Sehr geehrte Damen und Herren,
liebe Kund:innen,

wir hoffen, Sie sind alle gut und gesund ins neue Jahr gekommen.

Nach einer kleinen Weihnachtspause starten wir mit vollem Tatendrang mit der Januar-Ausgabe unserer Beratungsinformation für unsere Kunden.

Kein ruhiges Jahresende hatten Vertreter der EU-Kommission und Großbritanniens: In einem Verhandlungsmarathon haben sie sich am Jahresende noch auf einen Brexit-Vertrag und darin auf eine Verlängerung der Übergangsfrist u.a. in Sachen Datenschutz verständigt. Daher bringen wir als Nachschlag zum Jahresende 2020 ein Update zum Brexit.

Der Jahresanfang ist bei vielen die Zeit, um aufzuräumen. Datenschützer denken dann insbesondere auch an das Löschen von Daten. Unser Beitrag unter dem Motto „Frühjahrsputz im Datenschutz“ soll Sie dabei unterstützen.

Am 27.01.2021 sind die neuen Homeoffice-Vorgaben des Bundesarbeitsministeriums in Kraft getreten. Damit soll der Druck auf Arbeitgeber erhöht werden, in der Pandemie den Beschäftigten, wo das möglich ist, Heimarbeit anzubieten. Das ist für uns Anlass für Hinweise zur Datensicherheit im Homeoffice. Ein Thema, das uns auch nach der Pandemie sicher weiter beschäftigen wird.

Wenn Sie unsere Beratungsinformation regelmäßig lesen, finden Sie immer wieder etwas zum Thema Cookies. Auch diesmal haben wir das Thema wieder dabei, es bleibt also aktuell: Wir informieren Sie in dieser Ausgabe über einen Beschluss des LG Köln, das einen Wettbewerbsverstoß darin sieht, wenn Cookies ohne Einwilligung des Nutzers gesetzt werden.

Die Beraterinformation runden wir mit einem Hinweis in eigener Sache ab: Wir können unseren Kund:innen nun eine eigene Online-Datenschutz-Schulung als sog. eLearning anbieten. Testen Sie es, sprechen Sie uns an!

Ihr

Asmus Eggert

Inhalt

Update Datenschutz und Brexit – Verlängerung der Übergangsfrist!

Nach dem Austritt aus der EU am 31.01.2020 hat das Vereinigte Königreich nun zum 01.01.2021 auch den EU-Binnenmarkt und die Zollunion verlassen. In einem Verhandlungsmarathon haben die Europäische Kommission und das Vereinigte Königreich um die Bedingungen ihrer zukünftigen Zusammenarbeit gerungen. Ergebnis: Am 31.12.2020 einigte man sich auf ein Handels- und Kooperationsabkommen, in dem unter anderem auch Datentransfers aus der EU nach Großbritannien und deren datenschutzrechtliche Bewertung geregelt sind. Es wird darin etwa festgelegt, dass Großbritannien für eine weitere Übergangsfrist von 4 Monaten nicht als „unsicherer Drittstaat" eingestuft wird. Voraussetzung ist, dass die Briten für diesen Zeitraum an ihren auf der DSGVO basierenden nationalen datenschutzrechtlichen Regelungen festhalten. Eine Abweichung wäre nur mit Zustimmung der EU zulässig.

Bis Ende April kann daher der Datenverkehr unverändert weiter fließen. Diese Übergangsfrist kann dann noch einmal um zwei Monate verlängert werden. Bis spätestens Ende Juni muss die EU-Kommission dann jedoch einen sogenannten Angemessenheitsbeschluss erlassen.

Praxishinweis: Die Übergangsregelung für das Datenschutzrecht verschafft erneut Zeit für alle betroffenen Unternehmen, um sich für einen etwaigen Datenverkehr ins Vereinigte Königreich abzusichern. Es ist dabei nicht ratsam, dass sich betroffene Unternehmen auf einen rechtzeitig geschlossenen Angemessenheitsbeschluss der Europäische Kommission verlassen. Sie sollten sich auf die Situation vorbereiten, dass UK zumindest vorübergehend zu einem Drittland wird. Die erforderlichen Maßnahmen (beispielsweise Standarddatenschutzklauseln oder Binding Corporate Rules) lassen sich nicht „über Nacht" umsetzen, sondern bedürfen in Abstimmung mit den beteiligten Datenempfängern in UK und einer sorgfältigen Vorbereitung, um etablierte Geschäftsprozesse und Datenflüsse möglichst wenig zu beeinträchtigen.

Prüfen Sie den Handlungsbedarf für Ihr Unternehmen! Unsere Berater:innen unterstützen Sie bei Bedarf.

Praxishinweis: Frühjahrsputz im Datenschutz – Denken Sie ans Löschen!

Aufbewahrungsfristen beginnen grundsätzlich mit dem Schluss des Kalenderjahres, in dem die letzte Eintragung in das Buch gemacht, der Handels- oder Geschäftsbrief empfangen oder abgesandt worden, der Buchungsbeleg entstanden ist, die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind. Damit enden diese Fristen jeweils auch zum Ende eines Kalenderjahres und diejenigen Unterlagen die nunmehr 6 bzw. 10 Jahre aufbewahrt wurden, können ab 01.01.2021 entsorgt werden.

Ausgenommen sind Unterlagen und Daten, die Gegenstand von laufenden Prüfungen wie Betriebs-, Umsatz- oder Lohnsteuerprüfungen oder von steuerstrafrechtlichen oder bußgeldrechtlichen Ermittlungen oder bei Rechtsbehelfs- oder Klageverfahren sind.

Bei vielen Unternehmen gibt es daher zum Jahresanfang eine entsprechende Routine für die Vernichtung von z. B. Jahresabschlüssen, Buchungsbelegen wie Ausgangs- und Eingangsrechnungen, Kassenzetteln, Lieferscheinen, Kontoauszügen sowie von Jahresbilanzen, Inventaren, Kassenberichten, Kredit- und Steuerunterlagen, Geschäftsbriefen, Versicherungspolicen nach Ablauf, Verträgen und Mahnungen.

Die Löschpflicht ist eine wesentliche Pflicht der Verantwortlichen im Datenschutz. Das Löschen ist eine Verarbeitung von Daten. Sie sollten die Löschfristen und Aufbewahrungspflichten daher immer

im Verzeichnis der Verarbeitungstätigkeit (VVT) zum jeweiligen Verfahren aufnehmen. Denken Sie bei Ihrer Organisation der Löschaktion insbesondere auch an Folgendes:

- Beim Löschen auch an das Vernichten der Kopien denken! Das gilt für digitale Daten/Dokumente als auch für physische Daten.
- Beachten Sie die Sicherheitsanforderungen an eine Löschung/Entsorgung in Abhängigkeit der Sensibilität der Daten.
- Dokumentieren Sie die Löschung und auch die Entsorgung.

Sie sollten sich bei den Löschterminen an den entsprechenden Festlegungen in Ihrem VVT orientieren. Die Aufräumaktion können Sie im Übrigen nutzen, um das VVT inkl. des Löschkonzepts auf Aktualität zu prüfen. Stellen Sie dabei Anpassungsbedarf fest, planen Sie die Änderungen und leiten deren Umsetzung ein. So haben Sie einen sog. PDCA-Zyklus durchgeführt und dokumentieren damit das Funktionieren Ihres Datenschutzmanagements. Sollten Sie Beratung und Hilfestellung benötigen, sprechen Sie unsere Berater an. Wir unterstützen Sie gerne mit konkreten und praktischen Lösungsansätzen für Ihr Unternehmen.

Datensicherheit und Datenschutz im Homeoffice

Kriminelle versuchen derzeit gezielt Sicherheitslücken auszunutzen, wenn Mitarbeitende aus der Ferne auf das Unternehmensnetzwerk und Cloud-Anwendungen zugreifen. So haben 31 Prozent der deutschen Firmen seit Beginn von Covid-19 einen sprunghaften Anstieg der Cyber-Bedrohungen und Warnmeldungen um 25 Prozent und mehr erlebt.

Cisco hat zwei globale Studien, die auch Ergebnisse für Deutschland beinhalten, veröffentlicht. Sie zeigen die wachsenden Sorgen über den sicheren Datenaustausch während der Pandemie. Die wichtigsten Aufgaben sind für die befragten Unternehmen aktuell die Erhöhung der VPN-Kapazität (64 Prozent), gefolgt von der Einführung der Multi-Faktor-Authentifizierung (44 Prozent). An der Studie „Future of Secure Remote Work“ nahmen 3.196 Personen aus 21 Ländern teil, darunter 150 aus Deutschland. Für die „Consumer Privacy Survey“ wurden 2.600 Teilnehmer aus 12 Ländern befragt, davon 200 aus Deutschland.

Der Cisco Future of Secure Remote Work Report unterstreicht einmal mehr den Bedeutungszuwachs des Arbeitens im Homeoffice und des mobilen Arbeitens. Vor der Pandemie waren in Deutschland nur bei 15 Prozent der Unternehmen mehr als die Hälfte der Mitarbeitenden aus der Ferne tätig. Während der letzten Monate stieg der Anteil auf 53 Prozent an. Für die Zeit nach dem Lockdown erwartet man ein Niveau von 24 Prozent.

Laut der Studien ist die größte Herausforderung für die Cybersicherheit für die meisten Unternehmen und Organisationen der sichere Fernzugriff (64 Prozent). Die nächstgrößeren Bedenken von deutschen Unternehmen betreffen den Datenschutz (54 Prozent) sowie die Einhaltung von Richtlinien (43 Prozent).

Beim Schutz von Endpunkten gab jeder zweite Befragte an, dass die Absicherung von Büro-Laptops/Desktops (55 Prozent) und persönlichen Geräten (55 Prozent) in einer Remote-Umgebung schwierig ist. Danach folgen Cloud-Anwendungen mit 42 Prozent und Kundeninformationen mit 31 Prozent.

Quelle: GDD Mitteilungen 06/2020

Praxishinweis: Die Studien zeigen, dass sich das Arbeiten im Homeoffice oder am mobilen Arbeitsplatz von der adhoc-Lösung zum Beginn des ersten Lockdowns als feste Arbeitsplatzalternative manifestieren wird und als Arbeitsform auch nach der Pandemie relevant bleibt. Die Berichte von Cyberangriffen auf Unternehmen über mögliche Schwächen in der IT-Infrastruktur und -Ausstattung häufen sich. Nicht oder schlecht gesicherte IT-Arbeitsplätze erhöhen

daher das Risiko eines Angriffserfolges. Unternehmen sollten das Thema Datensicherheit und Datenschutz also ernst nehmen. Viele Unternehmen müssen nun ihre gesamte IT-Sicherheitsstrategie überdenken, um der neuen flexiblen Arbeitsumgebung gerecht zu werden. Dazu sind z.B. folgende Themen anzugehen:

- Umsetzung technischer Maßnahmen (Beschaffen und Bereitstellen von Sicherheitstechnologie, Software und datenschutzkonformer Apps)
- Umsetzung von organisatorischen Maßnahmen etwa durch Arbeitsanweisungen und Richtlinien

Wenn Sie hier Unterstützung (z.B. Muster für eine Mitarbeiterrichtlinie für Homeoffice und mobiles Arbeiten) benötigen, sprechen Sie unsere Berater an.

BayLDA: Typische Fehler bei Auskunftsersuchen

Ein zentrales Betroffenenrecht ist das Auskunftsrecht nach Art. 15 DSGVO. In der Praxis ist das Thema nach wie vor schwer greifbar. Laut der Aufsichtsbehörden spiegelt sich das auch in der hohen Anzahl von Datenschutzbeschwerden wider, bei denen Betroffene mit der Beauskunftung durch Verantwortliche unzufrieden sind und deshalb die Behörden um Unterstützung bitten.

In seinem Tätigkeitsbericht für das Jahr 2019 hat die Bayerische Datenschutz-Aufsichtsbehörde (BayLDA) typische Fehler als sog. „No-Go's" bei Auskunftsersuchen nach Art. 15 DSGVO sowohl für Unternehmen als auch für Betroffene identifiziert und dargestellt:

- No-Go 1: Ignorieren von Auskunftsbegehren bei Identitätszweifeln
- No-Go 2: Auskunft über ausschließlich Stammdaten als personenbezogene Daten
- No-Go 3: Einreichen der Beschwerde durch Betroffene vor Verstreichen der 1-Monats-Frist
- No-Go 4: Zweck des Rechts auf Auskunft außer Acht lassen
- No-Go 5: Geltendmachung des Rechts auf Auskunft gegenüber dem Anwalt der Gegenseite
- No-Go 6: Beschwerde ohne beweiskräftige Nachweise
- No-Go 7: Berufung auf unverhältnismäßigen Aufwand ohne Darlegung der Umstände

Quelle: www.lda.bayern.de/media/baylda_report_09.pdf

Praxishinweis: Lassen Sie eine Anfrage nicht liegen, sondern organisieren Sie eine fristgerechte Beantwortung. Ggfs. beantworten Sie die Anfrage in Stufen und begründen fundiert und belegbar ggfs. eine notwenige Fristverlängerung. Binden Sie Ihre:n Datenschutzbeauftragte:n immer frühzeitig ein. Sie bzw. er sollte Erfahrung im Umgang mit möglichen Fallstricken eines Auskunftsersuchens haben und ist verpflichtet, Sie hier zu beraten. Beugen Sie „Auskunftsstress" mit informierten Mitarbeiter:innen, klaren Zuständigkeiten, Vorlagen und einer Abwicklungsvorgabe vor.

Das Recht auf Auskunft dient ausschließlich dazu, Datenschutzziele zu verfolgen. Allerdings ist in der Praxis festzustellen, dass das Auskunftsersuchen durchaus weitere Motivationen hat z. B. das Sammeln von Beweisen für andere Konflikte zwischen Betroffenem und Verantwortlichem. Das sollten Sie erkennen und bei der Auskunft ggfs. berücksichtigen.

Cookies - LG Köln: Setzen von Cookies ohne Einwilligung ist Wettbewerbsverstoß

Das Setzen von Cookies ohne aktive Einwilligung des Betroffenen ist ein Wettbewerbsverstoß. Das hat das LG Köln, Beschl. v. 29.10.2020 - Az.: 31 O 194/20 entschieden. Die Antragstellerin erwirkte hier im Wege des einstweiligen Rechtsschutzes eine einstweilige Verfügung, weil der Antragsgegner auf seiner Homepage Cookies setzte, ohne dass der User zuvor aktiv zugestimmt hatte.

Praxishinweis: Der Beschluss des LG macht erneut die Relevanz des datenschutzkonformen Einsatzes von Cookies und der Umsetzung von Cookie-Bannern deutlich. Fehler können also neben Sanktionen

und Schadensersatzansprüchen auch wettbewerbsrechtliche Abmahnungen zur Folge haben. Hier droht aus unserer Sicht die nächste Abmahnwelle, denn geringe Prüfaufwände (hier das einfache Checken von Webseiten) lassen sich schnell und effizient zu verwertbaren Abmahnungen verarbeiten.

Beachten Sie daher bitte unsere Hinweise zum Thema „Cookies“ aus den letzten Beraterinformationen.

Sofortdatenschutz.de eröffnet e-Learning Plattform

Wir, das mip Datenschutzteam, sind den Wünschen unserer Kunden nachgekommen und haben eine eLearning-Plattform entwickelt. Hier können kostengünstig und auf einfachem Weg Online-Schulungen gebucht werden.

Wir starten ab sofort mit der **„Basisschulung Datenschutz für Mitarbeiter in einem Unternehmen“**. Hier vermitteln wir in acht Lektionen und Übungen das Grundwissen im Datenschutz. Die Sprecher der Lektionen sind Mitglieder des mip-Datenschutzteams. Vielleicht erkennen Sie ihre Stimmen wieder.

Die Schulung ist insbesondere geeignet, neue Mitarbeiter:innen des Unternehmens gleich zum Start der Tätigkeit, ohne erst auf eine Datenschutzschulung warten zu müssen, individuell zu sensibilisieren. Wenn die Teilnehmer:innen die Schulung erfolgreich durchgearbeitet haben (ca. 1,5 Stunden Zeitaufwand) wird direkt eine Teilnahmebescheinigung ausgestellt, die als Nachweis der Schulung zur Personalakte genommen werden kann.

Wenn Sie Interesse haben, melden Sie sich bei uns. Wir stellen gerne einen **kostenlosen Testzugang** zur Verfügung und freuen uns über Ihr Feedback.

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Yanick Röhricht, Asmus Eggert

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich im Sinne von § 18 Abs. 2 MStV: Asmus Eggert