EU-Datenschutz-Grundverordnung (DS-GVO):

Jeder verarbeitet personenbezogene Daten

Im Mai dieses Jahres treten europaweit neue Regelungen des Datenschutzes in Kraft. Dies ist die umfassendste Reform seit dem Bundesdatenschutzgesetz (BDSG) von 1990. Ab dem **25. Mai 2018** muss DS-GVO in allen EU-Staaten, also auch in Deutschland, umgesetzt werden. Sie dient der EU-weiten Vereinheitlichung der Verarbeitung von personenbezogenen Daten in Unternehmen und Verwaltungen. Im vergangenen Sommer wurde vom Bundestag und -rat zusätzlich das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU - auch BDSG neu) beschlossen. Dieses am 30. Juni 2017 beschlossene, neue Bundesdatenschutzgesetz tritt ebenfalls am 25. Mai 2018 in Kraft. Durch dieses Gesetz wird nur geregelt, was durch die übergeordnete Verordnung erlaubt ist. Die Landesdatenschutzgesetze verlieren im Mai ihre Gültigkeit.

Einwilligungen

Grundsätzlich dürfen personenbezogene Daten von Unternehmen nur verwendet werden, wenn hierfür eine Erlaubnis vorliegt oder eine gesetzliche Grundlage zur Datenverarbeitung vorhanden ist (Art. 6 Abs. 1 DS-GVO). Gesetzliche Grundlage sind Vertragsabschlüsse, rechtliche Verpflichtungen, lebenswichtige Interessen oder öffentliches Interesse. Dies gab es so auch schon im alten BDSG, und es gilt für alle personenbezogenen Daten, egal ob von Mitarbeitern, Lieferanten oder Kunden. Für die Einwilligung ist keine besondere Form erforderlich, sie sollte aber schriftlich vorliegen, damit sie auch dokumentiert ist. Vorausgefüllte Kästchen (Opt-out) gelten im Onlinebereich nicht als Einwilligung; das Kästchen muss aktiv vom Nutzer ausgefüllt werden (Opt-in). Ein Vertrag sollte zustande kommen, auch wenn die Werbung oder der Newsletter abgelehnt werden (Kopplungsverbot). Bei Minderjährigen unter 16 bzw. je nach Mitgliedsstaat unter 13 Jahren müssen die Erziehungsberechtigten einwilligen. Es besteht jederzeit ein Widerrufsrecht, das so einfach wie die Einwilligung erklärt werden können muss. Informiert werden muss darüber in verständlicher Sprache, und der Hinweis darf nicht im Kleingedruckten versteckt werden.

Auch von Mitarbeitern müssen Einwilligungen vorliegen. Hier sollte besonders sensibel vorgegangen werden, da ein Abhängigkeitsverhältnis besteht. Einwilligungen müssen freiwillig gegeben werden. Auch hier besteht das Widerrufsrecht.

Sollten Sie verschiedene Leistungen für Ihre Kunden erbringen, wie z. B. Verkauf, Reparatur, Änderung, ... muss jedes Mal das Einverständnis zur Werbung separat gegeben werden. Es besteht das Gebot der Zweckbindung. Daten, die Sie z. B. zur Rechnungsstellung erhalten haben, dürfen Sie ohne explizite Erlaubnis nicht für Werbung benutzen.

Mitteilungspflicht

Verstärkt wird künftig neben der Rechtmäßigkeit die **Datensparsamkeit** (also nur notwendige Daten zu erheben), die **Transparenz** und **Integrität** sowie die **Vertraulichkeit**. Auch wird die Rechenschaftspflicht ausgeweitet. Es gab laut § 34 BDSG ein Auskunftsrecht über die gespeicherten Daten. In der neuen DS-GVO (Art. 15 Abs 1) findet sich nun eine Liste, welche Informationen Fragenden mitgeteilt werden müssen.

- Werden überhaupt personenbezogene Daten verarbeitet?
- Wenn ja, welche genau?
- Verarbeitungszwecke müssen genannt werden - **neu**
- Kategorien der personenbezogenen Daten müssen genannt werden - **neu**
- Mögliche Datenempfänger müssen genannt werden
- Die geplante Speicherdauer muss genannt werden - **neu**
- Es müssen Informationen über die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie das Widerspruchsrecht nach Art. 21 DS-GVO gegeben werden - **neu**
- Zwingend ist die Information über das Beschwerderecht bei den Aufsichtsbehörden. EU-weit kann sich jeder an die nationale Datenschutzbehörde wenden - **neu**
- Falls die Daten nicht von der betroffenen Person zur Verfügung gestellt wurden, muss ihr die Quelle der Informationen genannt werden - **neu**
- Sollten die Daten automatisiert nach bestimmten Kriterien geordnet werden - Profiling - muss darüber informiert werden - **neu**

Diese Informationen müssen schriftlich, elektronisch oder mündlich gegeben werden (Art. 15 Abs 3 DS-GVO). Die Informationen müssen binnen von vier Wochen übermittelt werden. Eine schriftliche Übermittlung ist sinnvoll, da so die Übermittlung einfach dokumentiert werden kann.

Das alte BDSG enthielt detaillierte Vorschriften, wann Datenverarbeitung legitim und verhältnismäßig ist, ab Mai gelten nur noch die abstrakten Angaben der DS-GVO, was zur **Rechtsunsicherheit** für Unternehmen führt.

Zweckbindung

Verschärft wurde die Zweckbindung der Datennutzung. Personenbezogene Daten dürfen nur zu dem Zweck genutzt werden, zu dem sie erhoben wurden. Es ist künftig also fraglich, ob Kundenvertragsdaten auch für Marketingzwecke genutzt werden dürfen, wenn hierzu keine explizite Erlaubnis vorliegt. Alte Einwilligungen bleiben gültig, Sie müssen aber überprüfen, inwieweit sie dem neuen Recht entsprechen.

Transparenz

Art. 13 und 14 DS-GVO schreiben den Unternehmen höchstmögliche Transparenz vor. Als Unternehmer müssen Sie künftig alle Beteiligten (private und

Was sind personenbezogene Daten?

- Name
- Adressen,
- E-Mail-Adressen,
- Telefonnummern,
- Geburtsdatum,
- Kontodaten,
- Kfz-Kennzeichen,
- Standortdaten,
- IP-Adressen,
- Cookies ...

Also alle Daten, die Rückschlüsse auf die Identität zulassen.

Wo werden personenbezogene Daten genutzt?

Es ist nicht zu unterschätzen, wo überall personenbezogene Daten im Unternehmen genutzt werden. Im ECC-Rechtstipp Nr. 147 /2017 listet Rechtsanwalt Rolf Becker folgende Bereiche - nicht abschließend - auf: Bewerbermanagement, Reisekostenabrechnungssysteme, Schlüsselverwaltung, Zeiterfassungen, E-Mail-Systeme, Lieferantenverwaltung, Lagerverwaltung, Videoüberwachung, Firewall, Social Media, Kundenkartenprogramm, Trackingmaßnahmen, Direktwerbeformen, personalisierte Werbung, Veröffentlichungen von Gewinnern, Teilnehmerlisten, die verteilt werden, etc. Auch inoffizielle „Schubladenlisten" und Excel-Tabellen nutzen personenbezogene Daten. Alle Bereiche müssen dokumentiert werden und in sog. *„Verarbeitungsverzeichnissen"* erfasst werden.

gewerbliche Kunden, Lieferanten, Mitarbeiter) von sich aus umfangreich über alle Einzelheiten der Datenverarbeitung informieren. Sie müssen also auch Ihre Betriebsvereinbarungen überprüfen, ob sie den neuen Anforderungen genügen. Allgemein gehaltene Formulierungen sind künftig angreifbar. Sie sollten z. B. detailliert informieren, ob und wenn in welchem Umfang Sie elektronische Kommunikation überwachen.

Datenpannen

Sollte es zu Datenpannen kommen, z. B., dass Server gehackt wurden, dann muss dies binnen 72 Stunden den Betroffenen mitgeteilt werden, wenn ein hohes Risiko besteht; ebenfalls den Aufsichtsbehörden. Problematisch ist die Risikoabschätzung. Eine Meldung bei den Behörden zieht sicherlich eine Überprüfung nach sich. Fällt diese negativ aus, d. h., wenn das Datenmanagement unzureichend war, drohen Bußgelder.
Bislang mussten nur Datenpannen gemeldet werden, bei denen Bank- oder Gesundheitsdaten betroffen waren, jetzt gilt dies für alle Daten.
Gegen dieses Risiko können Sie sich mit einer **Cyberrisk-Versicherung** schützen.

Nähere Informationen hierzu erhalten Sie von unserem Rahmenabkommenspartner Hemmer und Felder: E-Mail:info@hefe-gmbh.de.

Datenschutzbeauftragte

In Paragraph 38 BDSG neu wurden die bisherigen Vorgaben zur Bestellung eines Datenschutzbeauftragten beibehalten, obwohl die DS-GVO dies nicht vorsieht. Ein Beauftragter - intern oder extern - muss bestellt werden, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind. Wird dies versäumt, drohen Bußgelder.

Recht auf Vergessen

Ebenfalls neu ist das erklärte Recht auf Löschung der Daten. Das Recht auf Vergessen wurde schon 2014 vom Europäischen Gerichtshof postuliert. Art. 17 Abs. 1 der DS-GVO räumt nun Betroffenen ein allgemeines Löschungsrecht ein. Dies gilt nicht nur für Suchmaschinen, sondern gegenüber jedem, der personenbezogene Daten verarbeitet. Dies gilt besonders, wenn der Grund für die Datenverarbeitung entfallen ist oder die Einwilligung widerrufen wurde. Neu ist, dass nicht nur Sie als derjenige, der die Daten erhoben hat, zur Löschung verpflichtet sind. Sie müssen auch dafür sorgen, dass Dritte diese Daten, die sie von Ihnen bekommen haben, löschen.

Datenportabilität

Sollten Sie auf Ihren Internetseiten Blogs, Chats oder eine Kommentarfunktion eingerichtet haben, dann müssen diese Daten für die aktiven Nutzer in einem strukturierten, gängigen und maschinenlesbaren Format ggf. zur Verfügung gestellt werden. Diese sog. Datenportabilität dient dazu, dass Nutzer ihre Profile und Bilder mitnehmen können. Wichtig ist dies auch bei Ihren Mitarbeitern bei einem Arbeitgeberwechsel.

Datensicherheit

Datensicherheit spielt weiterhin eine große Rolle. In Art. 32 der DS-GVO wird zur Sicherheit der Datenverarbeitung aber nicht explizit vorgeschrieben, welche Maßnahmen zu ergreifen sind. Hier sollten Sie sich an den bisherigen Regelungen im BDSG orientieren und an den Stand der Technik jeweils anpassen. Die DS-GVO ist techniklastiger als das BDSG, was sicherlich der zunehmenden Automatisierung geschuldet ist. Hier müssen Sie sicherstellen, dass die Technik alle Vorgaben der Verordnung umsetzt. Die Verantwortung und die Risikobewertung liegt beim Unternehmer.

Werbung

Im alten BDSG wurde in § 28 Abs. 3 Werbung mit Hilfe von personenbezogenen Daten geregelt. Es gab eine Reihe von Ausnahmen von der Einwilligung jedes Einzelnen. Diese Privilegien, das sog. Listenprivileg, entfallen künftig. Sie müssen nun alle Adressen nach Art. 6 Abs. 1 Lit. f im Rahmen einer Interessenabwägung überprüfen, falls Sie keine Einwilligung haben. Direktwerbung z. B. kann ein berechtigtes Interesse sein - Erwägungsgrund 47 der DS-GVO.
Die Einwilligungen, die Ihnen schon vorliegen, behalten ihre Gültigkeit, sofern sie den Vorgaben des BDSG entsprechen - Erwägungsgrund 171 der DS-GVO . § 7 UWG bleibt gültig. Ebenso das Kopplungsverbot.

Kontrollen

Datenschutz ist kein neues Thema, aber bislang waren die Kontrollen nicht so ausgeprägt. Die neuen Regelungen bauen auf den bestehenden auf, verschärfen sie und vor allem wollen die Aufsichtsbehörden in Zukunft viel genauer und systematischer hinschauen, ob die Regeln beachtet werden. Hinzu kommt die drastische Erhöhung der Bußgelder. Sie können bis zu vier Prozent des Weltjahresumsatzes betragen und bewegen sich somit im Bereich von Kartellrechtsstrafen. Künftig müssen Sie der Behörde nachweisen, dass Sie gesetzeskonform gehandelt haben. Hier wurde die Beweislast umgekehrt.

Rahmenabkommen

Wir haben im Januar ein Rahmenabkommen mit Brands Consulting abgeschlossen, das Ihnen bei der gesetzeskonformen Umsetzung der Verordnung hilfreich ist.

Nähere Informationen im Mitgliederbereich unserer Webseite unter Rahmenabkommen.

Mehr Informationen z. B. auch unter https://www.datenschutzbeauftragter-info.de/datenschutzmanagement-nach-der-dsgvo-leitfaden-fuer-die-praxis/

https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/

https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.