Informationsblatt

zur neuen EU-Datenschutz-Grundverordnung (DSGVO)

Ab dem 25.05.2018 gilt in der gesamten EU und darüber hinaus die EU-Datenschutz Grundverordnung (DSGVO). Deutschland kann in einem neuen Bundesdatenschutzgesetz (BDSG) nur noch eigene Regelungen treffen, wenn dies in der DSGVO ausdrücklich vorgesehen ist.

Um überflüssige Risiken zu vermeiden, möchten wir gerne kurz schildern, was es an wesentlichen Neuerungen gibt.

1. Einwilligungen in Telefonwerbung oder E-Mail Marketing

Die DSGVO erhält bei Einwilligungen die bisherigen Bedingungen aufrecht und stellt **zusätzliche** Anforderungen. So müssen **alle** Einwilligungen künftig **jederzeit widerrufbar** und nachweisbar sein. Über die jederzeitige Widerrufbarkeit muss die betroffene Person **vor** Abgabe der Einwilligung **informiert** werden.

Nach Auffassung der deutschen Datenschutzaufsichtsbehörden sollen bisher erteilte Einwilligungen grundsätzlich ohne zeitliche Begrenzung **fortgelten, wenn die Art der bereits erteilten Einwilligungen den Bedingungen der DSGVO entspricht.** Die Aufsichtsbehörden empfehlen, *"alle Einwilligungserklärungen soweit wie möglich zeitnah zu aktualisieren und bei neuen Einwilligungen die Rechtsvoraussetzungen genau zu beachten".*

Bitte achten Sie in Zukunft auch auf eine sorgfältige **Dokumentation** der Einwilligungen. Jede einzelne Einwilligung muss im Streitfall und bei Kontrollen der Datenschutzaufsicht **nachweisbar** sein.

2. Werbung per Post ohne Einwilligung wird einfacher

Werbung per Post bleibt auch in Zukunft ohne Einwilligung zulässig. Besser noch: Ab Mai 2018 ist die **Listenbegrenzung** abgeschafft. Dann kann z. B. das Geburtsdatum auch ohne Einwilligung der betroffenen Person für ein Geburtstags-Mailing eingesetzt werden.

Basis für die schriftliche Werbung und die vorgelagerte Zielgruppenanalyse wird die sog. **Interessensabwägung.** Dabei werden das **berechtigte Interesse eines Unternehmens an zulässigem Direktmarketing** gegen die schutzwürdigen Interessen seiner Kunden oder Interessenten abgewogen. Hat ein Kunde der Werbung **widersprochen, überwiegt** sein schutzwürdiges Interesse das geschäftliche Interesse und die Werbung per Post wird unzulässig.

Entscheidend ist in diesem Zusammenhang aber auch, welche **Informationen** der Kunde oder Interessent bei Erhebung seiner Daten für Werbezwecke erhalten hat.

3. Zusätzliche Informationspflichten durch Transparenzgebot

Das Transparenzgebot der DSGVO verlangt in Zukunft umfassende Informationen. Eine informationelle Selbstbestimmung ist nur möglich, wenn der Kunde weiß, was mit seinen Daten geschieht. Diese Information wir sinnvollerweise erteilt, wenn der Kunde die Daten zur Verfügung stellt, also **bei Erhebung** der Daten.

Schon bisher haben Sie darüber informiert, wer Sie sind, welche Zwecke Sie bei der Datenverarbeitung verfolgen und wer die Daten sonst noch erhält.

Die DSGVO verlangt deutlich **mehr** Informationen. So müssen Sie künftig mitteilen:

- die Rechtsgrundlagen der Verarbeitung;
- ob Sie die Daten in ein Drittland übermitteln wollen;
- die Kontaktdaten Ihres Datenschutzbeauftragten;
- wie lange Sie die Daten speichern oder zumindest die Kriterien für die Festlegung dieses Zeitraums;
- das Bestehen der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung, Datenübertragbarkeit und Beschwerde bei einer Datenschutzaufsichtsbehörde;

um nur die wichtigsten der neuen Informationspflichten zu nennen.

4. Auch die Auskunftspflicht wird erheblich erweitert

Fehlerhafte oder unzureichende Auskünfte waren schon in der Vergangenheit **Anlass für die meisten Beschwerden** bei Datenschutzaufsichtsbehörden. Mit dem **gestiegenen Bußgeldrisiko** müssen Sie und Ihre Kooperationspartner künftig **noch mehr als bisher** darauf achten, dass die Kundenbetreuung schnell und kompetent Auskünfte erteilt. Neben den bisherigen Informationen muss der Betroffene künftig auf die geplante **Speicherdauer**, seine Datenschutzrechte und sein Beschwerderecht bei einer Datenschutzaufsichtsbehörde hingewiesen werden.

Die Auskunft muss auf Wunsch **auch mündlich** erteilt werden, allerdings nur, soweit **die Identität des Kunden zweifelfrei nachgewiesen** wird.

5. Neue Rechte der betroffenen Person

a. Recht auf Widerspruch gegen Werbung

Hier bleibt alles beim Alten: Die betroffene Person kann **jederzeit** aus Gründen, die sich aus ihrer besonderen Situation ergeben, einer Verarbeitung auf Grundlage der Interessensabwägung widersprechen.
Bei einem ebenfalls **jederzeit** möglichen **Widerspruch gegen Direktwerbung** ist **keine Begründung** erforderlich. In diesem Fall dürfen die personenbezogenen Daten nicht mehr für Direktmarketingzwecke verwendet werden. Deshalb müssen die für die Berücksichtigung des Widerspruchsrechts erforderlichen Daten für diese Zwecke in Ihrer **Werbesperrdatei** gespeichert **(gesperrt)** und nicht etwa gelöscht werden. Die **Bestätigungsschreiben** für die Werbewidersprecher müssen allerdings an die neuen Vorschriften angepasst werden.

b. Recht auf Vergessenwerden

Die **Löschung** von Daten erhält durch die DSGVO eine erhebliche Relevanz. Weil das Internet nichts "vergisst", hat der Gesetzgeber in der DSGVO nach der Rechtsprechung des Europäischen Gerichtshofs das "*Recht auf Vergessenwerden"* eingeführt. Dabei handelt es sich im Wesentlichen um ein **Recht auf Löschung**, das der betroffenen Person unter bestimmten, im Detail geregelten Bedingungen zusteht.
Sie und Ihre Kooperationspartner müssen sich künftig verstärkt darüber Gedankten machen, **welche Daten wie lange gespeichert werden dürfen und wann die Daten gelöscht bzw. vollständig anonymisiert** werden müssen. Die **Speicherdauer** der Daten hängt im Regelfall vom jeweiligen **Verwendungszweck** ab.
Wenn die Speicherfristen feststehen, sollte über die Einrichtung von **Löschroutinen** nachgedacht werden.

c. Recht auf Datenübertragbarkeit

Neu ist auch das Recht auf **Datenübertragbarkeit**. Beruht die Datenverarbeitung auf einer Einwilligung oder auf einem Vertrag, kann Ihr Kunde verlangen, dass Sie seine Daten in einem **strukturierten, gängigen und maschinenlesbaren Format** (z. B. CSV) an ihn übermitteln. Der Kunde kann aber auch verlangen, dass Sie seine Daten in diesem Format **direkt an einen anderen Verantwortlichen übermitteln.** Das wird vorwiegend der Fall sein, wenn der Kunde zur Konkurrenz wechseln will.

6. Erstmals Bußgelder bei Datensicherheitsverstößen

Angesichts der wachsenden Cyberkriminalität erhält die Datensicherheit einen deutlich größeren Stellenwert als bisher. **Erstmals** werden **Verstöße gegen Datensicherheitsanforderungen** mit einem **Bußgeld** von bis zu 10 Mio. Euro oder 2% des letztjährigen Umsatzes belegt.

Schon in der Vergangenheit haben Sie und Ihre Kooperationspartner auf Grundlage der im BDSG geforderten technischen und organisatorischen Maßnahmen einen hohen Datensicherheitsstandard gewährleistet. Dieser muss nun **erweitert** werden.

Die **neuen Verpflichtungen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen** verpflichten Sie, schon bei Anschaffung und Konfiguration eines neuen CRM- oder HR-Systems darauf zu achten, dass bei ihrem Einsatz in der Datenverarbeitung die Grundlagen der DSGVO eingehalten werden können.

Die DSGVO verlangt bei der Datensicherheit ein **risikoangemessenes Schutzniveau** unter Berücksichtigung von **Eintrittswahrscheinlichkeit und Schwere der Risiken** für die betroffenen Personen durch Vernichtung, Verlust, Veränderung und unbefugte Offenlegung oder Zugang zu den Daten. Sie müssen also künftig für jede Datenart und ihren Verwendungszweck (1) den Schutzbedarf feststellen, (2) die Risiken bewerten, (3) geeignete Maßnahmen treffen sowie (4) die entsprechenden Nachweise bereithalten und bei Anfragen von Aufsichtsbehörden erbringen.

Bei zwei Datensicherheitsanforderungen wir die DSGVO allerdings sehr **konkret**: Sie verlangt eine weitgehende Verschlüsselung von personenbezogenen Daten und, wo möglich, deren **pseudonymisierte Verarbeitung**.

7. Verschlüsselung statt Meldepflicht bei "Datenpannen"

Die Gewährleistung einer **verschlüsselten Datenübermittlung** und einer **vorwiegend pseudonymisierten Datenanalyse** hat nicht nur bei den Rechtsgrundlagen und der Datensicherheit, sondern auch bei den Meldepflichten entscheidende Vorteile. Während einerseits die Schwelle für eine Meldepflicht von Datenschutzpannen und Datenverlusten bei den Aufsichtsbehörden und den Betroffenen gesenkt wird, besteht andererseits im Regelfall **keine Meldepflicht, wenn aufgrund von Verschlüsselung oder Pseudonymisierung der abhanden gekommenen Daten ein Risiko für die betroffenen Personen nicht zu erwarten ist**.

Angesicht der damit verbundenen **Vorteile** sollten Sie diesen beiden Datensicherheitsthemen große Aufmerksamkeit widmen.

8. Achtung: Drastisch erhöhtes Bußgeldrisiko

Ein deutliches Zeichen dafür, dass der Datenschutz EU-weit einen höheren Stellenwert genießt, sind die **drastisch erhöhten Bußgelder**. Wo derzeit noch keine oder moderate Bußgelder zu erwarten sind, drohen ab Mai 2018 **Geldbußen in Millionenhöhe**. Mindestens ebenso unangenehm ist die fast zwangsläufige negative Berichterstattung der Medien bei "Datenpannen".

Für Verstöße gegen die Datensicherheit, bei der Auftragsdatenverarbeitung oder bei der Meldung von Datenschutzpannen, ja selbst für fehlende Verfahrensverzeichnisse, drohen **Bußgelder von bis zu 10 Mio. Euro oder 2 % des gesamten, weltweit erzielten Vorjahresumsatzes**, je nachdem welcher Betrag höher ist.

Liegen Verstöße gegen die **Grundsätze der Datenverarbeitung**, einschließlich der Bedingungen für die Einwilligung, oder Verstöße gegen die Rechte der betroffenen Person vor, drohen **Bußgelder von bis zu 20 Mio. Euro oder 4 % des gesamten, weltweit erzielten Vorjahresumsatzes**, je nachdem welcher Betrag höher ist.

Sicherlich wurden diese hohen Bußgelder festgelegt, um internationale Unternehmen, die mit der Verarbeitung von personenbezogenen Daten sehr großen Umsatz machen, wirksam sanktionieren zu können. Ebenso sicher ist, dass ein mittelständisches Unternehmen bei einem Erstverstoß nicht mit diesen "Höchststrafen" zu rechnen hat. Jedoch schreibt die DSGVO **ausdrücklich** vor, dass die Sanktionen a**bschreckend** sein müssen. Deshalb muss man auch als Mittelständler bei einem Erstverstoß mit einem Bußgeld im unteren fünfstelligen Bereich rechnen.

Fazit: Die Umsetzungsfrist ist jetzt!

Beim Datenschutz und Datensicherheit gilt wie beim Zahnarzt: Die Prophylaxe ist billiger und weniger schmerzhaft als die Therapie. Durch zeitgerechte Anpassungen Ihrer Datenverarbeitungen an die DSGVO können Sie sich Kosten, Zeit, Ärger und schlechte Presse sparen. Viele der geschilderten Risiken lassen sich vermeiden, wenn die Umsetzung strategisch gut geplant ist und das Timing auf die Bedürfnisse der Organisation oder des Unternehmens zugeschnitten wird.