AS infotrack

Umgang mit der Datenschutzgrundverordnung «DSGVO»

Die Datenschutzgrundverordnung der EU, kurz DSGVO, ist zurzeit in aller Munde. Obwohl es sich dabei um Europäisches Recht handelt, reichen die Folgen über die Grenzen der EU hinaus und betrifft auch uns als KMU in der Schweiz. Es gibt wichtige To-dos, die die Informatik betreffen.

Die neue Datenschutzgrundverordnung gilt nicht nur für alle Unternehmen, die ihren Sitz in der EU haben, sondern auch für aussereuropäische Firmen, die auf dem europäischen Markt tätig sind (durch die Möglichkeit eine Webseite in der EU aufzurufen) oder personenbezogene Daten von EU-Bürgern verarbeiten.

Eine «Datenverarbeitung durch Dritte» liegt bereits dann vor, wenn Cloud-basierte Dienste verwendet werden, in denen personenbezogene Daten gespeichert werden. Solche Cloud-basierten Dienste sind beispielsweise Exchange Online, Dropbox, One Drive, Cloud-ERPs und viele weitere. In diesem Fall ist es wichtig auf die Konformität des jeweiligen Dienstes zu achten und/oder das Einverständnis der betroffenen Personen einzuholen.

Die Auswirkungen und Folgen der DSGVO für hiesige Firmen sind noch schwierig abzuschätzen. Als Vorbereitung schlagen wir Ihnen diese wichtigsten Massnahmen vor:

Erstellung eines Datenübersichtsverzeichnisses als Übersicht wo im Unternehmen überall sensible Daten verarbeitet und/oder gespeichert werden und welche Massnahmen zu treffen sind.

Erstellung interner IT- und Datenschutzrichtlinien mit konkretem Bezug auf die unternehmensinternen Abläufe, damit die Umsetzung durch die Mitarbeitenden möglichst reibungslos funktioniert.

Erstellung von Backup- und Notfallkonzept IT-Infrastruktur zur Sicherstellung der Datenintegrität, -Sicherheit und -Verfügbarkeit.

Sichere Verwahrung physischer Akten prüfen bzw. sicherstellen. Sensible Daten sollen nur in Räumen mit begrenztem Zutritt und/oder in abschliessbaren Schränken aufbewahrt werden.

Konzept der Datensparsamkeit prüfen. Hierbei gilt es zu überprüfen, ob allenfalls mehr Daten erhoben werden als für die Geschäftsabwicklung unbedingt notwendig sind.

Datensicherheit mobiler Geräte prüfen, um sicherzustellen, dass im Falle eines Verlusts oder Diebstahls die auf dem Gerät vorhandenen Daten vor unberechtigtem Zugriff geschützt sind.

Sensibilisierung der Mitarbeitenden, um das Bewusstsein für datenschutzrechtliche Probleme zu schaffen und die Mitarbeitenden zu datenschutzkonformem Verhalten zu befähigen.

Vertragliche Anpassungen prüfen, da es allenfalls Hinweistexte zur Begründung der Datenerhebung in bestehenden Verträgen braucht.

Überprüfung der Webseite auf Konformität mit der DSGVO (Datenschutzerklärung, die von jeder Seite aufrufbar ist; Hinweis bei Registrations- und Kontaktformulare sowie Kommentarfunktionen; Hinweis auf Tracking- und Analysedienste).

Erstellung Verarbeitungsverzeichnis (wo werden welche personenbezogenen Daten gespeichert und verarbeitet) inkl. Umsetzung der Massnahmen. Dies ist zwingend für Firmen mit mehr als 250 Mitarbeitenden, kleinere Firmen sind davon nur in Ausnahmefällen betroffen.

AS infotrack AG // Zentrumsplatz 3 // Postfach 61 // 5726 Unterkulm // +41 62 768 50 60 // www.asinfotrack.ch

Personenbezogene Daten

Nach EU-DSGVO sind «personenbezogene Daten» all jene Informationen, die sich auf eine natürliche Person beziehen und so Rückschlüsse auf deren Persönlichkeit erlauben. Beispiele für personenbezogene Daten sind Name, Geburtsdatum, Kontaktdaten wie Adressen und Telefonnummern oder auch andere eindeutige Merkmale wie Kontodaten, Sozialversicherungsnummern oder IP-Adressen.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert und dürfen nur mit ausdrücklicher Einwilligung der betroffenen Person verarbeitet werden.

Auch Bewerbungsunterlagen sind aufgrund der vielen persönlichen Angaben und Zeugnisse hier einzuordnen. Dabei ist beispielsweise zu beachten, dass die Daten rechtzeitig nach besetzen der Arbeitsstelle wieder gelöscht bzw. vernichtet oder zurückgesendet werden.

Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung. Das Speichern und Verarbeiten von personenbezogenen Daten ist daher nur unter Zustimmung des Betroffenen zulässig.

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Einmal erhobene Daten dürfen nicht zu anderen Zwecken als den ursprünglich festgelegten verarbeitet werden und der Zweck muss eindeutig definiert sein.

Meldepflicht & Sanktionen

Wenn der Schutz personenbezogener Daten verletzt wurde, etwa durch eine Datenpanne, muss ein Unternehmen dies innerhalb von 72 Stunden melden. Allerdings besteht eine solche Pflicht nicht, wenn diese Verletzung «voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt». Bei einem Vorfall lohnt es sich für die Einschätzung juristische Unterstützung beizuziehen.

Sehr empfindlich fallen die von der Datenschutzgrundverordnung vorgesehenen Konsequenzen bei Nichteinhaltung der Regelungen aus. Die Geldbussen können bis zu 20 Mio. Euro oder bis zu 4% des gesamten weltweiten Jahresumsatzes betragen.

Unser Angebot

Gerne unterstützen wir Sie bei all diesen Themen, um Ihr Unternehmen für die DSGVO zu wappnen. Hierzu verfügen wir über weiterführende Dokumente, vollständige Checklisten und Vorlagen. Nehmen Sie mit uns Kontakt auf, wir sind gerne für Sie da.

Andreas Gurtner
Bereichsleiter ICT-Services

+41 62 768 50 60
andreas.gurtner@asinfotrack.ch