FIT-Store meets Datenschutz

Die vorliegende Infobroschüre bietet einen Überblick zu den verschiedenen Datenschutzmodellen, die beim Leistungsaustausch nach dem „Einer-für-Alle"-Prinzip (EfA) über den FIT-Store Anwendung finden können. Bei weiteren Fragen kontaktieren Sie uns gerne direkt.

fit-store@fitko.de

Überblick

Mangels einer gesetzlichen Grundlage für eine länderübergreifende Datenverarbeitung wurden unterschiedliche Lösungen entwickelt, um bei länderübergreifenden Online-Diensten eine rechtmäßige Datenverarbeitung zu gewährleisten. Mit der kommenden OZG-Novelle werden diese Lösungen voraussichtlich entbehrlich werden.

Die FITKO verarbeitet in keinem Fall personenbezogene Daten. Sie ist weder verantwortliche Stelle noch Auftragsverarbeiter.

Die von der FITKO empfohlene Lösung setzt auf einen Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO. Es gibt aber auch einen Ansatz der gänzlich ohne den Abschluss eines AVV auskommt, indem gemäß Artt. 4 Nr. 7, 24 DSGVO die datenschutzrechtliche Verantwortlichkeit bei einer zentralen Stelle liegt.

Insbesondere diese beiden Lösungswege können den Angeboten, die über den FIT-Store zur Nachnutzung angeboten werden, zugrunde gelegt werden. Die FIT-Store-Nachnutzungsverträge sind als Software-as-a-Service (SaaS) konzipiert und datenschutzrechtlich neutral.

Auftragsverarbeitungsvertrag (AVV)

Die FITKO ist mit Abschluss der FIT-Store-Verträge datenschutzrechtlich nicht verantwortlich. Als Lösung empfiehlt sie einen Auftragsverarbeitungsvertrag (AVV). Der AVV wird direkt zwischen dem dienstbetreibenden IT-Dienstleister des umsetzenden Landes und der nachnutzenden Behörde geschlossen.

Diese Lösung ist schlank, datensparsam und einfach in Einrichtung und Betrieb. Sie wurde von der Kontaktgruppe der Datenschutzaufsichtsbehörden wohlwollend aufgenommen. Es gibt keine durchgreifenden rechtlichen Bedenken, die gegen dieses Modell sprechen. Es wird bereits von mehreren Ländern genutzt.

Die FITKO erarbeitete in Zusammenarbeit mit der zuständigen Kontaktgruppe der Datenschutzkonferenz einen Muster-AVV. Dieser basiert auf den Standardvertragsklauseln der EU-Kommission. Sinn und Zweck des Muster-AVV ist es, die Vertragsprüfung und das Aushandeln der Vertragsklauseln entbehrlich zu machen.

Der Muster-AVV ist zwischen dem dienstbetreibenden IT-Dienstleister des umsetzenden Landes und jeder nachnutzenden Behörde zu schließen. Aus diesem Grund schlägt die FITKO einen vereinfachten Vertragsschluss (Angebot & Annahme) vor.

Das sogenannte Beitrittsmodell bedeutet:

1. Der IT-Dienstleister verwendet den "FIT-Store Muster-AVV" und konkretisiert diesen für den Onlinedienst einmalig als AVV-Angebot an eine Vielzahl von Behörden.
2. Die nachnutzenden Behörden erklären ihre Annahme in Textform (das bedeutet über eine vollständige Erklärung des Anhang I des Muster-AVV per E-Mail oder, wenn vorhanden, über ein digitales Self-Service-Portal des IT-Dienstleisters).

Der Muster-AVV wurde im Benehmen mit der zuständigen Kontaktgruppe der Datenschutzaufsichtsbehörden entwickelt. Eine formelle Freigabe wurde wegen der begrenzten Ressourcen auf beiden Seiten nicht angestrebt. Es bestand Einigkeit darüber, dass mit dem FIT-Store-Muster-AVV ein gutes Werk für den Leistungsaustausch von EfA-Leistungen über den FIT-Store geschaffen worden ist. Dieser soll ein hohes Datenschutzniveau gewährleisten und dem Zweck der Standardisierung und damit der Arbeitserleichterung einer Vielzahl von Beteiligten (Reduzierung des Prüfungsaufwands) dienen.

Datenschutzrechtliche Verantwortlichkeit des umsetzenden Landes

Die datenschutzrechtliche Verantwortlichkeit wird von dem jeweiligen umsetzenden Land gemäß Artt. 4 Nr. 7, 24 DSGVO einer zentralen Stelle dieses Landes zugewiesen. Die Hamburger EfA-Online-Dienste werden beispielsweise von der Senatskanzlei, Amt für IT und Digitalisierung, über den Auftragsverarbeiter Dataport betrieben. Die Senatskanzlei ist als Betreiberin der Online-Dienste für die Datenverarbeitung im Online-Dienst datenschutzrechtlich ausschließlich verantwortlich im Sinne der Artt. 4 Nr. 7, 24 DSGVO.

Der Online-Dienst ist eine vom Verwaltungsverfahren unabhängige Leistung, die zentral erbracht wird. Nutzende gelangen über eine Suchmaschine oder über einen Link auf dem jeweiligen Landesportal zum gewünschten Online-Dienst. Nach dem Start des Online-Dienstes werden sie bei Nutzung dieser datenschutzrechtlichen Lösung darüber informiert, dass der Dienst von dem jeweils umsetzenden Land betrieben wird und die eingegebenen Daten auf Veranlassung des Nutzenden an die zuständige Behörde weitergeleitet werden. Die für das Verwaltungsverfahren zuständige Behörde weiß bis zur Übergabe der Daten nichts von der Datenverarbeitung im Online-Dienst. Das Verwaltungsverfahren beginnt erst mit dem Erhalt der Daten bei der zuständigen Behörde. Die technischen Dienste des Online-Dienstes und des Verwaltungsverfahrens sind also unabhängig und daher getrennt zu betrachten.

Erst mit der Übergabe der Daten an ein Fachverfahren (z.B. IFAS) über entsprechende Schnittstellen (z.B. XÖV) oder den Abruf der Daten durch die zuständige Behörde (aus der dDatabox) beginnt das Verwaltungsverfahren. Für diese Verwaltungsleistung ist die zuständige Behörde – wie gewohnt – datenschutzrechtlich verantwortlich. Die Verantwortlichkeiten greifen also nacheinander: Zunächst trägt das umsetzende Land die datenschutzrechtliche Verantwortung für den Online-Dienst und mit Übergabe der Daten an die zuständige

Verwaltungsbehörde ist diese wie gewohnt (originär) datenschutzrechtlich verantwortlich. Die EfA-Dienste wurden so konzeptioniert und umgesetzt, dass sie in dieser technisch-organisatorischen wie auch rechtlichen „Unabhängigkeit" vom Verwaltungsverfahren agieren (Beispiel Hamburg: Eingangsseite ist Hamburg-Seite, Datenschutzerklärung klärt über Verarbeitung der Daten als Dienst im EfA-Kontext auf).

Im Ergebnis obliegen alle datenschutzrechtlichen Pflichten der Datenverarbeitung im Online-Dienst der verantwortlichen Behörde, die den Dienst betreibt (= eine zu bestimmende Stelle im umsetzenden Land). Nicht nur die datenschutzrechtliche Dokumentation ist von dieser Stelle erbracht, auch die sog. technisch-organisatorischen Maßnahmen (TOM) wurden festgelegt. Die Betroffenenrechte für die Datenverarbeitung im Online-Dienst werden durch die verantwortliche Stelle gewahrt. Diese Verantwortlichkeit wird transparent durch die Datenschutzerklärung kommuniziert. Ein etwaiger negativer Kompetenzkonflikt ist damit ausgeschlossen. Dies ist ein klarer datenschutzrechtlicher "Gewinn" für die Betroffenen.

Diese Idee von hintereinander und getrennt zu betrachtenden datenschutzrechtlichen Verantwortlichkeiten des Online-Dienstes einerseits sowie des Fachverfahrens andererseits, findet sich auch im Entwurf der OZG–Novelle wieder und ist im Vorfeld offizieller Abstimmungen von Datenschutzseite mit Wohlwollen aufgenommen worden.

Rolle der FITKO

Die FITKO nimmt bei Abschluss der FIT-Store-Verträge keine Position als Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO ein. Sie bezieht Nutzungsrechte an betriebsbereiten EfA-Leistungen und bietet diese zur Nachnutzung an. Die Aufgaben bzw. die Rolle der FITKO ist daher vor allem aus der vergaberechtlichen und weniger aus der datenschutzrechtlichen Seite zu betrachten.

Die FITKO bietet über den FIT-Store einen Online-Dienst zur Nachnutzung an, für den die nachnutzende Stelle auf Basis eines SaaS-Nachnutzungsvertrags die Nutzungsrechte erwerben kann. Dies geschieht im Rahmen einer Interessenbekundung und nach interner Abstimmung mit dem eigentlichen Dienstanbieter.

Die Umsetzung der Verarbeitung personenbezogener Daten basiert auf direkt zwischen dem Dienstanbieter und der nachnutzenden Stelle geschlossenen Auftragsverarbeitungsverträgen gem. Art. 28 DSGVO. Nur der IT-Dienstleister des umsetzenden Landes erhält die Antragsdaten der Bürger:innen, verarbeitet diese und leitet sie der antragsbearbeitenden, nachnutzenden Behörde weiter.

Die FITKO hat keine bestimmende Funktion über die Verfügbarkeit der Leistungsgewährung. Eine Verarbeitung personenbezogenen Daten erfolgt weder durch die FITKO, noch durch die beteiligten Länder. Die FITKO entscheidet weder allein noch gemeinsam über Zweck und Mittel der Datenverarbeitung.

Die FITKO hat über die FIT-Store-SaaS-Verträge keine Einflussmöglichkeit auf die technischen Mittel der Verarbeitung personenbezogener Daten. Die Verträge zwischen der FITKO und den

einstellenden Ländern regeln ausschließlich schuldrechtliche Fragen der Leistungserbringung und definieren Mindeststandards bei Datenschutz und IT-Sicherheit.

Die FIT-Store-SaaS-Einstellungs-AGB sehen hierzu in Ziffer 9.1 die Verpflichtung des umsetzenden Landes vor, die für eine datenschutzrechtliche Prüfung seitens des anschließenden Landes erforderlichen Dokumente und Vorarbeiten (wie etwa Datenschutzkonzepte, Datenschutzfolgenabschätzungen oder Dokumentationen zur Abstimmung mit behördlichen Datenschutzbeauftragten und/oder Datenschutzaufsichtsbehörden) über die FITKO bereitzustellen. Eine eigene Überprüfung durch die FITKO ist jedoch grundsätzlich nicht vorgesehen.

Durch das beschriebene Vorgehen wird auch gewährleistet, dass die beteiligten Länder und die FITKO nicht nur tatsächlich keine Daten verarbeiten, sondern von vornherein keine Rechtsgrundlage für eine Datenverarbeitung haben. Damit wird der Grundsatz der Datensparsamkeit bereits in der Konstruktion verankert und hängt nicht davon ab, wie die Verträge verstanden und gelebt werden.

Auch den Zweck der Datenverarbeitung bestimmt die FITKO nicht, da sich aus den Verträgen keine Zweckfestlegung ergibt. Es werden ausschließlich schuldrechtliche Regelungen zur Nutzung einer technischen Lösung getroffen. Die Zweckbestimmung erfolgt daher allein durch die nachnutzende Behörde.

„Ketten- AVV“

Es gibt Lösungsansätze, bei denen AVV’e entlang der schuldrechtlichen Leistungsbeziehungen geschlossen werden sollen. In einigen Bundesländern sollen die Leistungen von einer zentralen Stelle bezogen und dann von dieser an die Fachbehörden oder Kommunen vermittelt werden. Es ist jedoch nicht zwingend, dass ein AVV den vertraglichen Leistungsbeziehungen folgt. Seitens der Datenschutzaufsichtsbehörden wurde es mitunter kritisch gesehen, dass (Unter-)Auftragsverarbeiter nominell Daten verarbeiten, obwohl sie hierzu weder technisch in der Lage noch rechtlich befugt sind. Die FITKO verhält sich zu dieser Problematik nicht, da sie keine Vereinbarung treffen wird, nach der sie verantwortliche Stelle oder Auftragsverarbeiter werden würde.

****