AGROSecur Newsletter

- Ausgabe 04/2018 -

EU-Datenschutzgrundverordnung (EU-DSGVO) und das neue Bundesdatenschutzgesetz: Was ist ab 25.05.2018 zwingend zu beachten?

Die EU-Datenschutzgrundverordnung (EU-DSGVO) ist derzeit in aller Munde und vor allem Unternehmen, die keinen Onlineshop betreiben oder nicht aktiv unternehmerisch im Internet präsent sind, stellen sich die Frage, inwieweit die Datenschutzgrundverordnung für sie relevant ist und was konkret zu tun ist.

Dieser Beitrag soll einen ersten, nicht abschließenden Überblick hierzu geben. Es wird ausdrücklich darauf hingewiesen, einen spezialisierten Berater für die konkrete Umsetzung hinzuzuziehen.

1. Was ist die EU-Datenschutzgrundverordnung und wann gilt sie?

Die EU-Datenschutzgrundverordnung (EU-DSGVO) ist eine EU-Verordnung, die **in der ganzen EU gilt** und den **Umgang** von Unternehmen **mit personenbezogenen Daten** regelt, um einheitliche Standards herzustellen. Das bisher in Deutschland geltende **Bundesdatenschutzgesetz** wird in diesem Zug **neu gefasst**. Die Verordnung gilt für alle Unternehmen, die in der EU ansässig sind und auch für Unternehmen mit Sitz außerhalb der EU, wenn sie eine Niederlassung in der EU haben oder wenn diese Daten von Personen aus der EU verarbeiten.

Neben der Vereinheitlichung soll das Datenschutzrecht für die jeweiligen Nutzer nachvollziehbarer werden und der Einfluss auf die eigenen Daten soll gestärkt werden.

Die DSGVO, die bereits am 25.05.2016 in Kraft trat und die EU-Mitgliedsstaaten ab dem **25.05.2018** anwenden müssen, betrifft jedes Unternehmen, das **im Internet tätig ist oder personenbezogene Daten nutzt**. Bis zum 25.05.2018 müssen Unternehmen ihre Prozesse an die neuen Datenschutz-Anforderungen anpassen.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. "Identifizierbar" ist eine Person dann, wenn sie direkt oder indirekt, vor allem mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten oder anderen besonderen Merkmalen identifiziert werden kann. Dabei reicht die Möglichkeit der Identifizierung aus. So sind beispielsweise Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtstag, Kontodaten, KFZ-Kennzeichen, Standort, aber auch IP-Adresse, Google Analytics, Plug-Ins, Facebook Like Button, Cookies usw. personenbezogene Daten nach dem Datenschutzrecht.

Autorin:
Rechtsanwältin Kristin Maryska
Maryska Rechtsanwälte

Paul-Geipel-Straße 1
08371 Glauchau

T: +49 3763/ 5039002
+49 3763/ 6495149
F: +49 3763/ 6495150

www.recht-extern.de

Praktisch relevant ist vor allem die Auftragsdatenverarbeitung. Diese liegt vor, wenn ein Betrieb zwar personenbezogene Daten für seine Zwecke nutzt, die tatsächliche Verarbeitung und Aufbereitung dieser Daten aber nicht selbst durchführt, sondern dies von einem Dienstleister vornehmen lässt. Das ist bereits dann der Fall, wenn ein Steuerberater eingeschaltet wird, der für den Betrieb Steuererklärungen erstellt. Hier bleibt der Betrieb trotz Einschaltung eines Dienstleisters auch weiterhin für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Es besteht eine gemeinschaftliche Haftung von Betrieb und Dienstleister.

2. Welche Neuregelungen gelten konkret?

Neu ist nicht alles, denn viele schon bestehende Verpflichtungen gelten weiter (z. B. dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten ist, es sei denn, es besteht eine Erlaubnis). Datensparsamkeit, Zweckbindung, Datenrichtigkeit wurden erstmalig festgeschrieben (z. B. Grundsatz der Datensicherheit).

Daneben gibt es einige ganz neue Prinzipien, die es zu beachten gilt. Die nachfolgende Übersicht gibt einen nicht abschließenden Überblick über die relevanten Anforderungen:

- Pflicht zur **Führung eines Verzeichnisses** aller Datenverarbeitungstätigkeiten (z. B. Zweck der Datenerhebung, erfasste Personen, technische Abläufe)
- **Dokumentationspflichten** und **Datenschutzfolgenabschätzung**
- **Neue** Anforderungen an **Einwilligungserklärungen** zur Verarbeitung der Daten (nicht nur online; Betroffener muss eindeutig zustimmen, d. h. keine vorangekreuzten Kästchen, zweckgebunden, freiwillig, Dokumentation, vergleichbar einfacher Widerruf für die Zukunft wie Erteilbarkeit, Einwilligung von Minderjährigen unter 16 nur bei Einverständnis der Eltern)
- Zusätzliche Vorgaben für **Datenschutzerklärungen** auf Webseiten/Homepages
- Pflicht zur **Datenportabilität** (Nutzer können verlangen, ihre personenbezogenen Daten in einem `gängigen Format´ an einen anderen Verantwortlichen weiterzugeben, wichtig z. B. bei Wechsel Bank, Arbeitgeber, (soziales) Netzwerk
- **„Recht auf Vergessenwerden“** von Nutzerdaten (Löschungspflicht der gesammelten Daten, wenn der Betroffene es verlangt oder die Daten für die beabsichtigten Zwecke nicht mehr benötigt werden oder der Betroffene seine erteilte Einwilligung widerruft oder die Datenerhebung unrechtmäßig war; erstmals niedergeschriebene Regelung; Dokumentation der Datenerhebungen, Löschungen und aller zusammenhängenden Vorgänge gegenüber jeder Stelle, die personenbezogene Daten verarbeitet)
- Änderungen bei der **Auftragsdatenverarbeitung** und **Mitarbeiterdaten** (Mitarbeiter i. d. S. sind z. B. auch Azubis, Leiharbeiter und Bewerber; Erhebung und Verarbeitung der Daten muss erforderlich sein; Einwilligung freiwillig und grundsätzlich in Schriftform, d. h. selbst unterschrieben; jederzeit widerruflich, Dokumentationspflicht, Informationspflicht bei Verstößen, Löschungspflicht usw. des Arbeitgebers, Beweislast

Autorin:
Rechtsanwältin Kristin Maryska
Maryska Rechtsanwälte

Paul-Geipel-Straße 1
08371 Glauchau

T: +49 3763/ 5039002
+49 3763/ 6495149
F: +49 3763/ 6495150

www.recht-extern.de

des Arbeitgebers vor Gericht, auch immaterielle Schäden einklagbar; Vereinbarungen mit Geschäftspartnern, die Zugriff auf Mitarbeiterdaten haben, sollten kontrolliert werden)

- Umgang mit personenbezogenen Daten von **Kindern**
- Prinzip des **„One-Stop-Shops“** (für Online-Händler: EU-Bürger können sich bei Beschwerden immer an ihre eigene Datenschutzbehörde in ihrem Land wenden)
- Funktion des **Datenschutzbeauftragten** (nötig, wenn besondere Kategorien von Daten nach der DSGVO verarbeitet werden oder "Kerntätigkeit" des Unternehmens eine "umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen" betrifft oder mehr als 9 Personen (als Angestellte oder Mitarbeiter) mit der automatisierten Verarbeitung personenbezogener Daten befasst sind; freiwilliger Datenschutzbeauftragter jederzeit möglich; jetzt auch ohne Schriftform möglich; interner Datenschutzbeauftragter muss „erforderliche Fachkunde“ haben und darf nicht die Geschäftsleitung oder Leitung der IT sein
- **Vertraulichkeit:** Zutrittskontrolle (Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren); Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können; Zugriffskontrolle: Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, Trennungskontrolle: Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können
- **Integrität**

  Weitergabekontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist;

  Eingabekontrolle/Verarbeitungskontrolle: Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme ein-gegeben, verändert oder entfernt worden sind; Dokumentationskontrolle: Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können;

  Auftragskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können;

  Verfügbarkeitskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

Autorin:
Rechtsanwältin Kristin Maryska
Maryska Rechtsanwälte

Paul-Geipel-Straße 1
08371 Glauchau

T: +49 3763/ 5039002
+49 3763/ 6495149
F: +49 3763/ 6495150

www.recht-extern.de

- **Belastbarkeit:** Maßnahmen, die gewährleisten, dass technische Systeme bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden. Daten müssen so gesichert werden, dass sie bei einem eventuellen Verlust wiederhergestellt werden können
- Meldepflicht bei **Datenpannen**
- **Rechenschaftspflicht:** Auf Aufforderung müssen Datenverantwortliche die Einhaltung aller Datenschutzprinzipien gegenüber der zuständigen Aufsichtsbehörde nachweisen können
- Weitere Haftung und **höhere Bußgelder** (bisher nach Bundesdatenschutzgesetz bei Bußgeld in Höhe von 50.000 Euro bzw. maximal 300.000 Euro für sehr schwere und vor allem dauerhafte Verstöße; jetzt Bußgelder von bis zu 20 Mio. Euro oder 4 % des weltweiten Vorjahresumsatzes)

Praxishinweis:

Sinnvoll ist eine Analyse der betrieblichen Abläufe, um Klarheit darüber zu bekommen, welche Bereiche und Schnittstellen im Unternehmen betroffen sind. Da Fehler auf der eigenen Homepage am schnellsten und einfachsten zu finden sind, sollten diese unbedingt überarbeitet und angepasst werden, um Abmahnungen zu vermeiden. Hier wird es wichtig sein, die technischen Abläufe umzustellen und neue Einverständniserklärungen einzufordern sowie diese zu dokumentieren. Nahezu alle Datenschutzerklärungen auf Webseiten müssen mit Geltung der DSGVO neu erstellt oder überarbeitet werden!

Auch wenn kein eigener Datenschutzbeauftragter notwendig sein sollte, bietet sich ein externer Datenschutzbeauftragter an, der die Anforderungen im Unternehmen umsetzt und kontrolliert. In diesem Fall sollten unbedingt die Verträge mit externen Dienstleistern kontrolliert werden.

Insbesondere sollten alle Unternehmen prüfen (nicht abschließend!):

- Wurde bei den Einwilligungen, die von Kunden und anderen Personen für die Verarbeitung personenbezogener Daten eingeholt wurden, auf ein jederzeitiges Widerrufsrecht hingewiesen? Falls nicht, muss dies nachgeholt werden.
- Werden besonders umfangreich Daten verarbeitet oder werden hierfür besondere Technologien eingesetzt, die die Rechte der betroffenen Person besonders gefährden? In diesem Fall ist eine Risikobewertung im Rahmen einer Datenschutzfolgenabschätzung notwendig.
- Sind mit IT-Dienstleistern Vereinbarungen zur Auftragsverarbeitung geschlossen worden? Falls ja, müssen diese überprüft werden: Genügen die Maßnahmen bei dem Dienstleister den Anforderungen?
- Gibt es einen festes Vorgehen hinsichtlich Einholung, Dokumentation von Einwilligungen und Umgang mit Widersprüchen?
- Wie und von wem werden Auskunftsersuchen beantwortet?
- Wie werden Verletzungen von Datenschutzrechten („Datenpannen“/IT-Sicherheitsvorfälle) innerbetrieblich behandelt?

Autorin:
Rechtsanwältin Kristin Maryska
Maryska Rechtsanwälte

Paul-Geipel-Straße 1
08371 Glauchau

T: +49 3763/ 5039002
+49 3763/ 6495149
F: +49 3763/ 6495150

www.recht-extern.de