BayLDA

Bayerisches Landesamt für
Datenschutzaufsicht

# Fragen und Antworten zur Sitzung des GDD-ERFA-Kreises Nürnberg vom 27.07.2023

# Frage 1: Datenschutzmeldung: Einschätzung geringes Risiko

Art. 33 DSGVO verlangt eine **Meldung an das BayLDA**, wenn eine Datenschutzverletzung ein „Risiko für die Rechte und Freiheiten“ des Betroffenen darstellt. Im **Formular** zur Meldung von Datenpannen heißt es, dass „ein **geringes Risiko** bedeutet, dass weder die mögliche **Schwere des Schadens** für den Betroffenen noch die **Eintrittswahrscheinlichkeit** hoch sind und in Kombination weder mittel noch hoch.“

Nach unserem Verständnis liegt ein solches geringes Risiko vor, wenn z.B. ein unberechtigter Dritter den **Namen und die dienstliche Email-Adresse eines oder mehrerer Betroffener** erhalten hat, da anders als bei privaten Adressdaten, nicht erkennbar ist, zu welchem Schaden das bei dem Betroffenen führen soll.

Deckt sich diese Ansicht mit der des BayLDA bezüglich der Definition „geringes Risiko“?

# Antwort 1:

Aus unserer Sicht lässt sich die Frage nicht ganz so pauschal beantworten. Es braucht natürlich immer eine Risikobewertung, die auch die **Ursache für die Offenlegung** betrachtet, also auch in den Blick nimmt**, wer der unberechtigte Dritte ist, der die E-Mail-Adresse erlangt hat**.

Ist die E-Mail-Adresse z. B. im Rahmen eines offenen E-Mails-Verteilers nur einem begrenzten Adressatenkreis bekannt geworden, lässt sich der Argumentation aus der Frage sicher folgen.

Sollte die E-Mail-Adresse jedoch im Rahmen eines Cyberangriffes abgegriffen worden sein, ist natürlich das Missbrauchspotential höher und somit muss die Risikoeinschätzung auch anders sein bzw. gegebenenfalls auch zu einem anderen Ergebnis kommen. Hier ist man dann schneller in der Meldeverpflichtung.

# Frage 2: Meldestelle nach HinSchG

a) **Wenn das nach HinSchG verpflichtete Unternehmen sich entscheidet die interne Meldestelle an einen Dritten auszulagern, ist zwischen den Parteien eine Auftragsverarbeitungsvereinbarung zu schließen oder erfolgt gemäß § 10 HinSchG eine Datenverarbeitung durch den Dritten als Verantwortlicher (=keine Auftragsverarbeitung)?**

Auch wenn es in der Gesetzesbegründung BT-Drs. 20/5992 heißt:
„Soweit externe Dritte im Rahmen einer Auftragsverarbeitung mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden, sind die Vorgaben für Auftragsdatenverarbeitungen zu beachten, vergleiche Artikel 28 DSGVO.“ , gehen wir davon aus, dass bei einer (vollständigen) Auslagerung im Regelfall eine Verantwortlichkeit der extern beauftragten Stelle bestehen wird. Die extern beauftragte Stelle wird regelmäßig selbst über die konkreten Zwecke der einzelnen Verarbeitungstätigkeiten und über die wesentlichen Mittel der Datenverarbeitung entscheiden.
Allerdings haben wir bisher noch keine praktischen Erfahrungen, wie ein externer Betrieb einer internen Meldestelle konkret ausgestaltet wird, so dass diese Einschätzung auf dem derzeitigen Kenntnisstand unter Betrachtung der Regelungen im Hinweisgeberschutzgesetz fußt.

# Frage 2: Meldestelle nach HinSchG

**b) Folgefrage: Falls eine Auftragsverarbeitungsvereinbarung zu schließen sein sollte, gilt dies auch, wenn als interne Meldestelle ein Rechtsanwalt oder eine Rechtsanwaltskanzlei zur Ombudsperson(en) bestellt wird?**

Siehe Antwort zu Frage a). Auch hier gehen wir von einer Verantwortlichkeit der Rechtsanwaltskanzlei bzw. der Rechtsanwältin/ des Rechtsanwaltes aus.

**c) Folgefrage: Falls eine Auftragsverarbeitungsvereinbarung zu schließen sein sollte, ist dann der Arbeitgeber als Verantwortlicher in der Datenschutzinformation der Meldekanäle zu nennen, obwohl das Betreiben der Meldekanäle Aufgabe der Meldestelle ist?**

Siehe Antwort zu Frage a); es wird nicht von einer Auftragsverarbeitung ausgegangen. In beiden Fällen ist jedoch transparent darzulegen, wem die Meldestelle zuzuordnen ist.

# Frage 2: Meldestelle nach HinSchG

**d) Gelegentlich ist die Meinung zu lesen, dass bei der Einrichtung einer internen Meldestelle stets eine Datenschutzfolgenabschätzung vorzunehmen ist. Wie ist hierzu die Haltung des BayLDA?**

„Die DSK-Orientierungshilfe zu Whistleblowing-Hotlines (abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf) sah das Erfordernis der Durchführung einer DSFA.
Ein zwingendes Erfordernis bei der Einrichtung interner Meldestellen zur Durchführung einer DSFA sehen wir derzeit jedoch nicht. Vielmehr bedarf es einer Betrachtung der konkreten Umstände und Risiken. Hierzu gehört z.B. auch die Größe eines Unternehmens sowie dessen Struktur und Einbindung in eine Unternehmensgruppe.“

# Frage 3: Konsequenzen des DataPrivacyFramework (DPF)

Auf Basis des **DSK-Beschluss zur „Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten“ vom 31. Januar 2023** sind an die **Sorgfalt der Zuverlässigkeitsprüfung im Sinne von Art. 28 Abs. 1 DSGVO besonders hohe Anforderungen** zu stellen, soweit eine Norm oder Praxis eines Drittlands die **abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus dem EWR in ein Drittland** durch eine als Auftragsverarbeiter tätige Stelle in dem EWR – z.B. die EWR-Tochtergesellschaft eines Drittlands-Unternehmens – begründet.

Festgehalten wird im Beschluss eine weitergehende Prüfpflicht dahingehend, ob der **Auftragsverarbeiter hinreichend Garantien dafür bietet, dass es nicht zu Verarbeitungen kommt, die nach den Maßstäben der DSGVO bzw. des anwendbaren mitgliedstaatlichen Rechts unzulässig sind**.

# Frage 3: Konsequenzen des DataPrivacyFramework (DPF) (2)

Soweit nun für die USA mit dem DataPrivacyFramework (DPF) ein angemessenes Datenschutzniveau in den USA festgestellt wird, kann nach unserer Lesart davon ausgegangen werden, dass damit keine abstrakte Gefahr einer unzulässigen Übermittlung von personenbezogenen Daten, die in der EU/EWR gespeichert sind, auf Basis des Cloud Acts in die USA bestehen kann, wenn sich der entsprechende Auftragsverarbeiter für das Data Privacy Framework zertifiziert hat.

Dann entfallen nach unserem Verständnis die weiteren Prüfpflichten, die im DSK-Beschluss festgehalten werden.

Aus unserer Sicht ergibt sich das daraus, dass der Cloud Act bestehende Zugriffsrechte in den USA extraterritorial, aber nicht materiell, erweitert. Wenn aber auf Basis der Gesetzeslage in den USA das Datenschutzniveau für die aktive Datenübermittlung als angemessen angesehen wird, kann aus unserer Sicht a maiore ad minus bei einer grundsätzlichen Datenverarbeitung in der EU durch ein Tochterunternehmen, dessen Konzernmutter unter den Angemessenheitsbeschluss des DPF fällt, nichts anderes gelten. Sonst wären die Prüfpflichten innerhalb der EU strenger als bei einer generellen Auslagerung in ein Drittland mit Angemessenheitsbeschluss.

Sehen Sie das auch so?

## Antwort 3:

Zum DPF ist festzuhalten, dass die Feststellung eines angemessenen Datenschutzniveaus durch die EU-Kommission nicht insgesamt für die USA gilt, sondern nur für Übermittlungen an US-Unternehmen, die auf der von der US-Administration geführten „DPF-Liste“ geführt sind und dort eine gültige Zertifizierung haben (https://www.dataprivacyframework.gov/s/participant-search).

Für die hier gestellte Frage, wie es sich mit Datenverarbeitung in der EU durch (EU-)Tochterunternehmen US-amerikanischer Konzerne verhält, gilt aus unserer Sicht folgendes:
Unseres Erachtens ist (anders als für echte Datentransfers in die USA, s.o.) bei Datenverarbeitungen in der EU durch EU-Tochtergesellschaften US-amerikanischer Konzerne bei der Frage von Zugriffsmöglichkeiten US-amerikanischer Behörden und der danach zu beurteilenden Zuverlässigkeit des Auftragsverarbeiters nicht danach zu unterscheiden, ob die US-Muttergesellschaft eine DPF-Zertifizierung besitzt.
Entscheidend ist in diesem Szenario vielmehr die Frage des Umfangs von Zugriffsmöglichkeiten der US-Behörden nach FISA702 und Executive Order 12.333 auf Daten außerhalb der USA (also z.B. bei den EU-Tochtergesellschaften US-amerikanischer Konzerne).

## Antwort 3:

Es geht somit hier darum, ob die im EuGH-Urteil „Schrems II“ vom 16.7.2020 für problematisch befundenen Punkte:

- der Verhältnismäßigkeit der Datenzugriffsmöglichkeiten nach FISA702 und Executive Order 12.333
- sowie des seinerzeit fehlenden Rechtsschutzes von EU-Personen gegen solche Zugriffe

inzwischen in der US-amerikanischen Rechtsordnung als behoben gelten können.

Maßgeblich ist hier die neue Executive Order 14.086 von US-Präsident Biden und ob also diese E.O. die beiden o.g. Problempunkte behoben hat. Laut Kommissions-Angemessenheitsbeschluss ist dies offenbar der Fall. Demnach führt die E.O. 14.086 und der ergänzende darauf basierende in den USA etablierte Rechtsschutzmechanismus Betroffener im Falle von Zugriffen von US-Nachrichtendiensten dazu, dass (so die Position der Europäischen Kommission im Angemessenheitsbeschluss) beide o.g. Probleme gelöst sind.

# Antwort 3:

Konkret:

1.) Problematik der Verhältnismäßigkeit:

Laut Erwägungsgrund 125 sind vom EuGH als problematisch eingestufte US-Regelungen FISA702 und Executive Oder 12.333 nun durch die E.O. 14086 so ergänzt worden, dass die Verhältnismäßigkeit von Datenzugriffsmöglichkeiten gewahrt ist (siehe Erwägungsgrund 125 – 153 der Angemessenheitsentscheidung). Die Datenzugriffsmöglichkeiten außerhalb der USA richten sich laut US-Regierung nicht nach FISA702, sondern nach E.O. 12.333. Laut Angemessenheitsbeschluss ist aber gerade auch E.O. 12.333 den durch die E.O. 14.086 eingeführten Anforderungen an die Verhältnismäßigkeit unterworfen (so Erwägungsgrund 124 und 125 – wichtig!). Auch wenn die Anforderungen für Datenzugang innerhalb der USA (für die FISA702 gilt) sogar noch zusätzlichen Anforderungen unterliegen (vgl. ErwGr 140 ff.), genügen gemäß dem Angemessenheitsbeschluss auch die Datenzugangsmöglichkeiten auf Basis der E.O.12.333 (also die Datenzugriffe außerhalb der USA) augenscheinlich nach Auffassung der Kommission somit den Anforderungen an die Verhältnismäßigkeit.

# Antwort 3:

2.) Rechtsschutz

Laut ErwGr 124 der Angemessenheitsentscheidung ist das Problem des fehlenden Rechtsschutzes gegen Datenzugriffe von US-Nachrichtendiensten nunmehr durch den neu eingeführten Rechtsschutzmechanismus (beschrieben in ErwGr 176-194 der Angemessenheitsentscheidung) gelöst worden. Auch dieser Mechanismus wurde durch dieselbe E.O. 14.086 von US-Präsident Biden etabliert; maßgebliche Bedeutung besitzen hier die auf Basis dieser E.O. erlassenen ergänzenden Regelungen des US-Justizministers (Attorney General Regulation establishing the Data Protection Review Court). Gemäß ErwGr 176 können EU-Personen diesen Rechtsschutzmechanismus nutzen und somit eine Beschwerde einlegen. Nach unserem Verständnis steht der Rechtsschutz somit nicht nur in solchen Fällen zur Verfügung, in denen formaljuristisch ein „Transfer personenbezogener Daten in die USA“ im Sinne von Kap. V DSGVO erfolgt ist, sondern immer, wenn eine EU-Person der Auffassung ist, dass sie von Überwachungsmaßnahmen nach E.O.12.333 (also außerhalb der USA) oder FISA702 (laut US-Regierung: innerhalb der USA) betroffen sein könnte. Einen Nachweis der eigenen Betroffenheit muss die Person im Übrigen nicht erbringen.

Die o.g. Analyse zeigt somit, dass die Problempunkte „Verhältnismäßigkeit“ und „Rechtsschutz“ nicht nur für Fälle gelöst wurden, in denen formaljuristisch eine „Übermittlung in die USA“ nach Kap. V DSGVO erfolgt ist, sondern auch für Fälle, in denen Daten etwa in der EU verarbeitet werden.

Vor diesem Hintergrund würden wir uns der in der gestellten Frage vertretenen Ansicht anschließen.

# *Vielen Dank für Ihre Aufmerksamkeit!*