

HINGESCHAUT

Datenschutz im Blick



Sehr geehrte Geschäftsführungen,
liebe Mandanten,

KW 15/2023

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.

ChatGPT, Chatbots und die „neue“ Unterstützung

Kürzlich habe ich eine Information meiner Versicherung erhalten. Diese schrieb: „... *Wir dürfen Sie beglückwünschen. Ab sofort steht Ihnen unser neues digitale Team für Fragen zur Verfügung. ...*“. Gut? Schön? Jeder muss für sich diese neue Art der Unterstützung bewerten. Aber aus Sicht des Datenschutzes bzw. der Datensicherheit kann man nur sagen: „Achtung!“.

Warum? Ist das nicht sicher genug?

Man muss ein wenig hinter die Kulissen schauen. Irgendwo werden ja nun Ihre Daten im Rahmen von Anfragen verarbeitet. In der Regel erfolgt dies auf Strukturen mit Drittlandbezug. Für Unternehmen kritisch, da es hier rechtliche Probleme gibt. Wer von Ihnen hat schon einmal eine solche Technik genutzt? Hierbei geben Sie Fragen oder Probleme ein und eine Technik mit künstlicher Intelligenz (KI) antwortet Ihnen. Hierbei werden Wissensdatenbanken weltweit durchsucht und mit Möglichkeiten der KI kombiniert. Was dann dort herauskommt, ist in sehr vielen Fällen richtig.

Den kleinen Nebeneffekt, dass es dort nicht ausreichende Regularien, wie bspw. den Jugendschutz, gibt, lassen wir heute außen vor. Auch die Themen Urheberrecht, Marken, Patente und Co. betrachten wir heute ebenfalls nicht..

Hier betrachten wir „nur“ den Datenschutz bzw. die Datensicherheit. Das Ergebnis zeigt, dass Tools, wie ChatGPT, für Betrug oder im Bereich der Cyberkriminalität missbraucht werden können. Man fragt nach Unternehmensinformationen und erhält sie von der neuen digitalen Unterstützung. Und das sogar kostenfrei.

Fazit?

Nein, die Entwicklung der KI können wir nicht mehr aufhalten. Aber die Unternehmen, und zwar JEDES, muss ganz schnell über den Tellerrand schauen, sofern noch nicht geschehen. Die Mitarbeiter*innen müssen geschult werden. Auch müssen Richtlinien für die Nutzung solcher Tools festgelegt werden. Und, wenn ein Unternehmen, wie bspw. meine o.g. Versicherung, diese Art von Techniken nutzen möchte, dann muss aus Sicht des Datenschutzes das Risiko betrachtet werden. Zudem müssen Betroffene ausreichend informiert werden.

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



Chatbot – Auch KI?

Chatbots werden in Unternehmen immer beliebter. Man stellt einen neuen Service auf der Website zur Verfügung. Hier können dann die Besucher Fragen zu Produkten o. ä, stellen. Klingt erst einmal gut. Ja, auch hier bewegen wir uns oftmals im Bereich der KI.

Und aus Sicht des Datenschutzes? Ok? Kritisch?

Wie bei allen anderen Bereichen müssen auch hier ein paar Punkte beachtet werden:

Beachtet man diese nicht, dann muss ein Unternehmen mit Problemen, Beschwerden und Bußgeldern rechnen.

Aber auch, wenn das Unternehmen weitestgehend alles umsetzt, heißt es nicht, dass es absolut problemlos läuft. Menschen denken unterschiedlich, was bedeutet, dass man als Unternehmen dennoch in kritische Situationen kommen kann.

Folgende Punkte sind das Mindestmaß, an was beachtet werden sollte:

- Recht auf Vergessenwerden/ Recht auf Löschung → die erfassten Daten dürfen nicht dauerhaft im System bleiben
- Datenauskunft → Kommen Anfragen von Nutzern, dann müssen diese innerhalb von max. 30 Tagen beantwortet werden.
- Einwilligung notwendig → Die Rechtsgrundlage! Wir benötigen für die Verarbeitung diese und in der Regel ist es eine Einwilligung.
- Auftragsverarbeitung → Externer Dienstleister mit dabei? Dann benötigen wir eine AVV.
- Datenschutzerklärung → Man muss gem. Art. 13/14 DSGVO die betroffene Person informieren. Dies erfolgt in der Regel in der Datenschutzerklärung auf der Website.

Fazit?

Ob gut, schlecht oder innovativ wichtig muss jedes Unternehmen auch hier wieder selbst entscheiden.

Wichtig ist aber, die oder den Datenschutzbeauftragte/n mit ins Boot holen. Ok, die/der spricht nicht immer „ins gleiche Horn“. Aber das soll sie/er ja auch nicht. Das Unternehmen sollte aber vorab ein paar Szenarien durchdenken.

Fernwartung mit Teamviewer

Teamviewer ist ein sehr beliebtes Fernwartungstool, was auch wirklich gut ist. Aber Zoom und Microsoft Teams sind auch gut, aber nicht datenschutzkonform. Bei Teamviewer verhält es sich wie bei vielen anderen Dienstleistern auch, man verlagert Dienste in Strukturen mit Drittlandbezug, wie bspw. Amazon Web Services (AWS). Oder, und davon kann sich KEIN Unternehmen freisprechen, man kämpft gegen Cyber-Attacken, bei denen dann Benutzerkonten gehackt werden und man so auf Serverstrukturen von Unternehmen gelangt.

Eine solche Verlagerung gab es bei Teamviewer. Da Unternehmen, die Teamviewer nutzen, eine Auftragsverarbeitung vereinbaren müssen, sind sie somit für diesen Dienstleister und die Beachtung aller datenschutzrechtlichen Anforderungen verantwortlich.

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



Und nun?

Man muss die Risiken abwägen. Die Praxis zeigt, dass die Nutzung von Infrastrukturen mit Drittlandbezug immer mehr Einzug nimmt. Ob und wann sich rechtliche Anforderungen dahingehend ändern, bleibt ungewiss. Ziel sollte sein, dass man nachweislich in Richtung Datenschutzkonformität geht und eine Optimierungsmöglichkeit stetig prüft.

Cyberattacken aus März 2023 in Deutschland *(Textliche Auszüge aus www.dsgvo-portal.de)*

Vorab, es geht hier nicht ums „Angstmachen“. Vielmehr ist das Ziel die Sensibilisierung
→ „So etwas ist ja auch bei uns vorgekommen.“

- Hahn Group
Hacker kompromittieren Netzwerke
- Badewelt Sinsheim
Hacker greifen Daten von Newsletter-Abonnenten ab
- Deutsches Rotes Kreuz
Attacken auf Netzwerk mit dem Ziel, dass die Server zusammenbrechen
- Helmholtz Zentrum München
Ausfall der Telekommunikationseinrichtungen nach einem Cyber-Angriff
- Ortho Form Sauerland
Hacker erbeuten Daten der internen Server

Europäische Bußgelder im März 2023? *(Textliche Auszüge von Dr-Datenschutz)*

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

- Bußgeld wegen permanentem Tracking bei Benutzung von Mietrollern
Behörde: Commission Nationale de l'Informatique et des Libertés
Branche: Roller Sharing-Anbieter
Verstoß: Art. 5 Abs. 1 lit. c) DSGVO, Art. 28 Abs. 3 DSGVO, Art. 82 La loi Informatique et Libertés
Bußgeld: 125.000 Euro
- Fehlende technische und organisatorische Maßnahmen
Behörde: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
Verstoß: Art. 32 Abs. 1 lit. b), c) DSGVO, Art. 32 Abs. 2 DSGVO
Bußgeld: 2.992 Euro
- Fehlerhafte Daten müssen gelöscht werden – sonst wirds teuer
Behörde: Tietosuojavaltuutetun toimisto
Branche: Kreditschutzorganisationen
Verstoß: Art. 5 Abs. 1 lit. a), d) DSGVO

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



Bußgeld: 440.000 Euro

- Verspätete Meldung eines Sicherheitsvorfalls

Behörde: Datatilsynet

Branche: Medizinische Verbrauchsgüter

Verstoß: Art. 33 DSGVO

Bußgeld: 218.365 Euro

- Unrechtmäßige Weitergabe von Kontodaten an Dritte

Behörde: Datenschutzaufsichtsbehörde Griechenland

Branche: Bankensektor

Verstoß: Art. 5 Abs. 1 lit. a), f) DSGVO, Art. 33 DSGVO, Art. 34 DSGVO

Bußgeld: 30.000 Euro

Fazit?

Hach, was soll man sagen. Bleiben Sie wachsam und prüfen Sie regelmäßig Ihre Infrastruktur. Auch sollten Dienstleistungen bzw. Dienstleister regelmäßig auf Datenschutzkonformität geprüft werden.

Früher waren sogenannte Penetrations-Tests nur etwas für sehr ausgewählte Unternehmen. Diese Pen-Tests waren früher und sind heute noch immer teuer. Aber durch die Digitalisierung und enorme Steigerung der Cyber-Risiken sollten Unternehmen überlegen, dass solche Tests regelmäßig gemacht werden. Auch diese stellen „nur“ einen weiteren, aber wichtigen, Baustein im Bereich der Sicherheit dar.

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