

INFO



DER BUNDESINNUNGSVERBAND INFORMIERT

EU-Datenschutzgrundverordnung Last-Minute-Hilfe gegen Abmahnungen und Bußgelder

Keine Übergangsfrist! Stichtag ist der 25.5.2018. Ab diesem Tag müssen sie die EU-DSGVO umgesetzt haben.

Was ist bis dahin zu tun?

1. Internetauftritt fit machen!

- Die Einführung der EU-DSGVO erfordert auf jeden Fall eine Anpassung der Datenschutzerklärung. Dazu gibt es kostenlose Generatoren im Internet, häufig angeboten von Anwaltskanzleien oder Webdienstleistern. Achten sie bei der Erstellung unbedingt darauf, dass Sie Ihre Daten korrekt und wahrheitsgemäß eingeben. Eine fehlerhafte Datenschutzerklärung mag besser sein als gar keine, jedoch schützt sie nicht vor einem Bußgeld. Sofern Sie bei technischen Angaben nicht weiterwissen, ziehen Sie ihren EDV-Dienstleister oder denjenigen hinzu, der ihre Webseite erstellt hat.
- Die Datenschutzerklärung muss zwingend per Ein-Klick-Regel erreichbar sein. Das bedeutet, dass der Besucher der Webseite diese mit nur einem Klick erreicht. Ein Aufruf tief in einem Untermenü genügt nicht den rechtlichen Anforderungen.
- Deutsche Websitebetreiber, welche personenbezogene Daten mittels ihrer Website erheben, z.B. Name und Adresse zwecks Kontaktaufnahme, haben die Pflicht für eine (sicherere) SSL-Verbindung (<https://>) zu sorgen.
- Sofern Ihr Unternehmen einen Datenschutzbeauftragten benötigt (mehr als neun Personen, die regelmäßig mit automatisierter Datenverarbeitung zu tun haben), muss dieser auch auf der Webseite genannt werden. Ebenso haben Sie die Pflicht, diesen der zuständigen Landesdatenschutzbehörde zu melden.

2. Mitarbeiter schulen!

Die EU-DSGVO verlangt nicht nur von Ihnen als Verantwortlichem ein Umdenken, sondern auch von Ihren Mitarbeitern. Weisen Sie ihre Mitarbeiter auf die kommenden Gesetzesänderungen hin. Wichtig ist ein Umdenken hin zu einem Problembewusstsein. Niemand verlangt von Ihnen, dass jeder Mitarbeiter umfassend und vollumfänglich aufgeklärt wird. Hingegen müssen Sie aber darauf aufmerksam machen und grundlegende Funktionen des neuen Gesetzes erklären. Sie sollten diese Aufklärung der Mitarbeiter durch eine Verpflichtungserklärung dokumentieren.

3. Dokumentation

Die Dokumentationspflicht ist eines der Kernprobleme bei der Umsetzung der EU-DSGVO. Hier müssen Sie wie bei einer Inventur ein Verarbeitungsverzeichnis erstellen, indem Sie detailliert darlegen, wie Daten in Ihrem Unternehmen verarbeitet werden. Jedoch hat der Gesetzgeber keinen äußeren Rahmen dafür vorgegeben. Wie das Verarbeitungsverzeichnis aussieht, das ist Ihre Sache. Den Anforderungen genügt auch eine simple Excel Tabelle, in der die einzelnen Verfahren beschrieben werden.

Die wichtigsten Punkte sind dabei:

- Wer? Von welchen natürlichen Personen erhalten Sie Daten?
- Warum? Zu welchem Zweck benötigen Sie diese?
- Welche? Welche Daten verarbeiten Sie?
- Wie? Wie gelangen die Daten zu Ihnen?
- Wie lange? Gibt es eine Speicherfrist?

4. Einwilligung? Einwilligung!

- Vorher fragen! Die EU-DSGVO verlangt, dass Sie vor der Verarbeitung personenbezogener Daten die Einwilligung des Betroffenen einholen. Zwingend ist dabei der zeitliche Ablauf. Eine Verarbeitung von Daten mit nachträglicher Einholung ist eine Genehmigung, keine Einwilligung und somit nicht statthaft.
- Sonderfall Vertragsschluss, gesetzlicher Vorbehalt, ...

In aller Regel benötigen Sie aber gar keine Einwilligung, denn es greifen Sonderregeln. Dazu zählt vor allem die Abwicklung eines Vertrages oder eine gesetzliche Pflicht. Sofern die Verarbeitung personenbezogener Daten für die Erfüllung von Vertragspflichten notwendig ist, benötigen Sie vom Betroffenen keine Einwilligung. Das betrifft etwa Name, Adresse, Bankdaten, Unterlagen bei Handwerksprojekten u.ä. Nur dann, wenn Sie über den Vertragszweck hinaus Daten nutzen möchten, etwa zu Werbezwecken, benötigen Sie die Einwilligung des Betroffenen. Aus praktischen Gründen empfiehlt es sich, diese gleich bei Vertragsabwicklung anzufordern. Ähnliches gilt auch für die Erfüllung einer gesetzlichen Pflicht. Sie dürfen ohne weiteres dann Daten verarbeiten (auch weiter geben), wenn Sie dazu von Gesetz wegen verpflichtet sind. Das können etwa Sozialversicherungsbehörden oder das Finanzamt sein.

5. Auftragsverarbeitung

- Daten weiter geben
Ein wichtiger Punkt ist die Auftragsverarbeitung. Sofern Sie Daten an andere weitergeben und dort verarbeiten lassen, werden diese zu Auftragsverarbeitern. Das ist von der DSGVO auch so vorgesehen. Der Auftragsverarbeiter wird dabei rechtlich so behandelt, als wäre er Teil des Unternehmens und gleichermaßen an dessen rechtliche Datenverarbeitungsgrundlagen gebunden.
- Drittländer
Möchten Sie Daten außerhalb der EU verarbeiten, so ist dies möglich. Allerdings müssen Sie hier darauf achten, dass die DSGVO ihnen einen vergleichbaren Schutz vorschreibt. Das bedeutet, dass Unternehmen außerhalb der EU dieselben Mechanismen zum Schutz personenbezogener Daten aufbauen müssen wie innerhalb der EU. Das zu überprüfen ist allerdings Ihr Risiko.

6. Auskunftsrechte, Datenschutzverletzungen und Co...

- Nicht nur müssen Sie die Einwilligung von Betroffenen einholen, Sie sind Ihnen auch zur Rechenschaft verpflichtet. Das betrifft Auskunftsrechte oder auch Löschansprüche. Auch hierzu müssen Sie Verfahren erstellen und möglichst darauf vorbereitet sein, wenn etwa ein Kunde oder Mitarbeiter Auskunft verlangt, was denn über ihn gespeichert ist.
- Verletzungen
Werden Rechte von Betroffenen verletzt, müssen Sie diese grundsätzlich der zuständigen Datenschutzbehörde melden. Ob und wie, das hängt vom Einzelfall ab. So macht es einen Unterschied, ob etwa eine Einwilligung eines Betroffenen fehlt oder sensible Gesundheitsdaten nach außen gelangen.

7. Technik prüfen!

EDV auf aktuellem Stand halten! Erstmals wird der Datenschutz im Unternehmen explizit auch anhand der Technik beurteilt. So schreibt der Gesetzgeber den Einsatz aktueller und zumutbarer Maßnahmen vor. Wichtig ist in diesem Zusammenhang, dass man Hard- wie Software regelmäßig prüft, aktualisiert und bei mangelnder Sicherheit auch austauscht. Windows Systeme, die nicht mindestens auf dem Stand Windows Server 2008 und Windows 7 sind, sollten unverzüglich entsorgt werden. Das betrifft auch den zehn Jahre alten Router, der zwar noch zuverlässig seinen Dienst tut, aber einfach nicht mehr sicher ist. Ebenso gehören aktuelle Virenschutzprogramme, verschlüsselte Verbindungen ins Internet und funktionierende Datensicherungen in das Pflichtenheft. Sind Sie sich unsicher, ob sie diese Anforderungen erfüllen, so setzen Sie sich mit Ihrem IT-Dienstleister in Verbindung.

8. Und zum Schluss? Ruhe bewahren.

- Die Umsetzung der EU-DSGVO verlangt weder umfassende juristische Kenntnis noch Fähigkeiten als Systemadministrator. Wichtig ist, dass Sie verstehen, warum der Gesetzgeber diese Regelungen eingeführt hat und wie Sie diese umsetzen können. Schützen Sie die Daten ihrer Kunden, Mitarbeiter und Lieferanten so, wie auch Sie Ihre Daten behandelt sehen wollen.

- Nicht alles auf einmal! Setzen sie die DSGVO Schritt für Schritt um. Zuerst sollte das Verstehen im Vordergrund stehen, dann das Gespräch mit Mitarbeitern. Sodann geht es in die praktische Umsetzung. Auch wenn der Stichtag der 25.5.2018 ist, wird die Welt nicht untergehen, wenn Sie bis dahin nicht alles umgesetzt haben. Bleiben Sie aber trotzdem dran und vor allem aktiv. Informieren Sie sich, sprechen Sie mit anderen Unternehmern und scheuen Sie sich nicht, externen Rat einzuholen. Denn jeder ist betroffen. Die DSGVO macht keine Ausnahmen und jeder Unternehmer hat die Pflicht zur Umsetzung.

(Quelle: Kreishandwerkerschaft Hochsauerland)

Bonn, 22.5.2018



Heribert Baumeister
Bundesinnungsmeister

