BayLDA

Bayerisches Landesamt für
Datenschutzaufsicht

Fragen und Antworten zur Sitzung des GDD-ERFA-Kreises Nürnberg vom 13.12.2023

Frage 1: Datenschutz und Künstliche Intelligenz

Angesichts der vielen Fragen, die allein deutsche Aufsichtsbehörden an Hersteller generativer KI richten, fällt es schwer, die aus Sicht des Datenschutzes wichtigsten Punkte zu identifizieren.

Worauf sollten Unternehmen aus Sicht des BayLDA vor allem achten, wenn sie Produkte wie ChatGPT, Microsoft Bing Chat Enterprise oder Microsoft Copilot für ihre Zwecke einsetzen möchten? Auf welche Aspekte sollten sich Datenschutzbeauftrage bei der Prüfung konzentrieren? Was sind die Dos und Don’ts?

Antwort 1:

Wird eine bestehende KI-Anwendung verwendet (also kein neues KI-Modell erstellt), dann sind erst einmal die gleichen Vorgaben wie bei sonstigen neuen Verarbeitungsprozessen wie Eintrag ins Verarbeitungsverzeichnis, DSFA-Prüfung, Hosting bzw. Auftragsverarbeitung und natürlich die Rechtsgrundlage zu klären (meist Interessensabwägung bzw. Einwilligung bei Daten gemäß Art. 9 DS-GVO). Da gerade die momentan stark beachteten großen Sprachmodelle (wie z. B. ChatGPT) meist aufgrund der enormen Hardwareanforderungen nicht selbst betrieben werden können, sind bei einem KI-as-a-Service-Anbieter insbesondere die Zweckbindung der Eingabe- und Ausgabedaten (da KI-Anbieter die Daten gerne für die Produktverbesserung verwenden wollen) und auch die Garantien zum Drittlandtransfer zu beachten (wie bei anderen Cloud-Diensten auch). Des Weiteren sind insbesondere die Risiken der Ausgaben einer KI-Anwendung für die betroffenen Personengruppen (z. B. diskriminierende oder gar hasserfüllte Ausgaben, Fake-News, aber auch fehlerhafte Ausgaben wie „Halluzinationen“) zu berücksichtigen – mitunter führen diese Risiken auch zu einer DSFA-Pflicht.

Frage 2: Meldepflichten bei Vorgängen innerhalb des Verantwortlichen

Als DSB war ich bislang immer der Auffassung, dass auch die unbefugte Offenlegung von bzw. der unbefugte Zugang zu personenbezogenen Daten innerhalb eines Unternehmens eine Datenschutzverletzung darstellen kann. Beispiel: Speicherung von datenschutzrechtlich sensiblen Dateien in einem unverschlüsselten Verzeichnis, auf das alle Mitarbeiter zugreifen können. Ein aktuelles Papier des Hamburgischen DSB lässt daran zweifeln, da es mehrfach auf eine „Offenlegung an Dritte“ abstellt. Dritter ist nach meinem Verständnis aber nicht der Verantwortliche selbst.

Ist das LDA ebenfalls der Auffassung, dass auch solche internen Vorgänge eine Datenschutzverletzung darstellen können? Falls ja, welche dieser Vorgänge wären nach Ansicht des LDA typischerweise meldepflichtig? Welche nicht?

Antwort 2:

Auch bei der unbefugten Offenlegung bzw. beim unbefugten Zugang zu personenbezogenen Daten innerhalb eines Unternehmens kann es sich um eine Datenschutzverletzung handeln, die gemäß Art. 33 DS-GVO der zuständigen Datenschutzaufsichtsbehörde gemeldet werden muss. Hierbei kommt es darauf an, um welche personenbezogenen Daten es sich handelt und wer im Unternehmen darauf berechtigt Zugriff haben darf. So ist beispielsweise bei Personalunterlagen der Zugriff in der Regel auf einen engen Personenkreis, nämlich die Personalabteilung und gegebenenfalls den Vorgesetzen, beschränkt. Werden diese Unterlagen dann ohne Zugriffsschutz auf einem Unternehmenslaufwerk abgelegt, könnten auch andere Mitarbeiter – und damit unberechtigte Dritte – auf diese Unterlagen zugreifen. Je nach Risikobewertung kann es sich in solchen Fällen um eine meldepflichtige Datenschutzverletzung handeln.

Frage 3: Datenschutz bei Auslandseinsätzen (I)

Unser Unternehmen entsendet Mitarbeiter in Projekte auf Baustellen weltweit. Für den dortigen Einsatz muss unser Unternehmen (besondere Kategorien von) personenbezogenen Daten für Visaanträge, Arbeits- und Aufenthaltsgenehmigungen bei Konsulaten und lokalen Behörden vor Ort und beim Kunden für den Zugang zur Baustelle übermitteln. Viele lokale Behörden oder auch die Konsulate unterliegen in der Regel einem Datenschutzrecht, dessen Niveau nicht dem in der Europäischen Union entspricht. Zu den zu übermittelnden Daten gehören u.a. die personenbezogenen Daten von Eltern und Lebensgefährten, Gesundheitsnachweise wie „fit for the job“-Zertifikate ohne Angaben von Befunden, HIV-Testergebnisse und die Religionszugehörigkeit. Die Anträge kann in der Regel der Mitarbeiter nicht selbst stellen.

Frage / Antwort 3: Datenschutz bei Auslandseinsätzen (II)

Hierzu stellen sich uns immer folgende Fragen:

1. Auf welcher rechtlichen Grundlage dürfen die personenbezogenen Daten Dritter (Eltern, Lebensgefährten) übermittelt werden?

In Betracht käme Art. 6 Abs. 1 S. 1 f) DS-GVO, wenn die Auslandseinsätze arbeitsvertraglich geschuldet werden und deshalb ein überwiegendes berechtigtes Interesse des Arbeitgebers angenommen werden kann. Ansonsten wäre die Einwilligung der betroffenen Personen einzuholen.
Zusätzlich zu einer Rechtsgrundlage nach Art. 6 DS-GVO sind, wenn die Daten in ein Drittland ohne angemessenes Datenschutzniveau übermittelt werden sollen, die Vorgaben des Kapitels V der DS-GVO einzuhalten. Für die Übermittlung an Behörden des betreffenden Drittlandes kommt aus unserer Sicht v.a. eine Einwilligung der betroffenen Angehörigen gem. Art. 49 Abs. 1 S. 1 a) DS-GVO in Betracht, u.U. auch eine Übermittlung auf Grundlage von Art. 49 Abs. 1 S. 1 e) DS-GVO.

Frage / Antwort 3: Datenschutz bei Auslandseinsätzen (III)

2. Ist ein Zertifikat, dass einem Mitarbeiter „fit for the job“ ohne Angabe medizinischer Befunde bestätigt oder ein negativer Test (z.B. HIV) als Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO zu bewerten? Wenn ja, auf welcher rechtlichen Grundlage dürfen diese Daten übermittelt werden, da in einem Arbeitsverhältnis die Einholung einer Einwilligung an der Freiwilligkeit scheitern dürfte?

Jedenfalls bei einem negativem HIV Testergebnis würden wir von einem Gesundheitsdatum ausgehen; es ist in diesem Zusammenhang auf § 26 Abs. 3 BDSG zu verweisen. Für die Frage, ob die Voraussetzungen der Vorschrift erfüllt sind, kommt es darauf an, ob die Auslandseinsätze arbeitsvertraglich geregelt sind bzw. solche von der geschuldeten Arbeitsleistung umfasst sind.

Auch hier muss zusätzlich zu den Voraussetzungen des Art. 6 und Art. 9 DS-GVO noch eine Übermittlungsgrundlage nach Kapitel V DS-GVO erfüllt werden. Für die Übermittlung dieses Datums an Behörden des Drittlands kann grundsätzlich, auf Art. 49 Abs. 1 S. 1 b) DS-GVO abgestellt werden, weil die Übermittlung als für das Beschäftigungsverhältnis erforderlich angesehen werden kann.

Frage / Antwort 3: Datenschutz bei Auslandseinsätzen (IV)

3. Dürfen die Daten ohne Einwilligung gespeichert werden, so dass die Mitarbeiter nicht bei jedem Visumantrag neu die Daten zur Verfügung stellen müssen? Wenn ja, welche (nicht)?

Eine Einwilligung ist möglich, allerdings kann nur in die Verarbeitung der eigenen Daten eingewilligt werden. Was Daten Angehöriger angeht, so müsste daher der jeweilige Angehörige in eine solche dauerhaften oder wiederholte Übermittlung einwilligen.

4. Dürfen die Daten auf Basis einer Einwilligung gespeichert werden, wenn unsere Mitarbeiter selbst anregen, die Daten dauerhaft zu speichern, um nicht für jeden neuen Antrag diese zur Verfügung stellen zu müssen?

Siehe Antwort zu Frage 3.

Frage 4: Unterauftragnehmer außerhalb der EU (I)

Unser Unternehmen verwendet Tools im Rahmen einer Auftragsverarbeitung von Dienstleistern. Bei manchen dieser Tools erfolgt ein Tracking durch den jeweiligen Dienstleister.

Das Tracking ist nicht Teil der von unserem Unternehmen beauftragten Leistungen, eine Auswertung der getrackten Daten erhält unser Unternehmen nicht.

Üblicherweise enthalten die Tools eine Cookie-Policy des jeweiligen Dienstleisters, die mit dem Tracking auch übereinstimmen. Andere verwenden das Tracking in anonymisierter Form.

Die meisten Tools verarbeiten lediglich personenbezogene Daten, die über den Geschäftskontakt nicht hinausgehen (Vorname, Familienname, geschäftliche Email-Adresse).

Frage 4: Unterauftragnehmer außerhalb der EU (II)

Beispiel: Ein Dienstleister bietet ein Tool an, dass mehrere seiner Kunden benutzen. Jeder Kunde greift auf das Tool über dieselbe Webseite zu. Auf der Webseite kann sich der jeweilige Nutzer anmelden. Ferner enthält diese Webseite einen Cookie-Banner mit Cookie-Policy aus der hervorgeht, dass personenbezogene Daten u.a. getrackt werden.. Nach dem Log In wir der Nutzer des Tools auf den jeweils für sein Unternehmen vorgesehen Bereich geleitet. In dem für unser Unternehmen reservierten Bereich, in dem unsere Mitarbeiter über das Log In gelangen, findet kein Tracking statt.

Da das Tracking im Interesse des Dienstleisters erfolgt, wäre nach unserer Auffassung dieser für die Verarbeitung der personenbezogenen Daten verantwortlich. Die Auftragsverarbeitung findet dagegen erst nach dem Log In statt.

Hier sollten bei einer Auftragsverarbeitung nur solche personenbezogenen Daten durch den Dienstleister verarbeitet werden, wie dies von unserem Unternehmen beauftragt wird (was in dem Beispiel der Fall ist).

- Uns stellt sich daher die Frage, ob unser Unternehmen vor dem Einsatz eines solchen Tools das Tracking des Dienstleister analysieren muss?
- Ist unser Unternehmen verpflichtet, das Tracking abstellen zu lassen? Wenn ja, ist das unter allen Umständen oder nur Risko basiert der Fall?
- Unter welchen Umständen geht das BayLDA davon aus, dass ein Tracking tatsächlich anonym ist und damit nicht in den Anwendungsbereich der DSGVO fällt?

Antwort 4 (I):

Grundsätzlich ist für jede Datenverarbeitung zu prüfen, wer hierfür Verantwortlicher im Sinne von Art.4 Nr. 7 DS-GVO ist. In dem dargestellten Sachverhalt wird im Einzelfall zu prüfen sein, ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vorliegt.

Zur Abgrenzung im Allgemeinen: https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf

So wie der Sachverhalt dargestellt wird, kann eine gemeinsame Verarbeitung nicht ausgeschlossen werden. Das „Tracking“ unterliegt nicht der Auftragsverarbeitung, allerdings veranlasst das Unternehmen durch den Einsatz des Dienstleisters, dass das „Tracking“ erst ermöglicht wird. Die Tatsache, dass das Unternehmen die Ergebnisse des Trackings nicht zur Verfügung hat, ist hierfür nicht von Bedeutung und schließt die gemeinsame Verantwortlichkeit nicht aus.

Sofern, wie hier angenommen, das „Tracking“ in eigener Verantwortlichkeit durch den Dienstleister durchgeführt wird, besteht grundsätzlich keine Verpflichtung des Unternehmens dies zu analysieren und zu prüfen. Art. 28 DS-GVO erlegt dem Verantwortlichen nur Pflichten im Rahmen des Auftragsverarbeitungsverhältnisses und damit den konkreten Datenverarbeitungen auf. Jedoch führen die Anforderungen aus Absatz 1 auch dazu, dass eine sorgfältige Auswahl des Dienstleisters stattfindet.

Antwort 4 (II):

Sollten daher dem Unternehmen offensichtliche Rechtsverstöße erkennbar werden, auch wenn diese nicht im Zusammenhang mit der Datenverarbeitung des Auftragsverarbeitungsverhältnisses steht, sollte dies zu einer erneuten Überprüfung führen, ob hier ein geeigneter Dienstleister ausgewählt wurde.
Dies gilt erst recht, wenn Verarbeitungstätigkeiten im Zusammenhang mit dem Auftragsverarbeitungsverhältnis stehen.
Unabhängig von der Konstellation ist es nicht erforderlich, das „Tracking“ zu untersagen. Die Frage ist, ob dieses rechtmäßig erfolgt. Im Regelfall bedarf es für „Tracking“ einer Einwilligung. Hierfür muss in einem ersten Schritt geprüft werden, ob der Anwendungsbereich des § 25 TTDSG eröffnet ist, also beispielsweise Cookies gesetzt werden und ob hierfür eine Einwilligung erforderlich ist (Cookies zum Zwecke des „Trackings“ bedürfen immer einer Einwilligung). § 25 TTDSG gilt unabhängig davon, ob personenbezogene Daten verarbeitet werden, also auch bei „anonymen“ Daten. In einem zweiten Schritt ist zu prüfen, ob die nachfolgende Datenverarbeitung der DS-GVO unterliegt (liegen personenbezogene Daten vor?) und eine Rechtsgrundlage nach Art. 6 DS-GVO einschlägig ist. Bei „Tracking“ ist auch hierfür im Regelfall eine Einwilligung erforderlich.

Antwort 4 (III):

Sofern also eine rechtswirksame Einwilligung nach DSGVO und ggfs. TTDSG eingeholt wird, kann das „Tracking“ weiterhin durchgeführt werden.

„Tracking“ kann an sich dem Begriff nach schon nicht anonymisiert erfolgen, da damit ja gerade eine Nachverfolgung bezweckt werden soll. Generell gelten auch im Kontext „Tracking“ die gleichen Vorgaben wie auch für andere Datenverarbeitungen, d.h. eine Anonymisierung liegt nur dann vor, wenn der Personenbezug komplett entfernt wird. Wie sich auch aus dem Beschluss der DSK zu Google Analytics vom 12.05.2020 (https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf) im Hinblick auf die Kürzung der IP-Adresse ergibt, ist eine Anonymisierung in diesem Kontext genau zu prüfen, da oftmals nur eine Pseudonymisierung vorliegt.
Aber wie bereits dargestellt, ist unabhängig davon im Regelfall schon eine Einwilligung nach § 25 TTDSG erforderlich, da dessen Anwendungsbereich auch bei nicht personenbezogenen Daten eröffnet ist.

Frage 5: Löschumsetzung und Umgang mit Betroffenenrechten bei Git-Repositories

GIT wird bei uns im Unternehmen für die Versionskontrolle von Code genutzt. Dabei können personenbezogene Daten der Nutzer im Rahmen der Commits verarbeitet werden.
Für die Löschumsetzung und den Umgang mit Betroffenenrechten (insb. das Recht auf Löschung) möchten wir im Unternehmen folgende Vorgehensweise implementieren. Ist dies aus Sicht des BayLDA ausreichend?

- Projekte im persönlichen Namespace der Mitarbeiter werden innerhalb von drei Monaten nach Ausscheiden des Mitarbeiters aus dem Unternehmen gelöscht.
- Der **aktive Code** inkl. der Commits muss regulatorisch für den Zeitraum der Nutzung des Codes nachvollziehbar gespeichert werden. Jedoch kann hier datensparsam eine Pseudonymisierung implementiert werden, indem die Klarnamen durch die Personalnummern ersetzt werden. Dadurch wäre im Zeitverlauf die Personenbeziehbarkeit a) nur mit Zusatzwissen und b) bei Ausscheiden aus dem Unternehmen nicht ohne Weiteres herzustellen. Die Mitarbeiter werden über dies Möglichkeit der Pseudonymisierung informiert und können diese selber in ihrem Profil einrichten. (=KANN-Regelung).
- Der **passive Code** (nach Deaktivierung einer Anwendung) wird in ein Archivsystem transferiert und geregelt; nach Ablauf der notwendigen Aufbewahrungsfrist gelöscht.
- Ein Löschersuchen eines Mitarbeiters wäre lediglich im persönlichen Namespace sofort umsetzbar. Im aktiven oder passiven Code überwiegen die Nachweispflichten des Unternehmens an einer durchgängigen Versionskontrolle.

Antwort 5:
…wird nachgereicht

Frage 6: Anschreiben des BayLDA an die Versicherungswirtschaft

Das LDA hat am 21.11.23 50 Firmen angeschrieben mit der Bitte, Verarbeitungen aufzulisten, die in einer Schwellwertanalyse zu einer DSFA geführt haben und weitere Informationen zu diesen Verarbeitungen erbeten. Es sind alle Versicherungen in Nürnberg betroffen. Vielleicht kann der Vertreter des LDA dazu etwas sagen.

Antwort 6:

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht als Datenschutzaufsichtsbehörde nach Art. 58 der DS-GVO die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich im Bundesland Bayern, d. h. in privaten Wirtschaftsunternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden. Zu diesem Zweck führt das BayLDA auch flächendeckende Prüfungen zu verschiedenen Schwerpunktthemen durch, bspw. um grundlegende Sicherheitslücken oder organisatorische Defizite aufzuzeigen und Verantwortliche somit auf den Bedarf an durchzuführenden Maßnahmen hinzuweisen. Auch wenn der vorbeugende Charakter der Datenschutzkontrollen des BayLDA hervorgehoben wird, besteht grundsätzlich weiterhin die Möglichkeit, bei Datenschutzverstößen Geldbußen gegen Verantwortliche zu verhängen.

Im November hat das BayLDA im Rahmen dieser gesetzlichen Aufgaben eine Datenschutzprüfung zum Thema Schwellwertanalyse von Verarbeitungstätigkeiten gestartet. Bei dieser Prüfung untersuchen wir zufällig ausgewählte Verantwortliche hinsichtlich Einträgen des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DS-GVO), bei denen die Schwellwertanalyse zur Datenschutzfolgenabschätzung (Art. 35 DS-GVO) wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen ergeben hat. Die von uns angeschriebenen Unternehmen kommen dabei aus ganz unterschiedlichen Branchen, so z. B. auch aus dem Bereich Versicherung, aber auch aus den Bereichen Gesundheit, Automobile/Maschinenbau oder Lebensmittel/Einzelhandel.

Vielen Dank für Ihre Aufmerksamkeit!