ERFA-Kreis Nürnberg 21.03.2023
-Antworten des BayLDA auf die eingereichten Fragen-

Frage 1: Verarbeitung von Daten durch die Revision
Bei einem meiner Kunden verarbeitet die Revision personenbezogene Daten im Rahmen von Prüfungen / Untersuchungen. Dies betrifft Daten von Beschäftigten, aber auch von Kunden / Lieferanten.
Muss für die Rechtmäßigkeitsgrundlage hierzu auf Art. 6 Abs. 1 lit. f DS-GVO mit den Hinweisen nach Art. 21 DS-GVO zurückgegriffen werden oder kann auch Art. 6 Abs. 1 lit. c DS-GVO in Verbindung mit § 130 Abs. 1 OWiG genutzt werden?
Der Vorteil dabei ist, es ist kein Verfahren erforderlich zur Information über Widerspruchsmöglichkeit und auch Daten besonderer Kategorien könnten über Art. 9 Abs. 2 lit. g DS-GVO umfasst sein (z.B. bei einer Prüfung von Ansprüchen aus dem SGB).
Natürlich werden im Rahmen der Prüfung soweit möglich pseudonymisierte Daten eingesetzt, dennoch bleibt es eine Verarbeitung pbD.

Die Datenverarbeitung von Beschäftigtendaten im Rahmen einer Revision ist in der Regel nach § 26 BDSG begründbar. Eine (präventive) Maßnahme kann im Rahmen des § 26 Abs. 1 S. 1 BDSG bzw. § 26 Abs. 3 BDSG möglich sein.
Eine Datenverarbeitung zur Aufdeckung von Straftaten (repressiv) ist unter den engen Voraussetzungen des § 26 Abs. 1 S. 2 BDSG möglich; bei sonstigen Pflichtverletzungen gem. § 26 Abs. 1 S. 1 BDSG.
Die Verarbeitung von Kunden- und Lieferantendaten kann gem. Art. 6 Abs. 1 S. 1 f) DS-GVO zulässig sein.
Art. 6 Abs. 1 S. 1 c) DS-GVO sehen wir vorliegend nicht als einschlägig an, da § 130 OWiG nicht den Anforderungen des Art. 6 Abs. 3 DS-GVO entspricht.

Anmerkung: Das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 30.03.2023 (Rechtssache C-34/21) lässt nach unserer Auffassung den Schluss zu, dass es sich bei § 26 Abs. 1 BDSG nicht um eine spezifische Bestimmung i.S.d. Art. 88 Abs. 1 DS-GVO handelt. Die Verarbeitung von Beschäftigtendaten zu Zwecken der Durchführung des Beschäftigungsverhältnisses ist daher aus hiesiger Sicht alleine auf Art. 6 Abs. 1 S. 1 b) DS-GVO zu stützen.

Frage 2: Nutzung von biometrischen Daten für Zwecke der Zeiterfassung
In Unternehmen außerhalb der EU ist es eine weit verbreitete Praxis, die Anwesenheitszeiten der Mitarbeiter mithilfe von biometrischen Daten zu erfassen, insbesondere über Gesichtserkennung oder den Fingerabdruck.
Sieht das BayLDA eine entsprechende Rechtsgrundlage für Unternehmen in der EU?
Was wäre Unternehmen mit Sitz in der EU zu raten, die diese Technologien für Zwecke der Zeiterfassung an Standorten außerhalb der EU einsetzen?

Die Zeiterfassung mittels Verarbeitung biometrischer Daten (Fingerabdruck, Gesichtserkennung) wird an § 26 Abs. 3 BDSG i.V.m. Art. 9 Abs. 2 b) DS-GVO zu messen sein, weil es sich bei den biometrischen Daten um besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1, Art. 4 Nr. 14 DS-GVO) handelt. Die Voraussetzungen der Vorschrift sind häufig nicht erfüllt, da diese Datenverarbeitung oftmals nicht erforderlich ist, da es eine geeignete und für die Beschäftigten weniger belastende Alternativen gibt. Ausnahmen können bei erhöhten Sicherheitsanforderungen gelten.
Dies gilt auch, wenn die Zeiterfassung durch einen in Deutschland niedergelassenen Verantwortlichen außerhalb der EU stattfindet (Art. 3 Abs. 1 DS-GVO).

Soweit die Datenverarbeitung durch einen Verantwortlichen in einem anderen EU-Mitgliedstaat erfolgt, kommt es hinsichtlich Art. 9 Abs. 2 b) DS-GVO darauf an, ob die Voraussetzungen erfüllt sind (insbes. nationales Recht).

Frage 3: Microsoft 365 an (Privat-)Schulen

Ich bin externer Datenschutzbeauftragter an verschiedenen Privatschulen in Bayern. Während der Corona-Pandemie haben einige Schulen auf Microsoft 365 (insbesondere MS Teams) als Lösung z.B. für den Distanzunterricht eingesetzt.
Inzwischen gibt es genügend datenschutzkonforme Lösungen auch im Bereich der Videokonferenzen (z.B. ByCS, Visavid).
Dennoch wollen manche Schulen an ihrer Microsoft-Lösung festhalten, obwohl die DSK am 25. November 2022 auf Basis einer Arbeitsgruppe zum eindeutigen Entschluss kam, dass Microsoft 365 (beinhaltet Office 365) auf der Grundlage des von Microsoft bereitgestellten "Datenschutznachtrags vom 15. September 2022" nicht datenschutzrechtskonform zu betreiben sei.

Im Tätigkeitsbericht 2022 positioniert sich nun das LfDI BW unter dem Punkt “3.1 Microsoft 365 an Schulen” ganz klar gegen eine solche Nutzung.
Wie ist hierzu die Position des BayLDA?
Wie kann mich das BayLDA als DSB unterstützen, damit ich die betroffenen Schulen zu einem Wechsel auf datenschutzkonforme Lösungen motivieren kann?
Gibt es seitens des BayLDA und des BayLfD eine gemeinsame mit dem Bayerischen Staatsministerium für Unterricht und Kultus abgestimmte Auffassung dazu?

Die Festlegung der DSK vom 25.11.2022 entfaltet keine unmittelbare Wirkung. Falls Beschwerden zu dieser Thematik bei uns eingehen, haben Verantwortliche (wie z.B. Privatschulen) uns ggü. den datenschutzkonformen Einsatz von MSO 365 anhand ihrer individuellen Vertragsunterlagen nachzuweisen. Der Nachweis ist unabhängig davon zu führen, ob MSO 365 zur Kommunikation mit Schüler:innen oder allein zur Kommunikation unter Lehrkräften genutzt wird.

Nichtsdestotrotz sollten Verantwortliche aufgrund der verfügbaren datenschutzkonformen Alternativen zu MSO 365 schon jetzt über eine Umstellung (bspw. auf das Videokonferenztool Visavid) nachdenken. Unseres Erachtens sollte der Umstand, dass damit bedeutend geringere datenschutzrechtliche Risiken verbunden sind, Motivation genug sein.

Frage 4: Transfer Impact Assessment bei jedem Drittlandstransfer?

Muss ein Transfer Impact Assessment bei jedem Drittlandstransfer gemacht werden, oder kann man auf ein bestehendes TIA zurückgreifen, sofern

- die Datenarten und deren Sensitivität und
- weiteren Parameter (Daten-Importeur, Data Residence, Zugriffe auf die Daten, TOMs)

identisch bzw. vergleichbar sind?
Ergänzende Frage: Was wäre ein angemessenes Zeitintervall bzgl. dem periodischen Re-Assessment?

Werden personenbezogene Daten in ein Drittland ohne Angemessenheitsbeschluss übermittelt, muss der Datenexporteur vorab im Rahmen eines TIA prüfen, ob die in Art. 46 Abs. 2, Abs. 3 DS-GVO genannten Garantien für sich genommen ausreichen oder aber um spezifische zusätzliche Maßnahmen ergänzt werden müssen (sofern keine der – restriktiv auszulegenden – Ausnahmen des Art. 49 DS-GVO einschlägig sind). Bei Vergleichbarkeit von Datenübermittlungen ist zwar ein Rückgriff auf bereits durchgeführte TIA denkbar, dies muss vom Datenexporteur jedoch in jedem Einzelfall geprüft werden.

Die Frage, in welchem zeitlichen Abstand ein Re-Assessment durchzuführen ist, lässt sich nicht pauschal beantworten, sondern hängt insb. von der Sensitivität der übermittelten Daten ab.

Zusatzfrage betr. neuer Angemessenheitsbeschluss: Wie ist damit umzugehen? Müssen Verantwortliche dann trotzdem ein TIA machen?

Auch wenn ein neuer Angemessenheitsbeschluss für die USA bereits absehbar ist, sind Verantwortliche derzeit noch zur Durchführung eines TIA angehalten. Nach Erlass des Angemessenheitsbeschlusses entfällt diese Verpflichtung (jedenfalls solange der Beschluss Bestand hat).

Frage 5: Verhältnis Konzernmutter und -Töchter

In unserer Unternehmensgruppe werden viele IT-Verfahren, die personenbezogene Daten verarbeiten, zentral an die Tochtergesellschaften im In- und Ausland ausgerollt. Die Verfahren verarbeiten z.B. HR-Daten von Mitarbeitern der Tochtergesellschaften, damit diese am Monatsende den Mitarbeitern das Gehalt entsprechend den Regelungen in der Tochtergesellschaft auszahlen können. In unserem Unternehmen gehen wir üblicherweise von einer Auftragsverarbeitung aus und schließen entsprechende Verträge mit den Tochtergesellschaften. In der Regel haben die Tochtergesellschaften diese IT-Verfahren verpflichtend zu nutzen, es sein denn aus dem jeweiligen Landesrecht ergeben sich Einschränkungen oder gar ein Verbot. Allerdings ergeben sich Zweifel, ob hier eine Auftragsverarbeitung vorliegt, da die Tochtergesellschaften als Verantwortliche nicht über Mittel und Zweck der Verarbeitung entscheiden können, sondern die zentral ausgerollten Verfahren nutzen müssen.

Grundsätzlich würden wir gerne wissen, inwieweit das BayLDA bei Unternehmensgruppen/Konzernen, bei der die einzelne Tochtergesellschaft in der Regel nicht über den Einsatz von IT-Verfahren entscheiden kann, von

- einer alleinigen Verantwortlichkeit der Muttergesellschaft, die Zweck und Mittel der Verarbeitung bestimmt (Art. 4 Nr. 7 DSGVO)
- einer gemeinsamen Verantwortlichkeit (Art. 26 DSGVO)
- einer Auftragsverarbeitung (Art. 28 Abs. 3 DSGVO)

ausgeht und auf welcher Grundlage die Muttergesellschaft die personenbezogenen Daten ihrer Töchter verarbeiten soll.

Zur Einstufung der Rolle einer Entity als Verantwortlicher, Gemeinsam Verantwortlicher oder Auftragsverarbeiter siehe die Leitlinien Verantwortlicher / Auftragsverarbeiter des Europäischen Datenschutzausschusses (Leitlinien Nr. 7/2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en).
In so gut wie allen Konzernen dürfte es „zentral ausgerollte Verfahren“ dieser Art geben wie hier beschrieben. Das heißt aber nicht, dass die Tochterunternehmen dann nicht Verantwortliche sein können. Die in diesen Fällen von der Mutter getroffene Vorgabe zur Nutzung eines bestimmten Systems / einer bestimmten Software ist „nur“ eine Entscheidung über „unwesentliche“ (nämlich bloße technische) Mittel der Verarbeitung; die Entscheidung über unwesentliche Mittel macht aber einen Akteur (hier: die Mutter) nicht zum Verantwortlichen. Verantwortlicher ist vielmehr, wer über die Zwecke (und wesentlichen Mittel) der Verarbeitung entscheidet. Bei der Lohnauszahlung ist Verantwortlicher der jeweilige Arbeitgeber des jeweiligen Beschäftigten, da er (dieser Arbeitgeber nämlich) es ist, der mit der Lohnzahlung seine arbeitsvertragliche Pflicht erfüllt und damit seinen eigenen Zweck (Arbeitsvertrag-Erfüllung) verfolgt – nicht einen Zweck der Muttergesellschaft.
Bitte lesen Sie dazu die maßgeblichen Randnummern im Leitlinienpapier Verantwortlicher/Auftragsverarbeiter durch unter Randnummern 32 - 45 des Papiers – dort stehen die entscheidenden Anmerkungen zum Thema wesentliche/unwesentliche Mittel.