FRT CONSULT GMBH
IT Dienstleistungen & Business Dienstleistungen

frtpartner

Telefon: 09221 / 900 - 0
Telefax: 09221 / 900 - 111
Kontakt: info@frtconsult.de
Adresse: Kurt-Schumacher-Str. 23
95326 Kulmbach

Datenschutz-Newsletter 2024 / IV

Aktuelles rund um den Datenschutz

Gesetz für Beschäftigtendaten

Nach langen Diskussionen und einer Entscheidung des EuGH aus 2023, die die Rechtslage in Deutschland in Frage stellte, wurde nun der Referentenentwurf für ein Beschäftigtendatengesetz (BeschDG) vom 8.10.2024 vorgelegt.

Der Entwurf umfasst 30 Paragrafen, so zum Umgang mit Bewerberdaten, zu Einwilligungen oder zur Erforderlichkeit als Rechtsgrundlage von Datenverarbeitungen, zu Kollektivvereinbarungen zum Datenschutz, zum Profiling und zur Übermittlung von Daten im Konzern. Der BeschDG-Entwurf regelt relevante Sachverhalte, hat aber auch Schwächen. So setzen viele datenschutzrechtliche Erlaubnisnormen eine Interessenabwägung im Rahmen einer Erforderlichkeitsprüfung voraus. Es werden viele sinnvolle Beispiele für entsprechende Kriterien genannt, viele Rechtsgrundlagen sehen jedoch auch eine unangemessene Verschiebung der Abwägungskriterien vor. Nach der DS-GVO ist eine Datenverarbeitung zur Wahrung berechtigter Interessen zulässig, wenn keine überwiegenden Interessen der betroffenen Person entgegenstehen. Jetzt soll der Arbeitgeber nachweisen, dass seine Interessen an der Verarbeitung überwiegen. Die DS-GVO gestattet den nationalen Gesetzgebern lediglich konkretisierende Regelungen – nicht jedoch neue Regeln mit anderen Maßstäben. Zudem ist die Abgrenzung von „Überwachung“ gegenüber zulässigen Kontrollen nicht gelungen und erschwert „normale“ Kontrollen.

Der Entwurf sieht auch Beweisverwertungsverbote z. B. bei unzulässiger Datenverarbeitung oder bei Kollektivvereinbarungen vor. Dies verstößt zum einen gegen Unionsrecht, zum anderen stellt dies auch einen Eingriff in die richterliche Unabhängigkeit dar.

Die zahlreichen umfassenden Informationspflichten des Arbeitgebers werden zu erheblichem Mehraufwand für Unternehmen führen. Auch der Betriebsrat soll künftig bei der Bestellung und Abberufung des Datenschutzbeauftragten mitbestimmen, der lediglich über die Einhaltung der Vorgaben des Datenschutzrechts wachen soll. Dies verstößt gegen die in der DS-GVO geforderte Unabhängigkeit.

Für praxisgerechte und rechtsklare Normen ist eine erhebliche Nacharbeit des Gesetzgebers erforderlich.

EDSA: Pflichten bei Auftragsverarbeitungsketten

Der Europäische Datenschutzausschuss (EDSA) hat in einer Stellungnahme 10/2024 die Pflichten von Verantwortlichen bei der Nutzung von Auftragsverarbeitern präzisiert. Der Fokus liegt auf der Rechenschaftspflicht, der Sicherstellung des Datenschutzes sowie auf Kontroll- und Dokumentationspflichten.

Kernaussagen der Stellungnahme:

1. Verantwortung bei langen Verarbeitungsketten:

Auch bei der Einbindung mehrerer Unterauftragsverarbeiter bleibt der Verantwortliche in der Pflicht. Dabei muss er die Identität und Tätigkeiten aller Beteiligten dokumentieren und regelmäßig aktualisieren lassen. Dies soll durch klare vertragliche Regelungen mit den Auftragsverarbeitern sichergestellt werden.

2. Prüfung und Kontrolle:

Verantwortliche sind verpflichtet, die Einhaltung der Datenschutzstandards auf jeder Stufe zu gewährleisten.

Sie können sich zwar auf die Prüfungen ihrer direkten Auftragsverarbeiter stützen, müssen jedoch bei Zweifeln oder Risiken selbst aktiv werden.

3. Keine generelle Pflicht zur Vertragsprüfung:
Es soll nicht erforderlich sein, systematisch alle Unterverarbeitungsverträge einzusehen. Eine Überprüfung ist jedoch notwendig, wenn Unklarheiten oder Risiken vorliegen.

4. Datenübermittlung in Drittländer:
Verantwortliche müssen sicherstellen, dass Datenübermittlungen außerhalb der EU den Anforderungen der Art. 44 ff. DSGVO entsprechen. Dies umfasst eine gründliche Prüfung der Garantien und Risiken bei der Verarbeitung in Drittländern.

5. Vertragliche Klarheit:
Der Auftragsverarbeitungsvertrag sollte präzise Regelungen zu Informationspflichten, Datenschutzstandards und Mitteilungen bei Änderungen enthalten, um Transparenz zu gewährleisten.

Fazit: Die Stellungnahme zeigt, dass Verantwortliche die volle Verantwortung für die Einhaltung der Datenschutzstandards entlang der gesamten Verarbeitungskette tragen. Eine enge Zusammenarbeit mit den direkten Auftragsverarbeitern sowie eine sorgfältige Vertragsgestaltung sind ausschlaggebend für eine Reduzierung der rechtlichen und operative Risiken.

BGH zu Facebook-Datenleck

Nach einem Datenleck bei Facebook haben die Nutzer allein aufgrund des Kontrollverlustes über die eigenen Daten einen Anspruch auf Schadensersatz. In seiner ersten Grundsatzentscheidung stellte dies der Bundesgerichtshof (BGH) heraus. Er schaffte damit Klarheit für tausende ähnliche Fälle im sog. Scraping-Komplex. Wegen mangelhafter Datenschutzvorkehrungen von Facebook waren zwischen Mai 2018 und September 2019 die Daten von weltweit rund 533 Millionen Facebook-Nutzern veröffentlicht worden. Laut BGH stellt bereits der kurzzeitige Kontrollverlust über die eigenen personenbezogenen Daten einen immateriellen Schaden im Sinne von Art. 82 DSGVO dar. Der Betroffene habe nur noch nachzuweisen, dass er Opfer eines Datendiebstahls war, nicht jedoch einen Missbrauch der Daten oder andere Beeinträchtigungen. Die Höhe des Schadensersatzes bei bloßem Kontrollverlust sei aber nicht allzu hoch. Der BGH halte dabei eine Summe von 100 Euro für ausreichend, wenn sonst keine Umstände für einen Missbrauch erkennbar seien (BGH vom 18.11.2024).

DSK- Stellungnahme zur Nutzung biometrischer Systeme

Die Datenschutzkonferenz (DSK) hat sich im September 2024 zu einem Gesetzentwurf zur Terrorismusbekämpfung kritisch geäußert, der den Einsatz automatisierter biometrischer Systeme wie Stimm- und Gesichtserkennung vorsieht. Der Entwurf ermöglicht dem BKA, derartige Daten aus öffentlich zugänglichen Quellen auszuwerten. Solche Eingriffe stellen jedoch erhebliche Eingriffe in die Grundrechte der Betroffenen dar. Besonders problematisch sei die anlasslose Erfassung großer Personengruppen im öffentlichen Raum und die heimliche Identifikation von Einzelpersonen. Die Fehleranfälligkeit dieser Systeme und die damit verbundenen Risiken für Betroffene wurden ebenfalls hervorgehoben. Der Einsatz biometrischer Systeme sei nur auf Grundlage verhältnismäßiger Regelungen zulässig. Die rechtliche Anwendung derartiger Technologien sei fragwürdig, der Gesetzgeber habe die Anforderungen aus Verfassungsrecht und KI-Verordnung zu berücksichtigen. Der Einsatz biometrische Systeme benötige einen ausgewogenen und klar regulierten Ansatz zum Schutz der Grundrechte, so der DSK.

Möglicherweise sind dies auch zu beachtende Grundsätze bei der fortschreitenden Technologie der Videoüberwachung.

Stand: 20. Dezember 2024

Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

RA/StB Thomas Hesz; WP/StB Marcel Peetz (M.Acc.); RAin Maria Gayer; Stefan Gräbe
Zertifizierte Datenschutzbeauftragte (TÜV)
Telefon: 09221 / 900 - 0
edsb@frtconsult.de www.frtpartner.de