Theoretisch war einmal, PRAXIS ist hier!

99 Dinge, die einem Unternehmer Kopfzerbrechen bereiten, und eine Erklärung, was mit den 99 Artikeln der europäischen Datenschutzgrundverordnung (EU-DSGVO) ab dem 25. Mai 2018 verbindlich auf Sie zukommt.

Das vorliegende Whitepaper hat folgendes Ziel: Ihre Augen für das Kommende zu öffnen, Ihnen Begrifflichkeiten, Änderungen und Abläufe der EU-DSGVO näherzubringen und Ihnen Ihren zielgerichteten Handlungsbedarf mit einigen Lösungsansätzen aufzuzeigen.

Worum geht es in der EU-DSGVO und was kommt ab dem 25. Mai 2018 verbindlich auf Sie zu?

Die Verordnung trat bereits am 25. Mai 2016 in Kraft, nach einer zweijährigen Übergangsphase findet die dieses Jahr verbindliche Anwendung statt.

Die EU-DSGVO regelt innerhalb der EU den einheitlichen Umgang mit personenbezogenen Daten und bildet damit die Grundlage für den Datenschutz im digitalen Zeitalter. Damit hat sie einen sehr starken Impakt auf die bestehenden Strukturen und Prozesse bei Unternehmen, welche im Internet oder bei internen Abläufen mit digitalen Daten arbeiten.

Bisher waren folgende Regelungen vorhanden:

Der Sitz des Unternehmens entscheidet über die anwendbaren Datenschutzrichtlinien. **Was heißt das?** Alle Daten, die in beispielsweise US-amerikanischen Servern von ihnen gespeichert sind – egal, ob wissentlich oder unwissentlich – unterliegen den dortigen Datenverarbeitungsrichtlinien. Ihre Handhabe, diese löschen zu lassen, Einsicht zu erhalten oder Missbrauch zu verhindern, richteten sich nach den lokalen Gegebenheiten.

Jetzt haben wir jedoch eine bevorstehende Verordnung von globalen Auswirkungen, denn die neue Datenschutzrichtlinie gelten nicht nur für alle Unternehmen, welche in der EU ansässig sind, sondern auch für alle anderen Unternehmen, die eine Niederlassung in der EU haben ODER/UND personenbezogene Daten von EU Bürgern verarbeiten. Personenbezogene Daten sind nach neuer Definition eindeutige Identifikatoren (z. B.: Name, Adresse, Telefonnummer, Geburtstag, Kontodaten, IP Adressen, Cookies, etc.), welche direkt oder indirekt durch Verknüpfungen Rückschlüsse auf die Person zulassen. Der Datenschutz wird besonders in Deutschland großgeschrieben und unterliegt schon heute strengen Richtlinien und Überwachungen. Für uns ändert sich also nicht so viel wie für andere Länder, was Deutschland einen klaren Vorteil bringen kann.

Wie können Sie geprüft werden?

Die bisher eher im deutschen Onlinehandel ansässige Unternehmen bekannte „One-Stop-Shop“ Regelung – also die Regelung, dass direkte Beschwerden bei der Datenschutzbehörde im eigenen Land eingereicht und bearbeitet werden – gilt nun für alle Datenverarbeitenden Sparten von Automotive über Energiewirtschaft bis zu Versicherungen. Nach Artikel 56 Absatz 1 EU-DSGVO wird dieses Prinzip ab sofort auch für Datenschutzverstöße, welche außerhalb ihres Landes geschehen oder aufgefallen sind, erweitert. Die Zuständigkeiten, also welche Behörde was übernimmt, ist noch nicht eindeutig geklärt.

Bei grenzüberschreitendem Datenverkehr soll dann allein die Aufsichtsbehörde am Sitz bzw. Hauptsitz eines Unternehmens bei Datenschutzverstößen zuständig sein. Dabei stellt sich aber zum Beispiel die Frage, wie sich die verschiedenen Zuständigkeiten verschiedener Behörden zum Beispiel auf die Höhe der Bußgelder auswirken werden.

Welche Bereiche sind betroffen?

Es sind alle Bereiche betroffen, welche mit gespeicherten personenbezogenen Daten arbeiten: Arbeitgeber, Personalvermittler, Betriebsräte und Behörden, denn selbst die Mitarbeiterdaten im Unternehmen unterliegen der EU-DSGVO.

Was ändert sich denn wirklich?

Verbot mit Erlaubnisvorbehalt:
Die Erhebung, Nutzung und Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, außer eine Einwilligung oder Erlaubnis der Person liegt vor. Das trifft Sie bereits jetzt schon in allen Bereichen. Als Beispiel: Sie schließen bei einem namenhaften Mobilfunkhersteller einen Vertrag am Telefon ab, Sie stimmen mündlich der Auftragsbestätigung zu und werden anschließend Zeuge der schnellsten Datenschutzbelehrung aller Zeiten. Denn der Agent schafft es, eineinhalb Seiten Datenschutzbelehrung mit Worten wie: „Weiterverarbeitung“, „Auswertung“, „gezielte Angebote“ etc. in eine Minute zu quetschen. Sagen Sie die Worte: „ich stimme zu“ haben sie gerade ihrer Datenspeicherung zugestimmt und eine Erlaubnis – auch als ausdrückliche Permission bezeichnet – erteilt.

Ein Tipp für Sie als Unternehmen: setzen Sie sich bei allen Daten ein sogenanntes „opt-in“ bzw. „opt-out“. So können Sie mit einem Klick Datensätze für bestimmte Zwecke wie zum Beispiel Werbung an- und abschalten.

Datensparsamkeit:
Hier gilt das klare Prinzip, es darf nur gespeichert werden, was absolut nötig ist. Weitere Informationen, die „versehentlich“ übermittelt wurden, für ihren Unternehmensablauf aber nicht relevant sind, dürfen nicht abgelegt werden. Das Unternehmen ist in der Pflicht bereits im Vorfeld irrelevante Daten auszufiltern und zu bereinigen.

Zweckbindung:
Daten dürfen nicht weitergegeben werden, denn es wird nur einer ganz bestimmten Verwendung zugestimmt. Gibt Ihnen ein Kunde also seine E-Mail-Adresse für ein Angebot für Fenster, dürfen Sie ihm nicht von ihrem Tochterunternehmen ein Angebot für Fenstergitter zukommen lassen.

Datenrichtigkeit:
Das Unternehmen ist dafür selbst dafür verantwortlich, dass alle Daten inhaltlich und sachlich korrekt und aktuell sind.

Datensicherheit:
Hier gilt für Sie was das Wort beinhaltet. Ihr Unternehmen ist dafür verantwortlich, dass niemand unbefugtes, auch innerhalb ihres Unternehmens Zugang erhält.

Löschung von Daten:
Jeder EU-Bürger hat ab sofort das Recht auf die Löschung von Daten innerhalb von bestimmten Fristen. Er hat also ein Recht darauf „vergessen zu werden“. Eine Regelung die es besonders in sich hat. Egal ob Suchmaschinen-Anbieter, Online-Händler oder Energieversorger, alle Unternehmen müssen Datenlöschung gewährleisten und auch selbst nachhalten. Gerade der letzte Punkt bereitet den meisten Unternehmen Kopfschmerzen, denn das Recht auf Widerruf ist bereits bekannt und wird gelebt.

Im Unternehmen selbstständig Datenlöschung und Datenverarbeitung zu kontrollieren, ist für die meisten Unternehmen DAS Problem. Ab sofort müssen alle Daten die ihren Zweck verloren haben, die einen Widerruf durch die Person erhalten oder unrechtmäßig erlangt wurden, vom Unternehmen selbst gefiltert und entfernt werden. Zusätzlich müssen Sie nachweisen, wie Sie an diese Daten gekommen sind.

Verstoßen Sie gegen eine dieser Regeln, dann wird es richtig teuer, denn die neuen Bußgelder sind schmerzlich höher als früher. **Wie hoch?** Die höchste Bußgeldsumme für Einzeltaten liegt bei 20 Millionen Euro, bei Großunternehmen und -konzernen können sich diese bis auf 4% des weltweiten Konzernumsatzes (aus dem Vorjahr) belaufen.

Alle diese genannten Punkte führen für Sie und Ihr Unternehmen zu unweigerlichen Umsetzungen, die Sie bedenken und zum 25. Mai 2018 bereits eingeführt haben müssen.

Holen Sie sich Hilfe von Spezialisten egal ob intern (z. B.: Datenschutzbeauftragten) oder von externen Unternehmen, die sich auf die neue Datenschutz-Grundverordnung spezialisiert haben und ihnen kompetent und objektiv zur Seite stehen, um mit ihnen ins neue digitale Datenschutzzeitalter gehen, Schwachstellen aufzuzeigen und beseitigen sowie aus 99 Dingen, die Ihnen Kopfzerbrechen bereitet haben eine große Sicherheit machen.

Weitere Informationen unter:

www.intense.de

INTENSE AG
Ludwigstraße 20
97070 Würzburg

Tel. 0931 66078 0
Fax 0931 66078 14
Mail info@intense.de