Neuigkeiten zur DSGVO im Jahr 2020

1. Der Datenschutz in „Corona-Zeiten“

1.1. Homeoffice

Bedingt durch die Coronapandemie werden viele Arbeitgeber ins Homeoffice geschickt. Datenschutzrechtlich sollte vor dem Einsatz mit allen Beteiligten transparent kommuniziert werden. Nicht alle Arbeitsprozesse sind im Homeoffice (auch datenschutzkonform) sinnvoll oder möglich auszuführen. Auf jeden Fall sollten die Zustimmungen der Mitarbeiter oder/und des Betriebsrats vor dem Einsatz im Homeoffice eingeholt werden.

Der Verantwortliche muss einen Überblick über die IT-Ausstattung gewinnen und den Einsatz von dienstlich gestellten und privaten Geräten regeln.

Für alle Prozesse im Homeoffice müssen Richtlinien, Regeln, Arbeitsanweisungen erstellt bzw. anpasst werden. Individualisierbare Muster und Vorschläge können Sie von uns erhalten.

1.2. Onlinemeetings

Bei der Auswahl des Online-Meetingtools sollte auch der Datenschutzbeauftragte zugezogen werden. Wenn möglich sollten Einstellungen getroffen werden, die eine Datenübertragung in die USA ausschließen. Außerdem sollten Datenschutzhinweise zu dem verwendeten Tool dem Geschäftspartner und dem Mitarbeiter vor der Nutzung zur Verfügung gestellt werden. Art. 25 DSGVO verlangt eine datenschutz-freundliche Voreinstellung. Dazu gehört beispielsweise, dass die Meetingteilnehmer selbst über Ihre Video- oder Audiofreigaben entscheiden können.

1.3. Beschäftigtendatenschutz und Arbeitsschutz

Bei der Analyse der Gefährdung, um Maßnahmen für besonders schutzbedürftige Beschäftigte zu ergreifen (SARS-CoV-2 Arbeitsschutzstandard), ist zu beachten, dass hierbei Gesundheitsdaten erhoben werden müssen, die besonders schutzwürdige Daten (gem. Art. 9 DSGVO) sind.

Es ist es den Arbeitgebern nicht gestattet z.B. spezielle Krankheitsbilder abzufragen. Eine Gefährdungsanalyse sollte nur in Zusammenarbeit mit dem (Betriebs-) Arzt vorgenommen werden. Weiterhin ist zu beachten:

- **Arbeitgeber dürfen das Betreten des Betriebes nicht von einer Messung der Körpertemperatur abhängig machen.**

- Coronatests für Mitarbeiter dürfen nur auf freiwilliger Basis durchgeführt werden (bei Symptomfreiheit).

- Mitarbeiter mit Krankheitssymptomen dürfen aufgefordert werden, den Betriebsarzt oder Amtsarzt zu besuchen.

- Mitarbeiter die positiv auf SARS- CoVD 2 getestet wurden, müssen eine Arbeitsunfähigkeitsbescheinigung vorlegen. Vom Gesundheitsamt werden Kontaktpersonen ermittelt. Es empfiehlt sich Mitarbeiter selbst eine Liste mit Kontaktpersonen anlegen zu lassen. Eine namentliche Benennung des Mitarbeiters im gesamten Unternehmen sollte vermieden werden

Auf was muss *„ich“* als Arbeitgeber noch achten? Hier erhalten Sie eine weitere Orientierungshilfe: https://www.b-in.de/Einschaetzung-Corona_B-iNStand20201203.pdf

1.4. Der Datenschutzbeauftragte und die Kurzarbeit

An der Benennungspflicht eines Datenschutzbeauftragten ändert sich nichts, auch wenn in der Kurzarbeitszeit zwischenzeitlich weniger als 20 Personen mit der Verarbeitung personenbezogener Daten betraut sind.

1.5. Erhebung von Kontaktdaten

Wenn Kontaktdaten von Gästen oder Kunden wie z.B. in Gastronomiebetrieben erhoben werden müssen, gilt:

- Namen und Kontaktdaten (Tel. oder E-Mail oder postalische Adresse) von jeweils einer Person pro Hausstand, Zeitraum des Aufenthalts
- Datenschutzgerechte Vernichtung der Daten nach 1 Monat
- Die Daten dürfen ausschließlich an das Gesundheitsamt zur Nachverfolgung möglicher Infektionsketten weitergereicht werden
- Der Betrieb darf die Daten nicht anderweitig nutzen (z.B. für Werbung)
- Die Daten sollten für jeden Gast auf einem Einzelbogen erfasst werden, unzulässig sind Listen, auf denen die Gäste die Daten der vorangegangen Personen einsehen können
- Der Betrieb muss die Gäste über die Verarbeitung der Daten informieren (Art. 13 DSGVO)
- Die Aufbewahrung der Daten muss so gestaltet sein, dass andere Gäste keinen Zugriff auf die Daten haben

Als mögliche Vorgehensweisen haben sich verschiedene APP’s etabliert, die die nachvollziehbare (lesbare) Erfassung und datenschutzgerechte Verarbeitung ermöglichen.

2. Schremms II

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 16. Juli 2020 den Beschluss 2016/1250 der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam erklärt. Zugleich hat der EuGH festgestellt, dass die Entscheidung 2010/87/EG der Kommission über Standardvertragsklauseln (Standard Contractual Clauses - SCC) grundsätzlich weiterhin gültig ist.

Für die Übermittlung personenbezogener Daten in die USA und andere Drittländer hat das Urteil folgende Auswirkungen:

1. **Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield ist unzulässig und muss unverzüglich eingestellt werden. Der EuGH hat das Privacy Shield für ungültig erklärt, weil das durch den EuGH bewertete US-Recht kein Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist.**
2. **Für eine Übermittlung personenbezogener Daten in die USA und andere Drittländer können die bestehenden Standardvertragsklauseln der Europäischen Kommission zwar grundsätzlich weiter genutzt werden.**
3. **Der EuGH betonte jedoch die Verantwortung des Verantwortlichen und des Empfängers, zu bewerten, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der Union genießen. Nur dann kann entschieden werden, ob die Garantien aus den Standardvertragsklauseln in der Praxis verwirklicht werden können. Wenn das nicht der Fall ist, sollte geprüft werden, welche zusätzlichen Maßnahmen zur Sicherstellung eines dem Schutzniveau in der EU im Wesentlichen gleichwertigen Schutzniveaus ergriffen werden können. Das Recht des Drittlandes darf diese zusätzlichen Schutzmaßnahmen jedoch nicht in einer Weise beeinträchtigen, die ihre tatsächliche Wirkung vereitelt.**

   Nach dem Urteil des EuGH reichen bei Datenübermittlungen in die USA Standardvertragsklauseln ohne zusätzliche Maßnahmen grundsätzlich nicht aus. Das bedeutet eine rechtliche Unsicherheit und hat Auswirkungen auf alle Anwendungen, die personenbezogene Daten in Drittländer übertragen.

Zu diesem Themenbereich wurde bereits etwas auf unserer Website veröffentlicht. Was gibt es Neues nach dem EuGH-Urteil vom 17.07.2020? Hier haben wir unsere Einschätzung gepostet: https://www.b-in.de/DatenschutzDepesche2020-01.pdf

Betroffen sind beispielsweise nachfolgende Anwendungen, von denen bekannt ist, dass sie personenbezogene Daten in die USA übertragen. D.h. es sollten überprüft werden:

- **Clouddienste**
- **Googledienste**
- **Messengerdienste von Apple, Facebook und WhatsApp**
- **MS Office 365**
- **Onlinemeeting-Werkzeuge wie Zoom**

- Social-Media Plattformen wie Facebook und Instagram
- Websiteserver und Website-Funktionen mit Cookies
- …

2.1. Beispiel für eine Bestandsaufnahme bei Webseite und Handlungsoptionen

1. Google Analytics zur Webseitenerfolgsmessen
2. Google Maps um Standortansichten und Routenplanung zu ermöglilchen
3. Google YouTube –-> Videoplattform
4. Google reCAPTCHA –-> Sicherheitsabfragen zum Spam-Schutz
5. Google Fonts –-> Schriften für Webseiten

2.2. ToDo: Erforderlichkeit prüfen

zu 1. Alternative: lokal installierte Anwendung „Matomo“
zu 2. Open Street Maps **oder**
Link zu Google erst nach Einwilligung freischalten
zu 3. Standbild einbinden **und**
Link zu Google erst nach Einwilligung freischalten
zu 4. ggf. Alternativen testen **oder** erst nach Einwilligung freischalten
zu 5. Schriften auf eigenem Server speichern und vom dort aus abrufen

2.3. Auswirkungen von Schrems II auf die Nutzung Office 365

Am 02. Oktober 2020 gab die Konferenz der unabhängigen Datenschutzaufsichts-behörden des Bundes und der Länder (DSK) eine Pressemitteilung heraus, in der sie sich zu der datenschutzrechtlichen Bewertung von Office 365 äußerte. Mit einer knappen Mehrheit von 9 zu 8 Stimmen kam die Datenschutzkonferenz zu der Entscheidung, dass kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich sei.

Im Moment stehen die Aufsichtsbehörden in regelmäßigen Kontakt mit Microsoft. Microsoft ist um die Anpassungen seiner Bedingungen bemüht. Demzufolge sehen wir im Moment keinen Grund den Einsatz von Microsoft 365 im Unternehmen zu beschränken.

3. Cookie Consent Banner

Da schon beim Aufrufen einer Website personenbezogene Daten ermittelt werden, sollte auf der Website ein Consent Banner Menü eingerichtet werden über das Einstellungen vom Nutzer durchgeführt werden können. Dieses Consent Banner

minimiert zwar die Conversionsrate etwas und einige Nutzer sind darüber nicht besonders erfreut, aber die nach außen hin sichtbare „Barriere“ zeigt auch, wer Datenschutz Ernst nimmt und wer nicht.

So funktioniert ein Consent Banner: Beim erstmaligen Besuch einer Website informiert der Verantwortliche über alle beabsichtigten Erhebungen und Verarbeitungszwecke und bietet mittels Checkboxen an, in die einzelnen Erhebungen und Verarbeitungszwecke einzuwilligen.

Die Checkboxen dürfen nicht vorbelegt sein, und zum Zeitpunkt der Anzeige des Consent Menüs dürfen noch keine Erhebungen und Übermittlungen stattfinden!!!

Auftragsverarbeitungsverträge auf Basis Standardvertragsklauseln bei internationalen Drittanbieter-Diensten sind obligatorisch.

4. „TOM’s“ und die Betroffenenrechte

Aus den letzten Bußgeldverfahren und den Entscheidungen des EuGH im Jahr 2020 kann man gut ableiten, worauf die Behörden besonderen Wert legen.

- **Im Fokus steht die sichere Datenverarbeitung** der personen-bezogenen Daten. Nebenbei erhalten Unternehmen damit auch höhere IT-Sicherheit und damit Schutz gegen Dritte oder Computerviren.
- Gleich dahinter bzw. besser gesagt **gleichauf rangieren die Betroffenenrechte** und deren Umsetzung. Schon im letzten Jahr 2019 hat man durch Bußgelder beispielsweise an die Deutsche Wohnen AG signalisiert, dass der Datenschutz-Aufsicht wichtig ist die Digitalisierung gepaart mit Kunden-und Mitarbeiter-Vertrauen in die Unternehmen voran zu treiben.

Hier die zuletzt ausgesprochenen Bußgelder:

November 2020

Die Strafe für Telekommunikationsanbieter 1&1 wegen nicht ausreichender Kunden-Authentifizierung am Telefon (Name und Geburtsdatum sei nicht ausreichend, um weitere, personenbezogene Daten zu erfragen) wurde mit 900.000 € entschieden.

Oktober 2020

Der schwedische Modekonzern H&M wurde wegen Ausspähung von Mitarbeitern zu einer Strafe von 35.000.000 € verklagt. Im Konzern wurden Informationen aus dem Privatleben der Mitarbeiter erfragt, dauerhaft gespeichert und sind durch einen IT-Fehler konzernweit sichtbar geworden.

Juli 2020

Die AOK Baden Württemberg bekam wegen einer nicht datenschutzkonformen Verwendung personenbezogener Daten eine Strafe in Höhe von 1.240.000 €. Es

wurden Daten aus einem Gewinnspiel ohne die Zustimmung der Teilnehmer für Werbezwecke genutzt.

Lassen wir es also gar nicht so weit kommen! Behalten Sie die Kontrolle und setzen Sie Ihr Geld nicht in den Sand – getreu diesem Motto unterstützen wir Sie weiterhin und stehen gerne mit Rat und Tat zur Verfügung.

Apropos „wir“:

Seit 01.08.2020 ist Frau Nadja Mitrea als weitere, zertifizierte Datenschutzbeauftragte „on board“. Somit können wir die gestiegenen Anfragen im Zusammenhang mit Digitalisierungsprojekten besser abarbeiten und gegenseitige Prüfungen oder Umsetzungsarbeiten realisieren, ohne Neutralitätsgesichtspunkte zu gefährden.

Und auch für IT-technische Analysen ist ein sehr erfahrener Mitarbeiter aus dem IT-Consulting dabei und freut sich über Ihre Anfragen.

Wie immer können Sie alle Termine über die Internetseite unter „Termine sofort vereinbaren“ selbst koordinieren oder Sie rufen einfach an.

Telefonisch erreichen Sie uns – auch zwischen den Feiertagen und Schulungen können bzw. wurden dieses Jahr online abgehalten – und können auch 2021 jederzeit so umgesetzt werden.

Doch am liebsten wollen wir Sie bald wiedersehen! Die Chancen stehen 2021 sehr gut, dass dies klappt. In diesem Sinne, alles Gute für den Jahreswechsel und -

bleiben Sie Gesund!

Ihr Team von B .i N BusinessCoaching+Consulting

gez. Jens Wiemeyer, Inhaber