Die Datenschutzgrundverordnung (DSGVO) auf einen Blick

Ein Service der netzGiraffe

WAS IST DAS UND WAS IST NEU DARAN?

Die DSGVO ist das ab 25.05.2018 geltende Gesetz zum Schutz personenbezogener Daten. Neu, im Gegensatz zum bisher geltenden Bundesdatenschutzgesetz, sind folgende Punkte:

1. Die Rechenschafts- und Dokumentationspflicht,
2. die Rechte der Betroffenen,

2.1 Informationsrecht, Auskunftsrecht, Recht auf Löschung, Recht auf Datenübertragung, Recht auf Meldung und Benachrichtigung,

3. der Datenschutz durch Technik,
4. drohende Bußgelder.

WARUM SOLLTE SIE DAS INTERESSIEREN?

Die DSGVO betrifft Unternehmen, die personenbezogene Daten automatisiert erfassen und/oder verarbeiten. Dabei sind nicht nur Unternehmen betroffen, deren Hauptsitz in Europa liegt. Unternehmen mit Niederlassungen in Europa, aber auch Unternehmen ohne Sitz oder Niederlassungen in Europa, die personenbezogene Daten von EU-Bürgern automatisiert erheben oder verarbeiten, sind von dem neuen Gesetz betroffen.

> **„Die DSGVO betrifft alle Unternehmen, die personenbezogene Daten von EU-Bürgern automatisiert erheben oder verarbeiten“**

Björn Lindner - Inhaber

Wird gegen Bestimmungen der DSGVO verstoßen, drohen ab dem 25.05.2018 Bußgelder. Das Höchstmaß beträgt 4% des weltweit erzielten Jahresumsatzes eines Unternehmens oder 20.000.000 €.

WAS SIND PERSONENBEZOGENE DATEN?

Dies sind Daten, welche dazu dienen, eine Person zu identifizieren oder identifizierbar machen. Dazu gehören u.a. Name, Geburtsdatum, Anschrift, aber auch IP-Adressen, E-Mail-Adressen,

...

...

Kfz-Kennzeichen, Telefonnummern, Standortdaten, Kontodaten oder andere Daten, die eine Person identifizierbar machen.

WELCHE FOLGEN KÖNNEN AUF SIE ZUKOMMEN?

Ihre Datenschutzerklärung sollte mit Eintreten der DSGVO auf dem neusten Stand sein. Ist sie das nicht, drohen:

1. Schadenersatzforderungen,
2. Verbandsklagen,
3. Regressansprüche,
4. Abmahnungen,
5. Bußgelder.

DIE PRINZIPIEN DER DSGVO

Wichtig zu wissen ist, in welchen Fällen Sie Daten legal erheben und verarbeiten dürfen.

1. BEI EINWILLIGUNG

Die Einwilligung des Betroffenen muss verständlich formuliert und frei zugänglich sein. Sie muss durch eine eindeutig bestätigende Handlung bekundet werden, sie muss nachweisbar und jederzeit widerrufbar sein. Außerdem gilt das Kopplungsverbot.

KOPPLUNGSVERBOT

Die Einwilligung der Betroffenen darf nicht an eine Vertragserfüllung gekoppelt sein. Damit ist gemeint, dass Betroffene für das Zustandekommen eines Vertrages nicht zur Einwilligung der Erhebung personenbezogener Daten genötigt werden dürfen. Die Einwilligung muss stets freiwillig erfolgen. Als nicht freiwillig erteilt gilt sie, wenn die Erfüllung eines Vertrages von ihr abhängig gemacht wird, obwohl die erhobenen Daten zur Erfüllung dieses Vertrages nicht notwendig sind. Die Vertragserfüllung darf also nicht ohne klar belegbaren Grund (Name und Anschrift sind für das Versenden bestellter und bezahlter Ware notwendig) an die Einwilligung zur Verarbeitung personenbezogener Daten gekoppelt werden.

2. ZUR VERTRAGSERFÜLLUNG

Ist die Erhebung personenbezogener Daten notwendig, um das Zustandekommen eines Vertrages zu gewährleisten, ist die Erhebung und Verarbeitung dieser Daten zulässig. So ist dies zum Beispiel für Online-Shops der Fall. Damit der Kunde seine bestellte Ware erhalten kann, sind personenbezogene Daten in Form von Name und Adresse notwendig und damit deren Erhebung zulässig. Auch die Kontodaten werden im Falle einer Retour benötigt, um den zu erstattenden Betrag überweisen zu können.

3. ZUR WAHRUNG BERECHTIGTER INTERESSEN

Ein berechtigtes Interesse liegt bei klarem Vorteil für den Betroffenen vor, wie Gewinnmaximierung oder Kostensenkung.

...

WAS MÜSSEN SIE JETZT TUN?

1. DATENSCHUTZERKLÄRUNG AUF FOLGENDE KRITERIEN PRÜFEN

- Transparent, leicht zugänglich und in präziser, klarer und möglichst einfacher Sprache verfasst.
- Nennt die Rechtsgrundlage der Verarbeitung (warum erhebe und verarbeite ich personenbezogene Daten).
- Nennt Betroffenenrechte.
- Nennt Widerspruchsrecht.
- Enthält Beschwerderecht bei Datenschutzaufsichtsbehörden.

Die Datenschutzerklärung sollte, solange sie die genannten Punkte enthält, in eigenen Worten verfasst werden. Sperrige und schwer verständliche, rechtliche Formulierungen tragen kaum zum Verständnis bei und sollten vermieden werden.

> **„Vor Inkrafttreten der DSGVO sollte Ihre Datenschutzerklärung entsprechend angepasst werden“**
>
>  Thomas Rothe - Inhaber

2. VERZEICHNIS DER VERARBEITUNGSTÄTIGKEIT

Das Verzeichnis Ihrer Verarbeitungstätigkeit dient als zentrales Verzeichnis der Dokumentationspflicht der Prüfung durch Datenschutzaufsichtsbehörden und der Selbstkontrolle und damit auch dem Selbstschutz. Das Verzeichnis muss schriftlich vorliegen und jede Änderung in der Verarbeitungstätigkeit muss darin dokumentiert werden. Die tabellarische Auflistung dokumentiert, welche Daten wann, in welcher Form, warum und von wem verarbeitet werden. Wichtig ist: Hierbei geht es nicht allein um Daten Ihrer Kunden! Auch die Verarbeitung personenbezogener Daten Ihrer Mitarbeiter und Aufraggeber muss ordnungsgemäß dokumentiert werden.

Dokumentiert werden müssen:

- Name und Kontaktdaten des Verantwortlichen/ Auftragsverarbeiters, der oder die personenbezogene Daten erhebt und verarbeitet,
- wenn vorhanden, die Kontaktdaten des Datenschutzbeauftragten,
- der Zweck der Verarbeitung personenbezogener Daten,
- eine Beschreibung der Kategorien betroffener Personen und der personenbezogenen Daten, (z.B. Kundenstammdaten [Name, Adresse, Telefonnummer], Bestellung [Anzahl, Größe, Farbe], Frisur [Haarschnitt, Haarfarbe]),

- die Kategorie von Empfängern, denen personenbezogene Daten offengelegt werden oder wurden (dazu gehören auch Empfänger in Drittländern),
- die Übermittlung der Daten in Drittländer,
- wenn absehbar, die vorgesehene Löschung der erhobenen und verarbeiteten Daten,
- eine Beschreibung der technischen und organisatorischen Maßnahmen (siehe Prozesshandbuch) um die Sicherheit personenbezogener Daten garantieren zu können.

Dieses Verzeichnis ist für die Verarbeitungstätigkeit der Verantwortlichen, wie auch für die Verarbeitungstätigkeit im Auftrag eines Verantwortlichen, also als Auftragsverarbeiter, zu führen.

3. PROZESSHANDBUCH

Das Prozesshandbuch soll die Sicherheit der Verarbeitung dokumentieren und garantieren. Die Verantwortlichen müssen durch geeignete technische und organisatorische Maßnahmen den sicheren Umgang mit erhobenen, personenbezogenen Daten gewährleisten. Folgende Angaben zum angemessenen Schutzniveau gehören in das Handbuch:

- Wie werden personenbezogene Daten pseudonymisiert und verschlüsselt?
- Welche Dienste und Systeme werden in der Verarbeitung der personenbezogenen Daten genutzt?
- Können Fähigkeit, Verfügbarkeit, Integrität, Vertraulichkeit und Belastbarkeit der Dienste und Systeme garantiert werden?
- Wie werden die Betroffenen über die Erhebung und Verarbeitung der personenbezogenen Daten informiert (mündlich, schriflich, in einer Infobox, in den AGB)?
- Wie wird auf Nachfragen von Betroffenen reagiert?
- Wie verläuft der Löschvorgang bei Einforderung der Löschung durch Betroffene?
- Wie wird im Fall eines Datenlecks vorgegangen?
- Wie verläuft der fristgerechte Löschvorgang?
- Wie werden Mitarbeiter und Verantwortliche zum Datenschutz und dem sicheren und transparenten Umgang mit personenbezogene Daten aufgeklärt und geschult?

4. DATENSCHUTZ-FOLGEABSCHÄTZUNG

Die Datenschutz-Folgenabschätzung betrifft Unternehmen, die besonders schützenswerte und besonders risikobehaftete Daten erheben oder verarbeiten. Das Risiko des Missbrauchs besonders sensibler Daten soll mit der Aufstellung einer Datenschutz-Folgeabschätzung gesenkt werden. Zu besonders sensiblen, schützenswerten und risikobehafteten Daten gehören Angaben zur Sexualität, Krankheiten, Finanzen, ethnischer und religiöser Zugehörigkeit und politischer Einstellungen. Dies ist in erster Linie für Ärzte und Versicherungen von Bedeutung. Auch hier müssen die Datenverarbeitungsvorgänge mit Zweck, dabei bestehenden Risiken, technischen und organisatorischen Sicherheits- und Kontrollmaßnahmen dokumentiert werden.

...

5. DATENSCHUTZBEAUFTRAGTER

Ein Datenschutzbeauftragter wird für jedes Unternehmen zur Pflicht, in dem von mindestens 10 Mitarbeitern regelmäßig personenbezogene Daten automatisiert verarbeitet werden. Dabei spielt es keine Rolle, ob ein Mitarbeiter in Teil-oder Vollzeit beschäftigt, frei oder fest angestellt, Praktikant oder Auszubildender ist. Sobald 10 Mitarbeiter regelmäßig mit personenbezogenen Daten (von Kunden oder Mitarbeiter) in Berührung kommen, wird ein Datenschutzbeaufragter Pflicht. Dies gilt auch bei weniger Mitarbeitern, wenn mit besonders schützenswerten Daten gearbeitet wird (siehe Datenschutz-Folgenabschätzung). Der Datenschutzbeauftragte unterrichtet und berät das jeweilige Unternehmen zu Pflichten und Vorschriften des Datenschutzes. Er überwacht und prüft die Einhaltung des Datenschutzes und er steht Mitarbeitern für Fragen und Unklarheiten zum Datenschutz zur Verfügung. Außerdem schult er Mitarbeiter zum Datenschutz und führt gegebenenfalls notwendige Datenschutz-Folgeabschätzung durch.

WAS IST BEI EINER DATENPANNE ZU TUN?

Sollte Ihnen eine Datenpanne in Ihrem Unternehmen bekannt werden, ist schnelles Handeln erforderlich. Informieren Sie umgehend Betroffene und Aufsichtsbehörden und falls sie Auftragsverarbeiter sind, die Verantwortlichen der Verarbeitung. In diesem Fall kommen Ihre Dokumentationen zu Verarbeitung und Prozessen zum Einsatz.

Kommen Sie für weitere Fragen gerne auf uns zu

Als unser Kunde halten wir Sie selbstverständlich über künftige Entwicklung im Feld der DSGVO auf dem Laufenden.

 Björn Lindner

 Thomas Rothe

HINWEIS!

Da wir keine Kanzlei sondern eine Webagentur sind, bitten wir Sie, unsere Handreichung als kurze Übersicht zu betrachten, jedoch nicht als rechtliche verbindliche Ausarbeitung.

netzGiraffe GbR
Lützner Str. 46
04177 Leipzig

Telefon (0341) 550 15 11 5
Fax (0341) 550 15 11 4
E-Mail info@netz-giraffe.de