HINGESCHAUT
Datenschutz im Blick

Sehr geehrte Geschäftsführungen,
liebe Mandanten,

KW 38/2023

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.

Löschen, löschen, immer wieder löschen

Ja, ja, nichts Neues. Oder doch? Unternehmen sind gem. der DSGVO verpflichtet, personenbezogene Daten, wie bspw. von Kunden, aber auch von Mitarbeiterinnen und Mitarbeitern, sicher zu löschen. Manche Unternehmen meinen nun, dass dies „mal so eben“ von der IT gemacht werden kann.
Achtung! Ein gefährlicher Irrglaube. Denn hierfür ist ein Konzept, ein Datenlöschkonzept, notwendig. Oder zumindest sehr zu empfehlen.

Warum nun wieder noch mehr Bürokratie? Warum nun ein Datenlöschkonzept?
Die DSGVO zeigt auf, dass Unternehmen auf Datenminimierung achten müssen. Zudem muss auf die Zweckbindung geachtet werden. Aus diesen beiden Grundsätzen ergibt sich nun die Notwenigkeit des fristgerechten Löschens.
Und das Ganze sollte dokumentiert werden, damit alle Mitarbeiterinnen und Mitarbeiter darüber Bescheid wissen. Aber auch, dass man dies bei einer möglichen Prüfung nachweisen kann.

Wie nun?
Grundsätzlich muss regelmäßig geprüft werden, wann welche Datenkategorie gelöscht werden muss. Aber dazu muss das Unternehmen erst einmal Klarheit haben über alle Datenkategorien. Also muss man diese erst einmal herausfinden, um im nächsten Schritt zu sehen, ob und welche Rechtsgrundlage zur Verarbeitung vorhanden ist bzw. wann die Löschung umgesetzt werden muss.

Ist ein Datenlöschkonzept schnell umgesetzt?
Nein, eigentlich nicht wirklich. Aber es kommt wie immer darauf an. Je nachdem mit welcher Wichtigkeit das Unternehmen diese Aufarbeitung betrachtet. Auf jeden Fall ist ein solches Konzept nicht statisch. Es muss regelmäßig auf Aktualität und Vollständigkeit geprüft werden.

Fazit?
Je früher die Unternehmen sich mit diesem Thema befassen, je eher liegt eine belastbare Dokumentation vor, die hilft Bußgeldrisiken oder sogar Schadenersatzansprüche zu senken. Schadenersatz? Korrekt. Nämlich dann, wenn personenbezogene Daten nach einer erfolgreichen Cyberattacke im Darknet gefunden wurden, obwohl diese eigentlich

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

schon längst hätten gelöscht werden müssen.

Hackerangriff bei Microsoft oder der mysteriöse Schlüssel

Was war passiert?
Im Juli 2023 wurden Mail-Postfächer einiger Regierungsbehörden der USA und westeuropäischer Staaten gehackt. Verantwortlich gem. Microsoft sollte die Gruppe „Storm-0558“ gewesen sein. Mittlerweile ist bekannt, dass sich die Angreifer nicht nur Zugang zu E-Mails verschaffen konnten.
Aber leider noch mehr …

Weiter ist bekannt, dass die Angreifer einen Microsoft account (MSA) consumer key erbeuten konnten. Diese Art von Schlüssel wird für die Anmeldung von Endnutzern bei Microsoft Diensten wie bspw. Outlook Online verwendet. Genauer gesagt, es konnten dann Zugangstoken zu einer Vielzahl an Microsoft Services, wie bspw. Teams und SharePoint, gefälscht werden.

Wie sieht die Bedrohungslage aus?
Phishing und Identitätsdiebstahl mit Daten aus MS Teams & SharePoint sind möglich.
Auch, wenn gem. Microsoft den gestohlenen Schlüssel gesperrt wurde und mit diesem Schlüssel signierte Tokens nicht länger gültig sind, so steht dennoch fest, dass aktiv Einsicht in E-Mails und deren Anhänge genommen werden konnte.
Auch besteht die Möglichkeit, dass mit der Mail-Adresse verknüpfte Dienste mittels einer „Passwort zurücksetzen“-Funktion gefährdet sind. Sofern eine unberechtigte Person so an das Passwort kommt, hat diese Person Vollzugriff auf die jeweiligen Dienste.

Fazit?
Stärkung der Awareness bei Angestellten! Ihre Mitarbeiterinnen und Mitarbeiter müssen auf „komische“ E-Mails oder auch ungewöhnliche Aktivitäten vom System bzw. der Software achten. Jede noch so kleine Veränderung sollte zur Sicherheit der IT gemeldet werden.
Wenn Sie betroffen sind, sollten Sie zu Ihrer Sicherheit alle Microsoft-Passwörter ändern.

Auch Geschäfts- oder Kooperationspartner können ein Risiko sein

Kooperationen sind gut. Aber Outsourcing ist nicht unkritisch. Kooperationen mit Drittpartnern haben viele Vorteile, aber auch Risiken.

Warum?
Die Kooperationspartner haben nicht selten Zugriff auf Daten. Das müssen nicht nur personenbezogenen Daten, es können auch sensible Unternehmensdaten sein.
Und nicht selten erfolgt der Zugriff von unternehmensfremden Strukturen aus. Wie steht es aber hier mit der Sicherheit

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

bzw. dem Risiko von Hacker-Angriffen?

Welche Risiken sollten grundsätzlich betrachtet und bewertet werden?

- IT-Security-Risiken
- Reputationsrisiken
- Finanzielle Risiken
- Betriebsrisiko

Fazit?
Es gilt wie immer die Risiken zu reduzieren.
Das bedeutet, dass der zukünftige Partner, je nach Art der Unterstützung bzw. Zusammenarbeit, vorab geprüft werden sollte. Auch sollte man sich von dem zukünftigen Partner die Vertraulichkeit und Sicherheit bestätigen lassen. Klar muss aber sein, dass es hier keine einhundertprozentige Standardisierung gibt. Zu vielfältig sind die Kooperationsmöglichkeiten.

Cyberattacken aus August 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*."

- Astrid-Lindgren-Schule
  Hacker verschlüsseln Server der Schule
- Regierung von Mecklenburg-Vorpommern
  Hacker attackieren Server
- Jodel
  Daten von Nutzern von Social-Media-App erlangt
- Münchner Verlagsgruppe
  Ransomware-Angriff
- S-Bahn Hannover
  Website fällt nach Attacke aus

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

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

- Echte Gesundheitsdaten auf Informationsplakat
  Branche: Gesundheitswesen
  Verstoß: Art. 5 Abs. 1 lit. a, c und f DSGVO, Art. 9 DSGVO, Art. 25 DSGVO, Art. 2-septies (8) Codice della privacy
  Bußgeld: 20.000 Euro

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

- Daten von 650.000 Kunden einsehbar
  Behörde: Datainspektionen (IMY)
  Branche: Versicherung
  Verstoß: Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 DSGVO
  Bußgeld: 2.945.632 Euro
- Empfänger versehentlich in CC gesetzt
  Behörde: La Agencia Española de Protección de Datos (AEPD)
  Branche: Verkehr
  Verstoß: Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 DSGVO
  Bußgeld: 4.800 Euro
- Fotos von fremdem Kind veröffentlicht
  Behörde: La Agencia Española de Protección de Datos (AEPD)
  Branche: Immobilien
  Verstoß: Art. 5 Abs. 1 lit. c DSGVO
  Bußgeld: 6.000 Euro
- Vielfältige Fehler im Consent-Management
  Behörde: La Agencia Española de Protección de Datos (AEPD)
  Branche: Website
  Verstoß: Art. 22 Abs. 2 LSSI
  Bußgeld: 6.000 Euro

Fazit?

Sicher war die Welt der IT noch nie. Wird sie auch nie werden. Je digitaler ein Unternehmen ist, je mehr Risiko ist vorhanden. Und diesmal meine ich nicht nur die IT-Sicherheit, sondern auch den Datenschutz. Den Unternehmen muss klar sein, dass jede erfolgreiche Cyber-Attacke eine Datenpanne gem. der DSGVO bedeutet.
Was dann kommt, ist in der Regel nicht angenehm.

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