

HINGESCHAUT

Datenschutz im Blick



Sehr geehrte Geschäftsführungen,
liebe Mandanten,

KW 12/2022

es ist wieder so weit. Wieder einmal weitere Informationen rund um die Themen Datenschutz und Datensicherheit. Auch, wenn Sie vermutlich regelmäßig mit einer Vielzahl von diversen Informationen förmlich zugeschüttet werden, so möchte ich Ihnen dennoch ans Herz legen auch diesmal wieder ein wenig zu schmökern. Durch die Digitalisierung, die unser Leben immer mehr bestimmt, ist die Beachtung von Datenschutz und Datensicherheit sowohl für Unternehmen als auch für Privatpersonen eine absolute Notwendigkeit.

Viel Spaß beim Lesen wünscht Ihnen das Team der DatCon GmbH.

Unverschlüsselte E-Mails – Kritisch oder machbar?

Der Versand der E-Mail musste schnell gehen und ging schnell schief. So in vielen Fällen die Aussage zur versuchten Rechtfertigung von Unternehmen, wenn etwas schief gegangen ist.

Die Realität zeigt, dass die E-Mail nach wie vor eins der intensiv genutzten Kommunikationsmedien ist. Hierüber werden nicht nur Bestellungen für Büromaterial, sondern auch sensiblere personenbezogene Daten, wie bspw. Gesundheitsdaten, verschickt. Aber wie sieht das mit dem notwendigen Schutz aus?

Stellen Sie sich bitte vor, Ihr Unternehmen erhält einen Anruf einer Kundin mit der Bitte bspw. bestimmte Versicherungsverläufe per E-Mail zu senden. Da es schnell gehen sollte, hat sich die Kundin für den E-Mail-Versand entschieden und nicht den postalischen Weg gewählt. Leider gab es einen Schreibfehler der E-Mail-Adresse und die E-Mail mit den sensiblen Inhalten wurde an eine falsche Person geschickt.

Schmerzensgeld? Gerichtliche Auseinandersetzung?

Möglich! Ggf. wird ein Schmerzensgeld wegen des in dem fehlerhaften E-Mail-Versand liegenden Datenschutzverstoßes gefordert. Vielleicht kommt ein Gericht auch zu dem Ergebnis, dass für diese Verarbeitung (Versand von E-Mails) die technischen und organisatorischen Maßnahmen, hier bspw. eine fehlende E-Mail-Verschlüsselung, nicht ausreichend sind. Auch wird immer wieder die regelmäßige Sensibilisierung der Mitarbeiter unter die Lupe genommen.

Einwilligung! Lösung für alles?

Nicht für alles, aber eine Möglichkeit. Man muss ein wenig das Gesamte betrachten. Eine Einwilligung für den Falschversand ist nicht möglich. Wie bekannt sein sollte, wird für jede Verarbeitung eine Rechtsgrundlage benötigt. Leider fehlt diese, wenn die E-Mail an eine falsche Person gelangt. Wir haben in der Regel keine Rechtsgrundlage personenbezogene Daten an eine dritte Person zu geben.

Aber vielleicht kommen wir mit einer Einwilligung für den unverschlüsselten Versand weiter. Das ist dann der Fall, wenn die betroffene Person Versandalternativen hat, wie bspw. den postalischen Weg. Wenn dieser von der betroffenen Person abgelehnt wird, sie aber über die Risiken des E-Mail-Transfers informiert wurde und am Ende in diesen Versandweg eingewilligt hat, greift in der Regel diese Einwilligung. Aber wie in allen Bereichen geht es in erster Linie um vollumfängliche Informationen. Wenn zudem kein Zwang für das Medium „E-Mail“ vorhanden ist, wird die Einwilligung noch mehr unterstützt. Fakt ist dann für die betroffene Person, dass durch die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO ein Verzicht auf

Impressum:

DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

HINGESCHAUT

Datenschutz im Blick



Anonymisierungs-, Pseudonymisierungs- sowie Verschlüsselungstechniken möglich ist.
Zu bedenken ist aber, dass auch ein Kontrollverlust von Daten zu einem Schmerzensgeldanspruch führen kann.

Wie war das noch mit der Aufsichtsbehörde in Österreich?

Die österreichische Aufsichtsbehörde hat im Jahr 2019 den Standpunkt vertreten, dass eine Einwilligung in den unverschlüsselten Versand, hier waren es Patientendaten, unwirksam ist. Die Begründung war seinerzeit, dass die Einwilligung dazu dienen sollte erforderliche Sicherheitsmaßnahmen nicht beachten zu müssen. Daher macht es in der Regel ein Unterschied, ob man alternative Versandmethoden vorhält oder nicht.

Personenbezogene Daten und die Löschpflicht

Richtig ist, dass bspw. für einen Autokaufvertrag diverse personenbezogene Daten benötigt werden. Richtig ist auch, dass diese verarbeitet und gespeichert werden müssen. Alles, was bspw. im Bereich von Handelsbriefen (rund um Angebote, Bestätigung, Rechnung) liegt, muss in der Regel 10 Jahre aufbewahrt werden. Aber jetzt wird das Eis schon ein wenig dünner.

Was ist mit Serviceleistungen, beim Autohaus bspw. die Erinnerung an den TÜV?

Neben der notwendigen Rechtsgrundlage muss auf die Löschpflicht geachtet werden. Je nachdem, ob vorab informiert bzw. diverse Daten regelmäßig benötigt werden, darf man diese im Rahmen der Kundenbetreuung aufbewahren. Ist aber der Zweck der Datenverarbeitung nicht mehr gegeben, müssen die Daten gelöscht werden. Wenn Kundendaten in ein CRM nur für die Abwicklung einer Bestellung aufgenommen worden sind, müssen diese rechtlich betrachtet nach Ablauf der Aufbewahrungsfrist komplett gelöscht werden. Alternativ, man informiert die betroffene Person vorab über einen anderen Zweck bzw. holt sich notwendige Einwilligungen ein. Eine Einwilligung ist auf jeden Fall im Bereich von zusätzliche Serviceleistungen oder auch Weitergabe an Dritte notwendig.

Bußgelder im Februar 2022? *(Textliche Auszüge von Dr-Datenschutz)*

Es ist nur eine **kleine** Übersicht! Aber es sind praxisnahe Fälle, die ggf. auch bei Ihnen auftreten können.

- Werbekampagne mit veralteten Kontaktdaten
Behörde: Garante per la protezione dei dati personali (Italien), Branche: Hörakustik Anbieter
Verstoß: Art. 5 Abs. 2 DSGVO, Art. 6 Abs. 1 lit. a DSGVO, Art. 12 DSGVO, Art. 14 DSGVO, Art. 15 DSGVO, Art. 24 DSGVO, Art. 28 DSGVO, Bußgeld: 30.000 Euro
- Datenpanne bei Gesundheitsunternehmen
Behörde: Garante per la protezione dei dati personali (Italien), Branche: Gesundheitswesen
Verstoß: Art. 5 Abs. 1 lit. f DSGVO, Art. 25 DSGVO, Art. 32 DSGVO, Art. 33 DSGVO, Bußgeld: 20.000 Euro
- Medienunternehmen kommt Auskunfts- und Löschanfragen nicht nach
Behörde: Autoriteit Persoonsgegevens (Niederlande), Branche: Medien
Verstoß: Art. 12 Abs. 2 DSGVO, Bußgeld: 525.000 Euro
- Aufzeichnung und Veröffentlichung einer Zoom-Videokonferenz

Impressum:

DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

HINGESCHAUT

Datenschutz im Blick



Behörde: Agencia española protección datos (Spanien), Branche: Fußballverband
Verstoß: Art. 6 Abs.1 DSGVO und 13 DSGVO, Bußgeld: 200.000 Euro

Fazit?

Die Praxis zeigt, es sind schwerpunktmäßig oftmals die gleichen Verstöße.

Hier sind es bspw. die Bereiche „Rechtsgrundlage“, „Informationspflicht“, „fehlende Beachtung der technischen und organisatorischen Maßnahmen“ und „Löschpflicht bzw. Aufbewahrungsfristen“.

Viele Unternehmen unterschätzen auch die mächtige Unterstützung durch regelmäßige Sensibilisierungsmaßnahmen.

Nicht immer handelt es sich „nur“ DSGVO-Bußgelder. In manchen Fällen kommen auch weitere Zahlungen, wie Schmerzensgeld oder Bußgelder aus anderen rechtlichen Gegebenheiten hinzu.

Sie haben Fragen? Melden Sie sich bitte bei uns! Es bleibt spannend!

Anmerkung: Die Nichtnennung der 3 Personalformen (m, w, d) soll keine Diskriminierung darstellen, sondern lediglich die Lesbarkeit/Umfang verbessern.

Impressum:

DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT