HINGESCHAUT
Datenschutz im Blick

Sehr geehrte Geschäftsführungen, KW 41/2022
liebe Mandanten,

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.

Nutzung von Onlineschriften – Und noch immer Risiken für Bußgelder und Schadensersatz

Eigentlich sollte es mittlerweile bekannt sein. Onlineschriften sollten auf Website nicht mehr auftauchen, wenn diese OHNE Einwilligung genutzt werden. Noch besser und auch sicherer, sie liegen lokal auf dem Webserver.
Das Thema „Nutzung von einwilligungspflichtigen Diensten ohne Einwilligung“ bezieht sich zwar nicht nur auf Onlineschriften, aber diese haben in den letzten Wochen dafür gesorgt, dass es hier zu Abmahnwellen gekommen ist bzw. kommt. Ich hatte hier bereits berichtet.
Was aber mit 100 Euro begonnen hat (Anfang des Jahres, Urteil vom Landgericht München), entwickelt sich zusehends zu sehr viel höheren Schadensersatzansprüchen, die eine Anwältin oder ein Anwalt vom Unternehmen abverlangt.
Am Ende ist es das Unternehmen bzw. die Vielzahl von Unternehmen die diese Gelder zahlen.

TIA – Transfer Impact Assesment. Was steckt dahinter?

„TIA“ – Richtig! Kein „Tier“. Ein TIA ist aus Sicht des Unternehmens eher weniger angenehm.
Es gibt die neuen EU-Standardvertragsklauseln (SCC), die bis zum 31.12.2022 umgesetzt bzw. angewandt werden müssen, sobald es eine Drittlandübermittlung gibt. Das Wort „Drittlandübermittlung“ ist oftmals schon der erste Diskussionspunkt. In der Regel, wie bspw. bei Microsoft oder Amazon, übermitteln deutsche Unternehmen an deutsche bzw. europäische Server des jeweiligen Providers. Also eigentlich keine Drittlandübermittlung. Und doch werden Daten, bspw. Analysedaten, in vielen Fällen direkt in die USA übermittelt. Auch gibt es da ja noch das amerikanische Gesetz (Cloud Act), was den Zugriff für die dortigen Behörden auf deutsche Server ermächtigt.
Also? Dann doch „TIA“.
Gem. Klausel 14 der SCC ist ein TIA eine Art Risikobewertung der Datenübermittlung. Ziel ist es hierbei, dass die Unternehmen durch das TIA eine Analyse des Sicherheitsniveaus des jeweiligen Drittlandes durchführen, in das die Daten übermittelt werden sollen. Ob das vollständig umsetzbar, ist aber eher zweifelhaft.

Warum?
Wie soll die Rechtslage im Drittland, bspw. USA, und die notwendigen Maßnahmen des Unternehmens in diesem Drittland, welches die Daten empfängt, um Schutz dieser Daten vor staatlichen Zugriffen, wie den Sicherheitsbehörden, beurteilt

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

werden? Es geht schlichtweg nicht!
Bedeutet, dass das TIA keine einseitige Aufgabe des Unternehmens in Deutschland ist. Es sollen beide Vertragsparteien (Unternehmen in Deutschland und deutscher/europäische Provider) daran mitwirken.

Und nun?
Wenn wir bei Microsoft bleiben, dann hat man gehofft, dass es hier eine erste Version geben sollte. Ist aber bis dato nicht passiert, es gab Hinweise und Regelungen. Nun gehen wir vom Besten aus, dass es hier und auch bei anderen Providern nur eine Sache der Zeit ist und das TIA von denen kommt. Dennoch ist aus Sicht des Datenschutzes auf jeden Fall zu empfehlen, dass man sich mit dem Thema auseinandersetzt. Als Auftragsverarbeiter wird man immer häufiger nach einer solchen Dokumentation gefragt.

E-Mail- und Internet-Nutzung am Arbeitsplatz. Warum sollte dies geregelt werden?

Warum sollte man als Unternehmen die Nutzung von E-Mail und Internet regeln? Hier geht es insbesondere um das Thema „Privatnutzung“. Die Antwort ist recht simpel. Dem Unternehmen gehört die Infrastruktur inkl. aller (geschäftlichen) Daten. Und hierüber hat das Unternehmen auch die komplette Verantwortung.
Bedeutet, dass es keine Durchmischung von geschäftlichen mit privaten Daten geben sollte. Solange alles so läuft und kein Bedarf besteht, dass man bspw. auf E-Mails von ehemaligen Mitarbeiter*innen zugreifen muss, ist alles paletti. Nun kommt aber ein solcher Fall. Und? Viele Unternehmen haben ein Problem, denn sie dürften es eigentlich nicht.

Warum?
Das Unternehmen hat eine private Nutzung NICHT verboten. Aber genau das ist der erste Schritt. Der zweite Schritt ist, dass sich die Geschäftsführungen von den ausscheidenden Mitarbeiter*innen bestätigen lassen, dass diese ihre E-Mail-Postfächer bzgl. möglicher privater E-Mails geprüft und ggf. diese gelöscht haben. Dann kann ein Zugriff bedenkenlos erfolgen.
Sind diese beiden Faktoren NICHT erfüllt, drohen Probleme bzgl. der Missachtung u.a. des TTDSG (Telekommunikation Telemedien Datenschutzgesetz) oder auch der DSGVO.

Und nun?
Auf jeden Fall das Verbot der Privatnutzung schriftlich aussprechen. Private E-Mail-Postfächer können heutzutage ohne weiteres auf dem privaten Handy geprüft werden.
§ 26 Abs. 1 Satz 1 BDSG ist für das Unternehmen wichtig, wenn dieses Zugriff auf das Postfach benötigt. Demnach darf der Arbeitgeber für Zwecke des Beschäftigungsverhältnisses mit Mitarbeiterdaten umgehen und diese verarbeiten, wenn er für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Gem. dem BayLDA gibt es die klare Empfehlung, dass E-Mail-Postfächer ausgeschiedener Mitarbeiter*innen möglichst zeitnah gelöscht werden. So erhalten die jeweiligen Absender eine Fehlermeldung und müssen sich bzgl. einer Kontaktaufnahme an das jeweilige Unternehmen wenden.

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

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

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

- Unzulässige Werbeanrufe mit unterdrückter Nummer
  Behörde: Information Commissioner‘s Office (UK), Branche: Handwerk/Dienstleister
  Verstoß: Reg. 21 PECR (Privacy and Electronic Communication Act), Bußgeld: 167.626 EUR
- Personalausweiskopie zu Unrecht verlangt
  Behörde: Agencia española protección datos (AEPD), Branche: Bankwesen
  Verstoß: Art. 5 Abs. 1 lit. c DSGVO, Bußgeld: 42.000 EUR
- Verstoß gegen Speicherbegrenzung und keine sicheren Passwörter
  Behörde: Commission Nationale de l'Informatique et des Libertés (CNIL), Branche: Wirtschaftliche Interessenvereinigung, Verstoß: Art. 5 Abs. 1 lit. e DSGVO, Art. 32 Abs. 1 DSGVO
  Bußgeld: 250.000 EUR
- Verstoß gegen Datenschutzrechte für Kinder
  Behörde: Data Protection Commission (Irland), Branche: Social-Media-Plattform
  Verstoß: Art. 5 Abs. 1 lit. a und c DSGVO, Art. 6 Abs. 1 DSGVO, Art. 12 Abs. 1 DSGVO, Art. 24 DSGVO, Art. 25 Abs. 1 und 2 DSGVO, Art. 35 Abs. 1 DSGVO, Bußgeld: 405.000.000 EUR
- Missbräuchliche Verwendung von Grundbuchdaten
  Behörde: LfDI Baden-Württemberg, Branche: Bauunternehmen
  Verstoß: Art. 5 Abs. 1 lit. b DSGVO, Art. 6 Abs. 1 lit. f DSGVO, Art. 14 DSGVO, Bußgeld: 50.000 EUR

Fazit?

Diesmal hat es Instagram mit satten 405 Mio. Euro erwischt. Personenbezogene Daten von Minderjährigen haben einen höheren Schutzanspruch. Aber auch die Aufsicht Baden-Württemberg hat ein „nettes“ Bußgeld ausgesprochen. Wir sind immer wieder froh, wenn die Unternehmen, die wir betreuen dürfen, einen solchen Bußgeldbescheid oder auch einen Brief vom Anwalt nicht erhalten. Aber realistisch betrachtet, die „Einschläge kommen näher“. Auch, wenn das Unternehmen für ein TIA keine Zeit hat, die gesetzliche Anforderung ist gegeben.
Und Privatnutzung von E-Mails? NEIN! Die Beschwerde-Level von Menschen, hier die (ehemaligen) Mitarbeiter*innen, sinkt immer weiter. Ein Unternehmen muss an diverse Punkte denken, um sich hinsichtlich Beschwerden bzw. möglicher Bußgelder abzusichern.
Eine Abmahnung aufgrund der Nutzung von Onlineschriften bedeutet auf jeden Fall Stress. Das Unternehmen wird gewissermaßen legal erpresst → entweder zahlt es oder der „Geschädigte“ spielt die Karten im Bereich der Möglichkeiten aus.

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