers, Pflichten des Auftragnehmers, Dokumentations- und Mitwirkungspflichten, sowie technischen und organisatorischen Maßnahmen des Auftragnehmers enthalten. Sollten zudem bereits in der Vergangenheit entsprechende Verträge abgeschlossen worden sein, so sind diese an die neuen gesetzlichen Anforderungen anzupassen. Datentransfers in Drittstaaten können auch im Rahmen der DSGVO aufgrund von Einwilligung, sog. Binding Corporate Rules, den **EU-Standardvertragsklauseln** oder eine Zertifizierung unter dem EU-US-Privacy-Shield stattfinden.

Dies ist für die Nutzung von Diensten relevant, die Server in den USA einbinden, wie zum Beispiel Google Docs und GMail, Slack oder unter Umständen Microsoft Office 365. Die Kommission kann zudem bestimmte Sektoren oder internationale Organisation für datenschutzrechtlich sicher erklären. Daher ist zunächst zu prüfen, ob eine solche Angemessenheitsentscheidung der EU-Kommission für das jeweilige Land, in das die Daten übertragen werden sollen, vorliegt.

8. Technische und organisatorische Maßnahmen

Der DSGVO liegt hinsichtlich der Verarbeitung personenbezogener Daten und der Sicherheit der Verarbeitung ein risikobasierter Ansatz zugrunde. Dies erfordert gemäß Art. 32 DSGVO die Implementierung von dem Risiko angemessenen technischen und organisatorischen Maßnahmen (TOM). Dazu ist es erforderlich, dass die verantwortliche Stelle das Risiko der Daten Verarbeitung genau bestimmt und dementsprechend Maßnahmen auswählt. Diese umfassen beispielsweise **Passwortrichtlinien**, die **Verschlüsselung**, Gewährleistung der **Integrität, Verfügbarkeit**, und **Vertraulichkeit** von Daten und Datenverarbeitungssystem sowie den richtigen Umgang mit IT-Sicherheits- und datenschutzbezogenen Vorfällen oder Verlusten und den Zugang zu Datenverarbeitungsanlagen. Erforderlich sind die Auswahl geeigneter Maßnahmen und deren Dokumentation. Die Dokumentation hat alle im Zusammenhang
mit der Datenverarbeitung eingesetzten Maßnahmen zu umfassen.

9. Welche Dokumente sind anzupassen

Zur Umsetzung der neuen gesetzlichen Anforderungen empfehlen wir, einen individuellen Umsetzungsplan zu entwerfen, um sicherzustellen, dass alle elementaren Voraussetzungen der Verordnung erfüllt werden.

Zunächst sind umfangreiche Dokumentationspflichten (bußgeldbewehrt) zu erfüllen und die entsprechenden Datenverarbeitungsprozesse zu dokumentieren. Im Wesentlichen sollten dabei die hier aufgeführten Dokumente angepasst bzw. erstellt werden:

- Verzeichnisse von Verarbeitungstätigkeiten (Verfahrensverzeichnisse)
- Dokumentation der technischen und organisatorischen Maßnahmen
- Dokumentation von Risiken der Datenverarbeitung
- Konzept Data Breach
- Löschkonzept
- Berechtigungskonzept
- Abschluss/Anpassung der Verträge zur Auftragsverarbeitung mit DSGVO-konformer Anlage zu den technischen und organisatorischen Maßnahmen
- Datenschutzerklärung für Mitarbeiter, Kunden und Dienstleister
- Datenschutzerklärung auf der Website
- Verpflichtungserklärung für Mitarbeiter auf die Vertraulichkeit
- Bestellung eines Datenschutzbeauftragten
- Durchführung der Datenschutz-Folgenabschätzung
- Erstellung von Einwilligungstexten

Eine Orientierung bieten die **Kurzpapiere** der Datenschutzkonferenz, welche auf der Seite der Bundesbeauftragten für Datenschutz und Informationsfreiheit unter abrufbar sind.[2] Diese geben die Sicht der deutschen Aufsichtsbehörden wieder. Eine spätere, davon abweichende Auslegung durch den Europäischen Datenschutzausschuss ist möglich.

2 https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Zudem finden sich auf den Websites der Landesdatenschutzaufsichtsbehörden Muster-Formulare, wie z. B. ein Strukturvorschlag für ein Verzeichnis über Verarbeitungstätigkeiten. Dieses kann auf der Seite der Datenschutzaufsichtsbehörde Sachen-Anhalt abgerufen werden. [2]

Eine einheitliche, konsolidierte Darstellung von aufsichtsbehördlichen Empfehlungen oder Mustern gibt es nicht.

10. Bußgelder (Art. 83 DSGVO)

Die zuständigen Aufsichtsbehörden sind künftig befugt, erheblich höhere Bußgelder zu verhängen. Bisher kannte das BDSG eine Höchstgrenze für Bußgelder von EUR 300.000,00. Mit Geltung der DSGVO können nun jedoch Bußgelder in Höhe von **bis zu EUR 20 Millionen** oder **4 % des weltweiten Vorjahresumsatzes** verhängt werden. Es ist das gesetzgeberisch erklärte Ziel der DSGVO, mit den Bußgeldern abzuschrecken. Zwar sind die Aufsichtsbehörden nach wie vor unterausgestattet. Das muss für die eigene Risikobewertung jedoch unbeachtlich bleiben.

Bitte beachten Sie schließlich, dass der Datenschutz und die IT-Sicherheit Bestandteil des von der Geschäftsführung zu besorgenden Risikomanagements ist, für dessen fehlerhaftes Betreiben ein Geschäftsführer auch **persönlich haftet** (§ 43 GmbHG).

3 https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/