WHITE PAPER Ein kurzer Ratgeber für Unternehmen

DSGVO

Die neue EU-Datenschutzgrundverordnung

cross media IT

Ab dem 25. Mai 2018 wird es ernst

In Emils Postfach poppt gerade eine E-Mail der Müller GmbH auf. Es ist ein Newsletter zur Bewerbung der neuen Möbelserie. Emil wundert sich, denn angemeldet hat er sich für den Newsletter nicht. Und so langsam nerven ihn die Newsletter der Müller GmbH, es ist der vierte in zwei Wochen. Emil erinnert sich an die neue EU-Datenschutzgrundverordnung (DSGVO) und ruft kurzerhand seinen Anwalt an, der ihm rät, auf Verstoß gegen die EU-DSGVO zu klagen…

So schnell kann es ab dem 25. Mai 2018 mit Klagen gegen Unternehmen gehen, denn dann endet die Übergangszeit und die neue EU-Datenschutzgrundverordnung tritt final in Kraft. Dabei handelt es sich nicht um eine lapidare EU-Verordnung, die auf nationaler Ebene kaum Wirkung hat. Vielmehr sind Unternehmen mehr als gut beraten, die neue DSGVO ernst zu nehmen, denn: Bei Verstößen drohen drakonische Strafen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Umsatzes. Betroffen sind davon nicht nur große Unternehmen, im Gegenteil sind viele Mittelständler, Einzelunternehmer oder auch Blogbetreiber von den neuen Anforderungen an den Datenschutz betroffen. Insofern bleibt Unternehmen – und gerade dem Mittelstand – nicht mehr viel Zeit, sich und ihre Unternehmens-IT datenschutzkonform aufzustellen.

Die DSGVO: Ein Buch mit sieben Siegeln?

Aber was genau soll eigentlich mit der DSGVO erreicht werden? Das Sammeln, der Zugriff, die Verwendung, das Speichern und die Weitergabe von personenbezogenen Daten werden durch die EU-Verordnung komplett neu geregelt und so vor allem Verbraucher(daten) besser geschützt.
Personenbezogene
Daten sind dabei Informationen, die sich einer natürlichen Person zuordnen lassen – sei es über Telefonnummer, Autokennzeichen, Nutzernamen, IP-Adressen, GPS-Koordinaten, Webtracking oder Likes und Statusmeldungen auf Facebook. In diesem Kontext sieht die DSGVO unter anderem das Recht auf Vergessenwerden in Art. 17 vor, womit Verbrauchern ein umfassendes Recht auf Löschung ihrer Daten zugestanden wird. In unserem Beispiel von oben heißt das: Emil kann die unverzügliche Löschung seiner Daten bei der Müller GmbH durchsetzen. Letztlich werden also die Verbraucherrechte aufgewertet und gestärkt.

Gestärkte Rechte der Verbraucher

Nicht verzetteln: Worauf müssen Unternehmen achten?

Aber was bedeutet das für Unternehmen? Zunächst einmal müssen sie sich in die geänderte Rechtslage und die juristischen Feinheiten einarbeiten und die internen Prozesse mit den neuen Anforderungen abgleichen. Das gut 200 Seiten starke Verordnungswerk besteht aus 99 Artikeln, die viele Aspekte detailliert regeln. Einige der datenschutzrechtlichen Konzepte und Prinzipien der DSGVO sehen aber nicht grundsätzlich anders aus als die bisherige EU-Datenschutzrichtlinie (Richtlinie 95/46/EG). Deren Vorschriften wurden bisher in Deutschland mit dem deutschen Bundesdatenschutzgesetz (BDSG) umgesetzt. Wer sich also bisher im Unternehmen schon detailliert mit dem Thema Datenschutz beschäftigt hat, muss auch nicht rasend werden und in Panik ob drohender Sanktionen verfallen.

Ein umfassender und vor allem individueller Check-Up des eigenen Datenschutz- und Datensicherheitskonzepts ist jedoch unumgänglich. Dabei müssen die individuellen unternehmerischen Kontexte berücksichtig werden: Ein Anbieter einer Spiele-App muss prioritär auf andere Vorschriften achten, wie ein IT-Dienstleister mit
Rechenzentrum oder ein Webshop-Betreiber. Insgesamt besteht aber überall dort, wo personenbezogene Daten verarbeitet werden, zukünftig eine erhebliche Dokumentations- und Informationspflicht. Das heißt also auch: unternehmensintern. Denn auch über Lohnabrechnungen, Arbeitsverträge oder Firmenhandys werden personenbezogene Daten verarbeitet.

Über all diese Prozesse der Verarbeitung sind entsprechende Nachweise und Verzeichnisse zu führen.
Unternehmen müssen also grundsätzlich die Fragen klären:

- Welche Daten haben wir?
- Dürfen wir alle diese Daten überhaupt haben?
- Wo sind diese Daten gespeichert?
- Was dürfen wir mit diesen Daten überhaupt tun?
- Wer hat Zugriff auf diese Daten?
- Und wie werden diese Daten vor Angriffen geschützt?

Diese Fragen müssen sich nicht nur Unternehmen innerhalb der EU stellen, denn es gilt das Marktortprinzip: Das besagt in Art. 3, dass auch Unternehmen, die außerhalb der EU sitzen, sich mit ihren Waren oder Dienstleistungen aber an Personen innerhalb der EU richten, sich an die DSGVO halten müssen.
Und mehr noch: Datenverantwortliche müssen innerhalb von 72 Stunden die entsprechende Aufsichtsbehörde nach Bekanntwerden des Datenschutzverstoßes informieren. Bisher galt diese Meldepflicht nur eingeschränkt für die Telekom und ISP-Serviceanbieter.

Wichtige Änderungen im Überblick

- Datenschutzverstöße müssen innerhalb von 72 Stunden gemeldet werden.
- Die Verwendung und Speicherung von Daten muss detailliert in Form von Verzeichnissen dokumentiert werden.
- Für sensible oder große Datenmengen müssen separate Datenschutzfolgenabschätzungen durchgeführt werden. Risiken für betroffene Personen sollen so frühzeitig erkannt und bewertet werden.
- Unternehmer und Datenschutzbeauftragte werden persönlich für die Einhaltung der EU-DSGVO-Vorgaben und Regeln haftbar gemacht.
- Die Einhaltung von wirksamen Datenschutzrichtlinien muss unternehmensseitig nachgewiesen werden können.
- Bieten im Ausland ansässige Unternehmen Waren und Dienstleistungen für Personen in der EU an, von denen sie Daten verarbeiten, müssen sie ebenfalls den europäischen Datenschutz einhalten.
- Unternehmen müssen die Zustimmung zur Datennutzung ausdrücklich einholen und ihre Produkte datenschutzfreundlich voreinstellen und das bereits beim Design berücksichtigen (Privacy by Design & Privacy by Default).

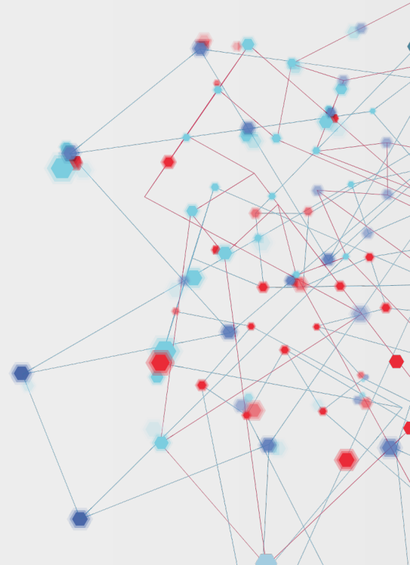
Check IT up: In 5 Schritten zu mehr DSGVO-Sicherheit

Die DSGVO bietet für Ihr Unternehmen eine gute Gelegenheit Ihr eigenes Datenschutz- und Datensicherungsmanagement zu überprüfen und an den entsprechenden Stellen anzupassen. Auf diese Weise können Sie gleichzeitig den eigenen Datensalat aufräumen, unnötige Dubletten löschen und nicht benötigte Daten effizient archivieren. Nur, wo und wie sollen Sie damit beginnen? Bei der datenschutzkonformen Aufstellung Ihres Unternehmens können Sie sich an fünf Punkten orientieren:

1. **Anschauen:** DSGVO verstehen und relevante Änderungen für das eigene Unternehmen erkennen
2. **Analysieren:** Prüfen, welche Daten vorhanden sind, welche davon personenbezogen sind, wie sie verwendet werden und wo sie gespeichert werden
3. **Absichern:** ausdrückliches, eindeutiges und freiwilliges Einverständnis bei jedem Datensubjekt zur Datennutzung einholen und möglichst wenige personenbezogene Daten sammeln
4. **Ablegen:** Daten sichern, schnellen Zugriff darauf gewährleisten sowie Notfallplan für Datenschutzverstöße entwickeln
5. **Aufbauen:** Richtlinien und Prozesse zum Datenmanagement entwickeln, die für alle einheitlich gelten und Mitarbeiter schulen

Wir unterstützen Sie gerne bei der Umsetzung eines DSGVO-konformen Datenschutzmanagements mit unserem DSGVO-Check Up in Ihrem Unternehmen. Wir durchleuchten mit Ihnen Ihr Datenschutz-Regelwerk, analysieren die Umsetzung Ihrer Rechenschafts- und Nachweispflichten, unterstützen Sie bei der Entwicklung oder Optimierung Ihres Risikomanagements und der Durchführung von Datenschutz-Folgeabschätzungen. So werden Sie fit für die neue EU-DSGVO.

Sprechen Sie gerne unsere IT-Sicherheitsexperten auf den Check-Up oder Ihr Security-Thema an.



cross media IT

Winkelstraße 2
33332 Gütersloh
Telefon: +49 5242 18 201-40
E-Mail: info@crossmedia-it.com
www.crossmedia-it.com