Bayerisches Landesamt für Datenschutzaufsicht

ERFA-Kreis

Nürnberg – 14.03.2024

Wer steht heute vor Ihnen?

Andreas Sachs

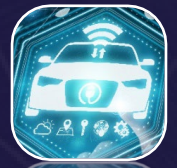
Bereichsleiter **Cybersicherheit und Technischer Datenschutz** &
Vize-Präsident beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Themenfelder:


Künstliche Intelligenz


Smart Things


Cybersicherheit


Automotive


Prüfstrategie Prüfverfahren


Verschlüsselung


Datenschutz-folgenabschätzung

Themen aus der Praxis

Punkt 1: Besondere Kategorien nach Art. 9 Abs. 1 DS-GVO?

Frage:
*„Nach § 22 Abs. 3 Personenstandsgesetz sind für **Angaben zum Geschlecht** die Felder weiblich, männlich, leer oder divers zu verwenden. Ergibt sich **allein aus diesen Angaben** dann ein Datum, das das den **besonderen Kategorien** nach Art. 9 Abs. 1 DS-GVO „sexuelle Orientierung" zuzurechnen ist?"*

Einschätzung BayLDA:
Wir würden uns der Ansicht anschließen, die darauf abstellt, dass sexuelle Orientierung sich an dem Interesse an anderen ausrichtet und eine **Ablehnung der Zuordnung zu Art. 9** Abs. 1 DS-GVO Daten vertreten.

Themen aus der Praxis

Punkt 2: Rechtsgrundlagen für Ausschüsse?

In unserem Unternehmen besteht ein Sprecherausschuss, der die Interessen der leitenden Angestellten vertritt. Der Sprecherausschuss möchte folgende Angaben zu den Leitenden Angestellten haben: Name, Geburtsdatum, Eintritt zur Betriebszugehörigkeit, Ernennung zum Leitenden Angestellten. Dies brauche der Sprecherausschuss um seinen Aufgaben nach dem Sprecherausschussgesetz nachkommen und um mittels Gratulationen zu bestimmten Jahrestagen und Geburtstagen seinen Beitrag zu einem guten Betriebsklima leisten zu können.

SprAuG lautet: § 25 Aufgaben des Sprecherausschusses
(1) Der Sprecherausschuß vertritt die Belange der leitenden Angestellten des Betriebs (§ 1 Abs. 1 und 2). Die Wahrnehmung eigener Belange durch den einzelnen leitenden Angestellten bleibt unberührt.
(2) Der Sprecherausschuß ist zur Durchführung seiner Aufgaben nach diesem Gesetz rechtzeitig und umfassend vom Arbeitgeber zu unterrichten. Auf Verlangen sind ihm die erforderlichen Unterlagen jederzeit zur Verfügung zu stellen.

*Reicht **§ 25 II SprAuG als Rechtsgrundlage** iVm Art. 6 Abs. I lit. c DS-GVO aus **oder** müsste die **Rechtsgrundlage über eine Zweckänderung** nach Art. 6 Abs. 4 DS-GVO begründet werden? **Alternativ** müsste für jeden Fall eine **Einwilligung** eingeholt werden.*
Und trifft dies auch für die Angabe der Geburtstage von Führungskräften (Abteilungsleiter / leitende Angestellte) gegenüber Vorständen zu, wenn Vorstände diesen gratulieren möchten? Gibt es dabei einen Unterschied zu den Daten aller Beschäftigten innerhalb eines Vorstandsbereichs?

Themen aus der Praxis

Punkt 2: Rechtsgrundlagen für Ausschüsse?

Einschätzung BayLDA:
„§ 25 Abs. 2 SprAuG werten wir **nicht** als eine **nationale Rechtsgrundlage** für die Verarbeitung gem. Art. 6 Abs. 1 Uabs. 1 Buchst. c DS-GVO, da es sich hieraus **keine konkrete** rechtliche Verpflichtung des Arbeitgebers ergibt. Vielmehr müsste die konkreten Aufgaben des Sprecherausschusses betrachtet werden, bspw. § 31 Spr.AuG und geprüft werden, inwieweit sich hieraus eine konkrete Verpflichtung des Arbeitgebers ergeben kann, die erforderlichen Informationen an den Sprecherausschuss weiterzugeben.

Die **Weitergabe** personengezogener Daten **an den Sprecherausschuss**, um zu **gratulieren**, kann ausschließlich auf eine **Einwilligung** gestützt werden.“

Themen aus der Praxis

Punkt 3: Weitergabe von Mitarbeiter-Daten des IT-Dienstleisters an den Kunden

Frage:

*Bei der **Leistungserbringung für unsere Kunden** werden für den **Remotezugriff unserer Mitarbeiter auf die Kundensysteme** eigene **Identifier/Accounts** durch den Kunden angelegt. Für die Erstellung eines solchen Identifier/Accounts werden **Name und geschäftliche E-Mailadresse** unserer Mitarbeiter an den Kunden weitergegeben. Als Rechtsgrundlage für die Weitergabe dieser Daten dürfte i.d.R. Art. 6 Abs. 1 Buchstabe f) DS-GVO herangezogen werden, d. h. es handelt sich um die Wahrung berechtigter Interessen des Kunden bzw. des Auftragsverarbeiter, soweit hier kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der Betroffenen überwiegt. Eine Weitergabe von Mitarbeiter-Namen und Mailadressen ist in dem Fall im Zuge einer Interessenabwägung nicht als besonders schutzwürdig zu sehen, das Interesse des Kunden sowie des IT-Dienstleisters ist in diesem Fall wohl höher einzustufen.*

*Wie aber verhält es sich, wenn **zusätzliche Angaben** gefordert werden, wie*

- *Geburtsdatum*
- *Geburtsort*
- *Nationalität*
- *Privatanschrift*
- *Kopie des Personalausweises*

*Welche **Rechtsgrundlage** könnte hier herangezogen werden? Weder das berechtigte Interesse noch die Einwilligung der Beschäftigten scheint uns für die Weitergabe dieser Daten passend.*

Themen aus der Praxis

Punkt 3: Weitergabe von Mitarbeiter-Daten des IT-Dienstleisters an den Kunden

Einschätzung BayLDA:

Die Datenschutzbehörde ist nicht allwissend – **ohne** dass uns der **genaue Zweck** bekannt ist, zu dem der Kunde meint, diese Daten(kategorien) zu benötigen, können wir **keine abschließende Bewertung** abgeben. Hier müssten Sie schlicht beim Kunden nachfragen, wofür genau das einzelne Datum benötigt wird.

Als **Rechtsgrundlage** wäre je nach Fall z.B. an **Art. 6 Abs. 1 Buchst. b** oder **Buchst. f** DSGVO zu denken.

In Fällen, in denen die **Daten zur Durchführung des Beschäftigungsverhältnisses erforderlich** angesehen werden können, kann **Art. 6 Abs. 1 Buchst. b DSGVO** einschlägige Rechtsgrundlage sein; dies kann z.B. der Fall sein, wenn es um Ansprechpartner für den Auftraggeber geht. In anderen Fällen kann grundsätzlich Buchstabe f in Betracht kommen. Soweit es evtl. irgendeine gesetzliche Verpflichtung für den Auftraggeber gibt, könnte auf dessen Seite auch Art. 6 I c DS-GVO eine Rolle spielen; dies wäre eben zu erfragen.

Themen aus der Praxis

Punkt 3: Weitergabe von Mitarbeiter-Daten des IT-Dienstleisters an den Kunden

Einschätzung BayLDA:

Jedenfalls: Stets dürfen nur solche Daten übermittelt werden, die für den **konkreten Zweck erforderlich** sind. Welcher Zweck es ist, müsste (sofern es nicht klar ist) mit dem Geschäftspartner geklärt werden. Wenn der Zweck in der Anlegung der Identifier/Accounts zwecks Ermöglichung von Remotezugriff liegt, wäre also zu fragen, welche Daten genau hierfür benötigt werden und welche nicht. Wir als Außenstehende können das auf der Basis der hier mitgeteilten knappen Informationen nicht abschließend bewerten. Diese Fragen müssten Sie daher an den Kunden stellen, d.h.: Warum genau soll jede einzelne der oben genannten Datenkategorien benötigt werden?

Nicht **ohne weiteres erkennbar** ist aus unserer Sicht z.B., wofür die **Privatanschrift** benötigt wird; hier ist zu vermuten, dass die Firmenanschrift des Arbeitgebers oder ähnliches genügt. Wenn das „technisch nicht möglich" ist o.ä., dann ist das datenschutzrechtlich nicht akzeptabel, d.h. die Software müsste dann an diesem Punkt geändert werden.

Ebenfalls **problematisch** ist grundsätzlich die **Kopie eines Personalausweises**; üblicherweise wir hiermit der Zweck verfolgt, die Person eindeutig zu identifizieren. Hier wäre vorrangig zu prüfen, ob eine andere Identifizierungsmöglichkeit zumutbar ist – d.h. eine solche, bei der keine unnötigen Daten (wie z.B. die auf der Kopie enthaltenen Personalausweisnummer, die sog. Zugangsnummer u.a.) erhoben werden ,sondern allein die zur Identifizierung erforderlichen Daten (hierfür genügen aus unserer Sicht in aller Regel Vor- und Nachname sowie Geburtsdatum; bei der Privatanschrift ist eigentlich nicht einzusehen, warum sie erforderlich sein soll, stattdessen genügt u.E. die Firmenanschrift des Arbeitgebers).

Themen aus der Praxis

Punkt 4 a: Besondere Kategorien nach Art. 9 Abs. 1 DS-GVO?

Frage:

*In der Praxis stellt sich manchmal die Frage, **wann Daten** unter die **besonderen Kategorien von personenbezogenen Daten** gem. Art. 9 Abs. 1 DSGVO **fallen**. In unserem Unternehmen verlangen Kunden von Zeit zu Zeit Gesundheitszertifikate, in denen dem Mitarbeiter lediglich bestätigt wird, dass **er für die Tätigkeit gesundheitlich fit** ist. Weitere medizinische Details, wie der Arzt zu der Feststellung kommt, werden nicht verarbeitet. Fällt die Bestätigung, dass jemand gesund ist unter Art. 9 Abs. 2 DSGVO?*

Einschätzung BayLDA:

Die Frage kann in der Abstraktheit nicht beantwortet werden, da sie vom konkreten Kontext abhängt. Der **Begriff der Gesundheitsdaten ist weit zu verstehen**. Der Befund, gesund zu sein, kann ein Gesundheitsdatum gemäß Art. 9 Abs. 1 DS-GVO darstellen, wenn durch die **Verknüpfung mit weiteren Informationen** (z.B. dem Ausstellungsgrund oder die Art der Tätigkeit, für die das Zertifikat ausgestellt wird) **Rückschlüsse auf die körperliche oder geistige Verfassung einer Person möglich** sind. Z. B. kann die gesundheitliche Eignung für eine Tätigkeit in tropischen Zonen Rückschlüsse auf die körperliche Belastbarkeit und den Impfstatus zulassen und wäre damit ein Gesundheitsdatum nach Art. 9 Abs. 1 DS-GVO.

Themen aus der Praxis

Punkt 4 b: Besondere Kategorien nach Art. 9 Abs. 1 DS-GVO?

Frage:
Für die Gehaltsabrechnung ist es zur Einstufung in eine Steuerklasse erforderlich, dass der Arbeitgeber den Familienstand des Mitarbeiters kennt. Wenn sich daraus ergibt, dass dieser mit einer ***Frau oder einem Mann verheiratet*** *ist, lassen sich* ***Rückschlüsse auf dessen sexuelle Orientierung*** *erkennen. Ähnliches gilt, wenn die Personalabteilung fragt, wen das Unternehmen im Notfall kontaktieren soll. Fällt die Information über den Familienstand unter Art. 9 Abs. 1 DSGVO, wenn sich aus dieser ergibt, ob jemand mit einem Mann oder Frau verheiratet ist?*

Einschätzung BayLDA:
Ja (vgl. Entscheidung des EuGH vom 01.08.2022, Az. C-184/20).

Themen aus der Praxis

Punkt 5: Zuständigkeit IT-Beurteilung TOM

Frage:
Gem. Art. 28 Abs. 3 e) DSGVO muss der Verarbeiter technische und organisatorische Maßnahmen gem. der Kritikalität der verarbeiteten Daten anbieten. Es stellt sich die Frage, wer diese im Vertrag zu bewerten hat:
a) eine IT-Abteilung, die diese technischen und organisatorischen Maßnahmen bewerten kann, auch im Hinblick auf andere, nicht personenbezogene Daten oder
b) die Datenschutzabteilung, nur weil die Anforderung in der DSGVO steht, aber nicht über die fachliche IT-Expertise verfügt, um die Maßnahmen bewerten zu können?

Themen aus der Praxis

Punkt 5: Zuständigkeit IT-Beurteilung TOM

Einschätzung BayLDA:

Letztlich spricht viel dafür, dass es ein „**gemeinsames Werk**“ aus den operativen Einheiten des Unternehmens (etwa der IT-Abteilung) und dem Datenschutzbeauftragten ist. Die Aufgabe kann jedenfalls **nicht allein auf den Datenschutzbeauftragten** delegiert werden, denn **die operative Verantwortung zur Einhaltung der datenschutzrechtlichen Anforderungen hat stets der Verantwortliche** – und nicht der Datenschutzbeauftragte.

Der **Datenschutzbeauftragte** hat gemäß Artikel 39 Abs. 1 DSGVO eine **beratende und überwachende Funktion**, nicht jedoch eine operative Funktion. Der Datenschutzbeauftragte muss jedoch vom Verantwortlichen (d.h. von der zuständigen Fachabteilung, z.B. typischerweise im vorliegenden Fall etwa von der IT-Abteilung) gemäß Art. 38 Abs. 1 DSGVO **ordnungsgemäß** und **frühzeitig** in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **eingebunden werden**. Es wird aber immer so sein, dass der Datenschutzbeauftragte lediglich „beraten“ und „überwachen“ kann; die datenschutzrechtliche Verantwortung verbleibt bei der Geschäftsleitung bzw. den von dieser beauftragten Fachabteilungen - wobei die Geschäftsleitung bei Delegation auf Fachabteilungen jedenfalls die Pflicht zur Auswahl geeigneten Personals und zur allgemeinen Überwachung hat (d.h. sie muss sich Bericht erstatten lassen).

Wir verweisen zu den Aufgaben des Datenschutzbeauftragten auf das Arbeitspapier 243rev.01 der Artikel-29-Gruppe der Datenschutzbehörden (der Europäische Datenschutzausschuss hat sich dieses Papier zu eigen gemacht, siehe https://ec.europa.eu/newsroom/article29/items/612048).

Vielen Dank für Ihre Aufmerksamkeit

Gibt es noch Fragen?