

# HINGESCHAUT

## Datenschutz im Blick



Sehr geehrte Geschäftsführungen,  
liebe Mandanten,

KW 51/2023

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.

### **E-Mail. Fake oder nicht.**

E-Mails sind alles andere als tot. Das hat man noch vor ein paar Jahren gemeint. 😊

Cyberangriffe starten oftmals über eine E-Mail. Auf was sollte man nun achten? Stellen Sie sich immer diese Fragen:

- Ist der Absender bekannt? Name UND echte E-Mail-Adresse prüfen.
- Soll etwas „Komisches“ unternommen werden? Ok, „komisch“ ist relativ. Passt die vom Absender gewünschte Handlung zum Unternehmen bzw. dem Absender?
- Macht die E-Mail überhaupt Sinn?
- Soll etwas schnell passieren? Wird Druck aufgebaut?
- Sollen persönliche Informationen herausgegeben werden? Ist da etwas ausstehend, was diese Angaben begründet?

Fazit?  
Die Fragen im Hinterkopf zu haben ist zwar keine hundertprozentige Lösung. Aber das Denken daran unterstützt zumindest.

### **Angriffe auf das IT-System OHNE Technik**

Ohne Technik? Also ist der Mensch im Mittelpunkt.  
Man hört es immer in den Medien. Aber keiner glaubt so richtig daran, dass es einen selbst treffen kann. Und es ist so einfach ...

Phising  
Kennen sie, man versucht Sie irgendwie zur Herausgabe von Informationen zu überrumpeln. Entweder konkrete Daten zur möglichen Anmeldung oder man erstellt ein Profil über Sie.  
Der Versuch läuft oftmals über E-Mails ab.

#### 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](mailto:sorge@DatCon.de) | Web [www.DatCon.de](http://www.DatCon.de)

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

# HINGESCHAUT

## Datenschutz im Blick



### Baiting

Kennt vielleicht nicht jeder.

„Interessante“ Hilfsmittel, wie ein USB-Stick oder auch eine USB-Powerbank, kommen ins Spiel. Es wird geködert. Der neugierige Mensch möchte wissen, was da so drauf ist oder freut sich, dass er eine Powerbank geschenkt bekommen hat. Die Freude trübt dann schnell, wenn man irgendwann merkt, dass das kleine Tool auf diesem Hilfsmittel die Tastatureingaben protokolliert.

Und ganz ehrlich. Wer nutzt virtuelle Tastaturen, um Zugangsdaten einzugeben?

### Piggybacking

Oder wie kommt man huckepack ins Unternehmen?

Wenn man in ein Unternehmen hineinkommen möchte, so kann auch der klassische Weg interessant sein. Natürlich unerkannt. Und das ist dann, wenn die Türen sehr häufig geöffnet sind, wie bspw. Arbeitsbeginn, Pausen oder Arbeitsende. Oder die Türen sind für einen gewissen Zeitraum, bspw. tagsüber, für Besucher auf.

So, man hat es geschafft. Nun kann man in aller Ruhe und mit ein wenig Fantasie Zugriff auf die technische Umgebung sich verschaffen.

### Fazit?

Klar ist, dass kleinere Unternehmen solche Szenarien vermutlich nicht erleben, da man sich sehr gut kennt. Aber sobald viel Kundschaft in den Laden kommt, kann es schon ein Risiko sein, wenn es ein Leichtes ist an technische Geräte unerkannt heranzukommen.

## 2024 und die Datenschutzaufsichten

Ja, Datenschutz ist und bleibt ein Brennpunkt. Die einen vertreten die Meinung, dass es immer schlimmer wird, die anderen möchten noch mehr Klarheit und Schutz. Wie so oft ist vermutlich aus Sicht der Praxis das Ziel irgendwo in der Mitte.

Ein Unternehmen muss sich den eigenen, für sich selbst vertretbaren, Weg suchen. Bestenfalls mit Unterstützung durch Datenschutzberater und natürlich möglichst datenschutzkonform.

Da muss man schon schmunzeln, wenn man hört, dass der Datenschutz schuld sein soll, wenn ein Unternehmen, hier war es eine weiterführende Schule, keine ausreichende Datensicherung hat. Die Begründung war, dass dies eben der Datenschutz verbietet. Totaler Quatsch. Genau das Gegenteil ist der Fall.

Nun dürfen sich Lehrer und Schüler Gedanken machen, wie sie wieder zu ihren Unterlagen kommen, die teilweise abiturvorbereitend waren.

Eine Befragung von Unternehmen zeigt die Wahrheit auf. 92 % der Unternehmen sind sich mittlerweile bewusst, dass das Thema Datenschutz ein Dauerbrenner ist und eigentlich nie abgeschlossen werden kann.

Nehmen wir nur mal das Cyberrisiko. Dieses Risiko steigt unermüdlich. Das wiederum bedeutet, dass Unternehmen reagieren müssen, damit zum einen sie geschützt bleiben und zum anderen die Anforderung gem. Art. 32 DSHVO erfüllen. Hier steht, dass der Schutz ausreichend sein muss. Also stetig prüfen und anpassen. Und genau das prüfen die

### 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](mailto:sorge@DatCon.de) | Web [www.DatCon.de](http://www.DatCon.de)

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

# HINGESCHAUT

## Datenschutz im Blick



Aufsichtsbehörden immer häufiger.

Oder die Betroffenenrechte. Die Nutzung von Cloud-Diensten steigt immer mehr. Hier sollten Unternehmen darauf achten, dass Betroffenenanfragen korrekt und vollständig umgesetzt werden können. Wissen Sie als Unternehmen alles Notwendige von Ihrem Cloud-Dienstleister? In den wenigsten Fällen ist das der Fall. Also fahren wir hier schon einmal im Nebel.

Oder auch der grenzüberschreitende Datentransfer. Den gibt es, den wird es auch weitergeben. Insbesondere für Unternehmen, die globaler aufgestellt sind. Oder sehr innovativ ausgeprägte Adern haben.

Und schon haben wir die nächste Diskussion mit der Aufsicht. Warum keine Alternativen? Und, wenn das Produkt, welches aus Sicht der DSGVO nicht datenschutzkonform umgesetzt werden kann, dann nicht mit möglichst vielen Ansätzen, damit eben doch der Datenschutz nicht gänzlich wegfällt?

Oder die KI-Frage?

Ok. Die stellen wir uns heute nicht, das würde zu weit führen.

Mal schauen, was der ai-Act so schafft, welcher ein Regulierungsansatz der EU für die künstliche Intelligenz ist bzw. sein soll.

<https://digital-strategy.ec.europa.eu/de/policies/european-approach-artificial-intelligence>

Fazit?

Schon jetzt, es bleibt spannend. Unternehmen müssen einfach, ob sie wollen oder nicht, die Themen Datenschutz und Datensicherheit in ihre Planungen mit aufnehmen. Sie sollten es zumindest in ihrem eigenen Interesse.

### Hilft ChatGPT als Mittäter bei Cyberangriffen?

Geht das überhaupt. Wie würde jetzt mein Kollege aus Köln sagen: „Aber sischa dat.“

KI kann viel mehr als die meisten von uns erahnen können. Und es wird mehr.

Folgende Frage ist essenziell: Wie müssen Verteidigungsstrategien erarbeitet bzw. angepasst werden, damit KI-gesteuerte Angriffe möglichst nicht das Ziel erreichen?

KI unterstützt bspw. immer mehr die Perfektionierung der Gestaltung von Phishing-Mails. KI lernt stetig und somit sieht eine bisherige Phishing-Mail nicht mehr so „gruselig“ aus, wenn KI dabei hilft.

Ablauf eines Angriffes?

- Schritt 1: Der Erstzugriff: erfolgt in der Regel durch Phishing.
- Schritt 2: Es wird erkundet und gesammelt. Welche Konten könnten interessant sein?
- Schritt 3: Nun greift man auf Anmeldeinformationen zu.
- Schritt 4: Man hat durch die Vielzahl der gesammelten Informationen dem System eine falsche Identität vorgespielt. Nun hat man dauerhaften Zugriff. Die Daten kommen nun „frei Haus“.

#### 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](mailto:sorge@DatCon.de) | Web [www.DatCon.de](http://www.DatCon.de)

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

# HINGESCHAUT

## Datenschutz im Blick



Fazit?  
Kann man etwas dagegen machen? Oha, ein Nein wäre falsch. Aber ein klares Ja ist auch nur bedingt richtig. Fakt ist, dass eine weitere Anforderung der DSGVO eingehalten werden muss, nämlich „Privacy by Default“. Unternehmen müssen sich anpassen.

### Cyberattacken aus November 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.“

- Deutsche Energieagentur  
Das Unternehmen erleidet einen Ransomwareangriff.
- Münchener Verkehrsgesellschaft  
Angriff auf die Website
- Verkehrsverbund Nürnberg  
Angriff auf die Website
- Gräbener Maschinenteknik  
Hacker greifen auf interne Datenbanken zu
- Stadt Berlin  
Angriff auf die Website

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

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

- Millionenbußgeld für Arbeits- und WohlfahrtsverwaltungBehörde: Agencija za zaštitu osobnih podataka (AZOP)  
Behörde: Datatilsynet  
Branche: Behörde  
Verstoß: Art. 5 Abs. 2 DSGVO, Art. 24 Abs. 1, Abs. 2 DSGVO, Art. 32 Abs. 1, Abs. 2 und Abs. 4 DSGVO  
Bußgeld: 1.706.994 Euro
- Gesundheits- und Führungszeugnis für den Kursbesuch  
Behörde: Agencia Española de Protección de Datos (AEPD)  
Branche: Ausbildungs-/ Schulwesen  
Verstoß: Art. 5 Abs. 1 lit. c DSGVO, Art. 6 Abs. 1 DSGVO, Art. 9 Abs. 2 DSGVO  
Bußgeld: 72.000 Euro
- Gesundheitsdaten im Lost Place  
Behörde: Garante per la protezione dei dati personali (GPDP)  
Branche: Gesundheitswirtschaft

#### 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](mailto:sorge@DatCon.de) | Web [www.DatCon.de](http://www.DatCon.de)

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

# HINGESCHAUT

## Datenschutz im Blick



Verstoß: Art. 5 Abs. 1 lit. a, e, f DSGVO, Art. 32 DSGVO, Art. 75 codice della privacy  
Bußgeld: 50.000 Euro

- Mülldaten nicht entsorgt

Behörde: Autoriteit Persoonsgegevens

Branche: Gemeinde

Verstoß: Art. 5 Abs. 1 lit. a DSGVO, Art. 6 Abs. 1 lit. e DSGVO, Art. 14 Abs. 1 lit. c, d DSGVO

Bußgeld: 30.000 Euro

- GPS-Überwachung von Dienstfahrzeugen

Behörde: Commission Nationale pour la Protection des Données (CNPD)

Branche: Behörde / öffentliche Stelle

Verstoß: Art. 13 DSGVO, Art. 5 Abs. 1 lit. b DSGVO

Bußgeld: 2.500 Euro

Es geht nicht vorrangig um das Bußgeld. Auch nicht welche Behörde zuständig war. Die Unternehmen sollen sich hier bspw. die Fragen stellen: „Kann uns das auch passieren? Oder ist das auch bei uns so?“

### Gesamtfazit?

Das Jahr 2023 war schon recht turbulent, nicht nur im Bereich Datenschutz. Auch, wenn Unternehmen an vielen Fronten kämpfen müssen, so ist es wichtig die Unternehmensstrategie stetig zu prüfen und ggf. anzupassen. Hierunter dann auch der Bereich Datenschutz und Datensicherheit.

Eins der Top 5 – Bußgelder betrifft den Bereich GPS. Aus Erfahrung weiß ich nun, dass immer mehr Unternehmen diese Technik aus verschiedenen Gründen einsetzen wollen. Gerade bei solchen diskussionsreichen Themen sollte man lieber eine Runde mehr drehen um wirklich alle Risiken, Möglichkeiten bzw. Alternativen zu prüfen.

Risiken, wie KI, entwickeln sich. Macht man als Unternehmen nichts, droht eine massive Cyberattacke, die erfolgreich auf der ganzen Linie abläuft und am Ende feststellen muss, dass das Unternehmen keine Daten mehr hat um diese zu bearbeiten. ENDE!

### Was kommt in der nächsten Ausgabe von HINGESCHAUT?

Schauen wir mal. 😊

Ein Thema wird aber das „**Die verheerenden Folgen von Datenmissbrauch**“ sein.

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

*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](mailto:sorge@DatCon.de) | Web [www.DatCon.de](http://www.DatCon.de)

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT