HINGESCHAUT
Datenschutz im Blick

Sehr geehrte Geschäftsführungen,
liebe Mandanten,

KW 50/2022

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.

BEM – Welche Daten vom Betrieblichen Eingliederungsmanagement darf der Betriebsrat vor der Kündigung von Mitarbeitern erhalten?

Gem. § 102 Abs. 1 S. 1, 2 BetrVG muss der Arbeitgeber vor Ausspruch einer Kündigung den Betriebsrat anhören und ihm die wesentlichen Kündigungsgründe mitteilen, sofern ein solcher vorhanden ist. Insbesondere krankheitsbedingte Kündigungen sorgen in der Praxis aber regelmäßig für Diskussionen und Beschwerden. Hierbei ist immer eine Frage präsent: „Welche personenbezogenen Daten muss bzw. darf der Arbeitgeber dem Betriebsrat mitteilen?“ Aufgrund der Inhalte eines möglicherweise zuvor durchgeführten Betrieblichen Eingliederungsmanagements (BEM) ist diese Frage relevant und birgt enorme Risiken.

Warum?
Wenn die/der betroffene Mitarbeiter*in der Beteiligung des Betriebsrates zuvor ausdrücklich zugestimmt hat, darf der Betriebsrat an den BEM-Gesprächen beteiligt werden. Gem. dem Bundesarbeitsgerichts (BAG) muss der Betriebsrat zur Ausübung seiner Überwachungs- und Kontrollpflicht zwar Kenntnis davon haben, welchen Mitarbeitern ein BEM-Verfahren angeboten wurde, aber dies erfasst nicht automatisch die Beteiligung des Betriebsrats an den inhaltlichen Gesprächen. Zudem in einem BEM-Verfahren in der Regel (umfangreich) Gesundheitsdaten (besonders schützenswerte Daten) verarbeitet werden und hier in der Regel von der betroffenen Person eine ausdrückliche Freigabe zur Weitergabe erfolgen muss. Zu beachten ist auch, dass beim BEM die Vertraulichkeit in datenschutzrechtlicher Hinsicht das wesentliche Kriterium ist.

Fazit?
Im Ergebnis bleibt unklar welche (und in welchem Umfang) Gesundheitsdaten zu dem Punkt „Prognose einer Erkrankung“ gehören und somit dem Betriebsrat noch mitgeteilt werden dürfen. Fakt ist aber und das sollte jedes Unternehmen peinlichst beachten, dass dem Betriebsrat kein Zugriff auf die BEM-Akte gewährt werden darf. Diese Unterlage in der Regel umfangreich sensible Daten enthält, als für die Anhörung nach § 102 BetrVG erforderlich sind.

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

HINGESCHAUT
Datenschutz im Blick

Microsoft 365 – Und ewig grüßt das Murmeltier

25. November 2022! An diesem Tag hat die Datenschutzkonferenz (DSK) (das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder) eine Stellungnahme zu Microsoft 365 veröffentlicht. Wir erinnern uns, im Jahr 2020 kam die DSK zu dem Ergebnis, dass M365 nicht datenschutzkonform eingesetzt werden kann.
Grundlage der aktuellen Bewertung der DSK ist aus Sicht der DSK die intransparente Verarbeitung von Daten durch Microsoft zu eigenen Zwecken sowie die Datenübermittlung in die USA, wobei hier die neue Executive Order des US-Präsidenten vom 07.10.2022 ausdrücklich noch nicht mit bewertet wurde
Noch am gleichen Tag hat Microsoft auf die Bewertung der DSK reagiert und eine eigene Stellungnahme veröffentlicht. Nach deren Aussage erfüllen die Microsoft-365-Produkte die strengen EU-Datenschutzgesetze nicht nur, sondern übertreffen diese oft sogar.

Fazit?
Naja, wie oftmals liegt vermutlich auch hier irgendwo die Wahrheit dazwischen, wobei man realistisch auch die Faktoren „Praxisbezug“ oder auch „Wünsche und Anforderungen bei der Digitalisierung“ berücksichtigen sollte.
Keine Frage, nach den Anforderungen der DSGVO ist ein datenschutzkonformer Einsatz von MS365 derzeit nicht machbar. Aber ist das heutzutage mit den Anforderungen an Produkte und Prozesse überhaupt machbar? Gibt es eine echte Alternative für den Ersatz von der Microsoft-Welt?

Festplattenverschlüsselung - Schutz vor fremdem Datenzugriff

Warum Verschlüsselung?
Hierfür gibt es mehrere Gründe. Zum einen hat man die Anforderung der DSGVO bzgl. „Privacy by Design bzw. Default“ zu beachten. Also, aufgrund von Entwicklungen muss der Datenshcutz bzw. die Datensicherheit stetig angepasst werden. Und zum anderen sind diverse Schutzmaßnahmen hinsichtlich des Zugriffes durch Dritte zu beachten. Gem. Art. 32 Abs. 1 DSGVO müssen personenbezogene Daten mit geeigneten technischen und organisatorischen Maßnahmen gesichert sein. Das Verschlüsseln von Daten ist hier explizit als Beispiel aufgeführt.
Eigentlich nichts Neues, aber die Praxis zeigt noch immer große Lücken. Die Verschlüsselung ist ein zentraler Baustein in der IT-Sicherheit. Noch immer tun sich viele Unternehmen schwer mit der Umsetzung dieser Anforderungen. Dabei profitieren Unternehmen eigentlich davon, denn es geht nicht nur um die personenbezogenen Daten, sondern auch um die Geschäftsdaten. Und diese müssen gem. dem Geschäftsgeheimnisgesetz geschützt werden.

Fazit?
Der Prozess einer Datenpannenmeldung ist stressig und zeitraubend. Aber notwendig, wenn bspw. nicht verschlüsselte Datenträger verloren gehen. Ist dieser Datenträger hingegen verschlüsselt, erspart sich ein Unternehmen viel Diskussion und Arbeit.

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

Geldbußen für DSGVO-Verstöße in Deutschland

Vorab, es geht hier nicht ums „Angstmachen“. Vielmehr ist das Ziel die Sensibilisierung
→ „*So etwas ist ja auch bei uns vorgekommen*.“
Von vielen Unternehmen wurden und werden wir immer wieder angesprochen, ob es auch Bußgelder in Deutschland gibt. Ja, sie gibt es.

- Informationspflicht gegenüber Kunden wurde nicht beachtet
  Behörde: LfDI Baden-Württemberg, Verstoß: Art. 6 Abs. 1 DSGVO, Art. 14 DSGVO
  Bußgeld: 50.000 Euro
- Auswertung von Kundendaten ohne Rechtsgrundlage
  Behörde: LfD Niedersachsen, Verstoß: Art. 6 Abs. 1 lit. f DSGVO
  Bußgeld: 900.000 Euro
- Unrechtmäßige Audio- und Videoüberwachung von Beschäftigten
  Behörde: LfD Niedersachsen, Verstoß: Art. 5 Abs. 1 lit. f DSGVO, Art. 6 Abs. 1 lit. f DSGVO, Art. 17. Abs. 1 lit. a DSGVO, Art. 35 Abs. 3 lit. c DSGVO
  Bußgeld: 900.000 Euro
- Verarbeitung von sensiblen Daten von Mietinteressenten
  Behörde: Aufsicht Bremen, Verstoß: Art. 6 Abs. 1 DSGVO, Art. 5 Abs. 1 DSGVO, Art. 9 Abs. 1 DSGVO, Art. 12 Abs. 1 DSGVO, Art. 15 DSGVO
  Bußgeld: 1.900.000 Euro
- Übermittlung von Kundendaten trotz Widerspruch
  Behörde: Aufsicht Hamburg, Verstoß: Art. 5 Abs. 1 lit. a DSGVO, Art. 6 Abs. 1 DSGVO
  Bußgeld: 12.500 Euro

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

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

- 265 Millionen Euro Bußgeld für geleakte User-Daten bei Facebook
  Behörde: Data Protection Commission (Irland), Branche: Social-Media-Plattform
  Verstoß: Art. 25 Abs. 1, Abs. 2 DSGVO, Bußgeld: 265.000.000 Euro
- Aufbewahrung von Kundendaten ohne Einwilligung
  Behörde: Garante per la protezione dei dati personali (Garante)
  Branche: Einzelhändler, Verstoß: Art. 5 Abs. 1 lit. b), e) DSGVO, Art. 6 DSGVO, Art. 7 DSGVO, Art. 12 Abs. 1 DSGVO, Art. 13 Abs. 2 DSGVO, Art. 25 Abs. 1 DSGVO, Bußgeld: 1.400.000 Euro
- Ungenügende Aufbewahrungsprozesse und unsichere Passwörter
  Behörde: Commission Nationale de l'Informatique et des Libertés (CNIL), Branche: Online-Telekommunikations-Anbieter, Verstoß: Art. 5 Abs. 1 lit. e) DSGVO, Art. 13 DSGVO, Art. 25 Abs. 2 DSGVO, Art. 32 DSGVO, Art. 35 GDPR, Bußgeld: 800.000 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

- Bank gibt fehlerhaft Kunden Zugriff auf fremde Konten
  Behörde: La Agencia Española de Protección de Datos (AEPD), Branche: Finanzdienstleister
  Verstoß: Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 DSGVO, Bußgeld: 80.000 Euro
- Callcenter-Marketing ohne Einwilligung
  Behörde: Garante per la protezione dei dati personali (Garante), Branche: Telekommunikations-Dienstleister
  Verstoß: Art. 5 Abs. 1 lit. a) DSGVO, Art. 6 DSGVO, Art. 7 DSGVO, Art. 12 Abs. 1 DSGVO, Art. 130 Abs. 1, Abs. 2, Abs. 3 Codice della privacy, Bußgeld: 500.000 Euro

Fazit?

Es bleibt auch weiterhin in vielen Bereichen eine Gratwanderung zwischen Praxis und Theorie („Das Gesetz muss beachtet werden.“). Dazu kommen dann noch diverse Punkte, wie Kundenwünsche, Qualitätssteigerung oder Digitalisierung dazu. Und schon ist das Chaos perfekt. Die Frage bleibt, ob es in allen Bereichen „perfekt“ sein kann. Jedes Unternehmen ist individuell aufgestellt. Daher kann diese Frage nicht pauschal beantwortet werden.

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