ETL | Rechtsanwälte

Umsetzung der
Datenschutz-Grundverordnung

Ein Überblick über die Pflichten, welche **Unternehmen, Vereine und Freiberufler** nach der Datenschutz-Grundverordnung (DSGVO) umsetzen müssen…

Die Datenschutz-Grundverordnung (DSGVO)

Seit dem 25. Mai 2018 gilt in der Europäischen Union die DSGVO. Sie ersetzt das bisherige deutsche Datenschutzrecht sowie die Datenschutzgesetze der übrigen Mitgliedsländer der EU. Es ist zwar am 25. Mai 2018 auch ein neues Bundesdatenschutzgesetz (BDSG) in Kraft getreten. Dies beinhaltet jedoch nur bestimmte Bereiche des Datenschutzrechts, in dem die Mitgliedsstaaten eigene Regelungen zum „Ausfüllen" der DSGVO treffen dürfen, z.B. zum Beschäftigtendatenschutz.

Personenbezogene Daten dürfen seit dem 25. Mai 2018 nach der DSGVO – vereinfacht dargestellt – nur noch in nachfolgenden Konstellationen verarbeitet werden:

- Die Datenverarbeitung ist erforderlich, um Pflichten aus einem ***Vertragsverhältnis*** mit dem Betroffenen zu erfüllen oder sie ist zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage des Betroffenen erfolgen.
- Es liegt eine wirksame ***Einwilligung*** des Betroffenen vor.
- Es gibt eine ***gesetzliche Pflicht*** zur Datenverarbeitung (z.B. eine Aufbewahrungspflicht).
- Die Datenverarbeitung ist erforderlich, um ***lebenswichtige Interessen*** der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Die Datenverarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen der betroffenen Person (oder seine gesetzlich eingeräumten „Datenschutzrechte") überwiegen (Datenverarbeitung auf Basis einer ***Interessenabwägung***).

Umsetzung der Vorgaben aus der DSGVO ist ratsam

Die Hauptgründe für die Verantwortlichen, sich um die Umsetzung der DSGVO kümmern (zu müssen), sind:

- Die DSGVO bringt eine sog. ***Rechenschaftspflicht*** mit sich (vgl. Art. 5 Abs. 2 DSGVO). Aus dieser Regelung ergibt sich, dass der Verantwortliche die Einhaltung der Vorgaben der DSGVO im Falle einer Prüfung durch die Datenschutzbehörden nachweisen muss. Die DSGVO bringt demnach eine Menge Arbeit mit sich.
- DSGVO-Verstöße können von den Aufsichtsbehörden mit ***Bußgeldern von bis zu 20 Millionen Euro*** (oder bis zu 4% des weltweiten Jahresumsatzes) geahndet werden.

- ➡ Die DSGVO ist ***„hartes Compliance-Recht"***. Die Nichteinhaltung kann u.U. zur ***persönlichen Haftung*** von vertretungsberechtigten Personen von Kapitalgesellschaften führen.
- ➡ Neben Kapitalgesellschaften sind auch ***Personengesellschaften, Einzelunternehmer, Vereine*** und ***Freiberufler*** grundsätzlich verpflichtet, die Vorgaben der DSGVO einzuhalten.

Mit Blick auf die ***erheblichen Bußgeldrisiken*** müssen ***Verantwortliche*** schnellstmöglich Risikovorsorge treffen, um das Risiko der (u.U. sogar persönlichen) Haftung wegen Datenschutzverstößen nach der DSGVO auszuschließen oder zumindest zu minimieren.

Welche Änderungen sind relevant?

Die DSGVO bringt einige äußert relevante und arbeitsintensive Änderungen mit sich. Die relevantesten Änderungen sind folgende:

- ➡ Verschärfte ***datenschutzrechtliche Informationspflichten*** (vgl. Art. 13 und Art. 14 DSGVO): Insbesondere müssen Datenschutzhinweise in Verträgen, Formularen und auf Internetseiten sowie für Beschäftigte und Bewerber überarbeitet werden.
- ➡ Alle ***Auftragsdatenverarbeitungsverträge*** müssen überprüft und an die neue Rechtslage angepasst werden.
- ➡ Erfolgen Datenverarbeitungen auf einer ***ausdrücklichen Einwilligung Betroffener*** sind die Einwilligungserklärungen zu prüfen. Einwilligungen, welche nicht die Voraussetzungen der DSGVO einhalten, werden automatisch ab dem 25.05.2018 unwirksam.
- ➡ Grundsätzlich sollte nur ***datenschutzfreundliche Hard- und Software*** („Privacy by Design") mit ***datenschutzfreundlichen Voreinstellungen*** („Privacy by Default") eingesetzt werden (Grundsatz der Datenminimierung). Dies muss zukünftig sowohl bei der Produktentwicklung (insbesondere der Softwareentwicklung) als auch bei der Produktauswahl von IT-Systemen und der Implementierung der IT-Systeme im Betrieb beachtet werden.
- ➡ Bei risikoreichen Datenverarbeitungen müssen vorgelagerte ***Datenschutz-Folgenabschätzungen*** durchgeführt werden (als risikoreiche Datenverarbeitungen nennt die DSGVO z.B. die Verarbeitung besonders sensibler Daten, z. B. Gesundheitsdaten, der Einsatz neuer Technologien, Profiling, die umfangreiche öffentliche).
- ➡ Es müssen ***Konzepte für die Wahrung von Betroffenenrechten*** sowie für die verschärften ***Meldepflichten bei Datenpannen*** gegenüber Betroffenen und Aufsichtsbehörden implementiert werden.
- ➡ Jeder Verantwortliche hat ein sog. ***„Verarbeitungsverzeichnis"*** anzufertigen (welches auch in regelmäßigen Abständen zu prüfen und gegebenenfalls zu aktualisieren ist), in welchem ***sämtliche Verarbeitungsprozesse von personenbezogenen Daten im Unternehmen beschrieben*** werden. Dieses Verzeichnis betrifft sämtliche ganz oder teilweise automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten. Jeder Verantwortliche ist verpflichtet, mit der Aufsichtsbe-

hörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge im Unternehmen anhand dieses Verarbeitungsverzeichnisses kontrolliert werden können (vgl. Art. 30 Abs. 4 DSGVO). In dem ***Verarbeitungsverzeichnis*** sind die folgenden ***Informationen*** anzugeben (vgl. insbesondere Artikel 30 Abs. 1 DSGVO):

- ☞ der ***Name und die Kontaktdaten des Verantwortlichen*** und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, ***des Vertreters*** des Verantwortlichen sowie eines etwaigen ***Datenschutzbeauftragten***;
- ☞ eine ***Beschreibung der Kategorien betroffener Personen*** und der ***Kategorien personenbezogener Daten*** (z.B. Name, Anschrift, E-Mailadresse, Telefonnummer, Bankverbindungen von Kunden und/oder Lieferanten);
- ☞ eine ***Beschreibung des konkreten Verarbeitungsprozesses*** (z.B. erheben, speichern, abfragen, offenlegen von Daten);
- ☞ den ***Zweck*** des konkreten Verarbeitungsprozesses;
- ☞ die ***Rechtsgrundlage*** des jeweiligen Verarbeitungsprozesses;
- ☞ die ***Herkunft bzw. die Quelle*** der Daten;
- ☞ die ***zugriffsberechtigten Personen/Personengruppen*** auf den jeweiligen Verarbeitungsprozess (nach Funktion und ohne namentliche Angabe);
- ☞ die ***Kategorien von Empfängern***, gegenüber denen die personenbezogenen Daten offengelegt werden (z.B. Banken, Versanddienstleister, Sozialversicherungsträger, Finanzämter, unternehmensinterne andere Datenempfänger, Gläubiger bei Lohn-/Gehaltspfändungen, Träger der Betriebsrente, Auftragsverarbeiter, Muttergesellschaft etc.);
- ☞ sofern personenbezogenen Daten an ein ***Drittland*** oder an eine ***internationale Organisation*** übermittelt werden, die Angabe des konkreten Empfängers der Daten sowie das betreffende Drittland oder die internationale Organisation, sowie die Rechtsgrundlage für die Übermittlung (eine Übermittlung in Drittländer erfolgt auch, wenn sich dort der Server befindet oder der Mailversand hierüber abgewickelt wird. Ebenso kann eine Übermittlung in Drittländer vorliegen, wenn Supportdienstleistungen aus diesem erbracht werden);
- ☞ sofern möglich, die vorgesehenen ***Fristen für die Löschung der verschiedenen Datenkategorien*** (z.B. die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personaldaten, Kundendaten etc., vom Verantwortlichen festgelegte Überprüfungs-/Löschungsfristen);

☞ sofern möglich, eine allgemeine ***Beschreibung der technischen und organisatorischen Maßnahmen***, welche zum Schutz der personenbezogenen Daten zu treffen sind (Einzelheiten siehe nachfolgend Erläuterungen);

☞ ***Auftragsverarbeiter*** haben ein gesondertes Verarbeitungsverzeichnis nach Artikel 32 Absatz 2 DSGVO zu führen;

➡ Das Verarbeitungsverzeichnis ist ein wichtiges zentrales datenschutzrechtliches Dokument zur Erfüllung der Rechenschaftspflicht nach Art. 5 Absatz 2 DSGVO. Verstöße durch fehlende oder unvollständige Verarbeitungsverzeichnisse können seit dem 25.05.2018 mit Geldbußen von ***bis zu 10 Millionen EUR*** oder von bis zu ***2% des gesamten weltweit erzielten Jahresumsatzes*** des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist.

Technische und organisatorische Maßnahmen zur Datensicherheit

Im Bereich der Datensicherheit sind ***technische und organisatorische Maßnahmen zur Sicherheit von personenbezogenen Daten*** zu treffen, welche dem ***Stand der Technik*** entsprechen. Die Maßnahmen müssen umfangreicher sein, wenn der Schutzbedarf der Daten hoch oder sehr hoch ist. Grundsätzlich dürfen bei der Wahl der Datensicherheitsmaßnahmen auch die Implementierungskosten berücksichtigt werden.

Es sind folgende ***technischen und organisatorischen Maßnahmen*** zum Schutz von personenbezogenen Daten zu treffen (vgl. insbesondere Artikel 32 DSGVO):

➡ ***Pseudonymisierung*** personenbezogener Daten (z.B. Trennung von Kundenstammdaten und Kundenumsatzdaten, Verwendung von Kunden-, Personalkennziffern statt Namen)

➡ ***Verschlüsselung*** personenbezogener Daten (z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien und bei der elektronischen Übermittlung von personenbezogenen Daten).

➡ ***Gewährleistung der Vertraulichkeit*** der Systeme und Dienste (die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen, beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder zu Dritten, z.B. Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Trennungskontrolle)

➡ ***Gewährleistung der Integrität*** der Systeme und Dienste (Maßnahmen die gewährleisten, dass personenbezogene Daten nicht unbemerkt geändert werden können, z.B. Eingabekontrolle sowie organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen/Revision etc.)

- ***Gewährleistung der Verfügbarkeit*** der Systeme und Dienste (Maßnahmen die sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden. Hierzu zählen u.a.: Verfügbarkeitskontrolle, Auftragskontrolle)

- ***Gewährleistung der Belastbarkeit*** der Systeme und Dienste (Maßnahmen die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben, z.B. Speicher-, Zugriffs- und Leitungskapazitäten)

- ***Wiederherstellung der Verfügbarkeit*** personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall (z.B. Backup-Konzept, Redundante Datenspeicherung, Cloud-Services, Doppelte IT-Infrastruktur, Schatten-Rechenzentrum etc.)

- ***Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung*** der Wirksamkeit der vorgenannten Maßnahmen (z.B. Entwicklung eines Sicherheitskonzepts, Prüfungen des DSB, der IT-Revision, externe Prüfungen, Audits, Zertifizierungen etc.).

- Den vorbenannten Verpflichtungen zur Schaffung einer ordnungsgemäßen Daten- und Informationssicherheit im Unternehmen sowie zur Entwicklung eines zertifizierten Sicherheitskonzeptes kann realistisch gesehen nur mit der ***Implementierung eines aufwendigen und kostspieligen Daten- bzw. Informationssicherheitsmanagementsystems*** nachgekommen werden, welches sich an anerkannten Standards (z.B. ISO 27001, VdS 3473 oder VdS V10010) orientiert. Werden die Kosten für ein zertifiziertes Sicherheitsmanagement gescheut, muss hier im Rahmen des unternehmerischen Risikos ein **risikobasierter Ansatz** verfolgt werden, was gegebenenfalls zu Beanstandungen (und im schlimmsten Fall zu Bußgeldern) der Aufsichtsbehörden führen kann.

Was ist zu tun?

- Identifizierung und Analyse aller datenverarbeitenden Prozesse im Unternehmen
- Überprüfung der Rechtsgrundlagen für die einzelnen datenverarbeitenden Prozesse
- Erstellung eines Verarbeitungsverzeichnisses
- Überarbeitung von Datenschutzerklärungen auf Webseiten und sonstige datenschutzrechtlich relevanten Dokumenten
- Umsetzung der datenschutzrechtlichen Vorgaben in Beschäftigungsverhältnissen samt Bewerberverfahren
- Überarbeitung von Auftragsdatenverarbeitungsverträgen
- Gegebenenfalls Umstellung von Cookie-Infobannern von „Opt-out“ zu „Opt-in“
- Gegebenenfalls Überarbeitung von Einwilligungen für Datenverarbeitungsprozesse
- Gegebenenfalls Durchführung einer Datenschutz-Folgenabschätzung
- Gegebenenfalls Implementierung eines Datenlöschkonzeptes

- Gegebenenfalls Änderung der Soft- und Hardware sowie der jeweiligen Einstellungen im Hinblick auf die Grundsätze der Datenminimierung („*Privacy by Design*“ und „*Privacy by default*“)
- Gegebenenfalls Implementierung bzw. Anpassung von technischen und organisatorische Maßnahmen zur Sicherheit von personenbezogenen Daten (Datensicherheitsmanagement)
- Kontinuierliche Überprüfung, Dokumentierung und gegebenenfalls Verbesserung der Datenschutzprozesse im Unternehmen in regelmäßigen Abständen (von z.B. 6 Monaten)
- Gegebenenfalls Implementierung von Prozessen für die Wahrnehmung von Betroffenenrechten
- Gegebenenfalls Implementierung von Prozessen für die Meldung von Datenschutzverstößen

Unser Konzept zur Umsetzung der Pflichten der DSGVO

Gerne sind wir Ihnen bei der ***Umsetzung der datenschutzrechtlichen Verpflichtungen*** nach der DSGVO sowie der ***kontinuierlichen Überprüfung und Verbesserung der Datenschutzprozesse*** in Ihrem Unternehmen behilflich.

Der ***erste (und ein sehr wichtiger) Schritt*** zur Umsetzung der Pflichten der DSGVO ist eine ***Identifizierung und Analyse der Datenverarbeitungsprozesse im Unternehmen*** und die anschließende Erstellung eines ***rechtskonformes Verarbeitungsverzeichnisses***, in welchem sämtliche datenschutzrelevanten Verarbeitungsprozesse im Unternehmen beschrieben werden.

Um Ihnen die ***Identifikation und die Analyse*** der datenschutzrelevanten Prozesse in Ihrem Unternehmen zu erleichtern, haben wir ein praktikables Konzept entwickelt, welches weitestgehend auf vorgefertigten Musterformularen beruht, um so den ***anwaltlichen Beratungsaufwand für die Umsetzung der Pflichten nach der DSGVO so gering wie möglich*** zu halten.

Ganz ohne ergänzende anwaltliche Beratungsleistungen wird es erfahrungsgemäß allerdings nicht gehen. Der Beratungsaufwand hängt dabei von Ihren ***unternehmensinternen Datenverarbeitungsprozessen***, Ihren ***Fragen bei der Bearbeitung der Musterformulare*** und Ihren ***allgemeinen Fragen zum (neuen) Datenschutzrecht*** ab. Allgemeine Aussagen zu dem entstehenden Beratungsaufwand bei der Umsetzung der Pflichten der DSGVO sind daher leider nicht möglich.

Sofern Sie unsere Kanzlei mit der Beratung bei der Umsetzung der Pflichten nach der DSGVO beauftragen möchten, muss der hier entstehende Beratungsaufwand daher auf der ***Grundlage fairer Stundensätze*** abgerechnet werden.

Sprechen Sie uns einfach, wir erstellen Ihnen gerne ein Angebot.

Ergebnis

Die Umsetzung der DSGVO bringt eine ganze Menge Arbeit für alle Verantwortlichen mit sich. Die grundlegenden Verpflichtungen nach der DSGVO müssen ***bis zum 25. Mai 2018 umgesetzt*** sein. Anderenfalls besteht das ***Risiko empfindlicher Bußgelder*** der Aufsichtsbehörden sowie ***kostenpflichtiger Abmahnungen*** von Wettbewerbern, Verbraucherschutz- und Wettbewerbsvereinen.

Auch bringt die Einhaltung der Verpflichtungen der DSGVO nicht nur ***„einmaligen Umstellungsaufwand“*** mit sich, sondern es müssen ***„Prozesse zur kontinuierlichen Überprüfung und Verbesserung der Datenschutzprozesse“*** geschaffen werden.

Im Ergebnis sollten daher die ***grundlegenden Verpflichtungen nach der DSGVO*** im Unternehmen oder im Verein umgesetzt werden und dann ***kontinuierlich*** an einer Verbesserung der datenschutzrechtlichen Pflichten nach der DSGVO gearbeitet werden.

Für Rückfragen stehen wir Ihnen natürlich gerne zur Verfügung.

Kanzlei

ETL-Rechtsanwälte GmbH (Niederlassung Köln)
Eiler Straße 3 B
51107 Köln
Tel. + 49 (0)221 / 880 40 60
E-Mail: jens.reininghaus@etl.de

Jens Reininghaus
Rechtsanwalt
Fachanwalt für IT-Recht
Fachanwalt für Gewerblichen Rechtsschutz