Landesbeauftragte
für Datenschutz
und Akteneinsicht

Datenschutzrechtliche Hinweise für die Nachnutzung von EfA-Online-Diensten

Stand: April 2023

Impressum

Herausgeberin: Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de
Internet: https://www.LDA.Brandenburg.de

Inhalt

1 Ziele dieses Dokuments

Im Rahmen der Umsetzung des Onlinezugangsgesetzes entwickeln so genannte Themenfeldführer Online-Dienste nach dem „Einer für Alle"-Prinzip (EfA). Eine Stelle / Behörde / Einrichtung, die einen EfA-Online-Dienst (nach-)nutzt, welche personenbezogene Daten verarbeitet, ist aus datenschutzrechtlicher Sicht Verantwortlicher i.S.d. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO). Sie muss gem. Art. 5 Abs. 2 DS-GVO nachweisen können, dass der Einsatz dieses Online-Dienstes datenschutzkonform ist und die Datenschutzgrundsätze gemäß Art 5 Abs. 1 DS-GVO eingehalten werden. Das sollte spätestens vor der Produktivsetzung des Dienstes erfolgen.[1]

Die Informationen in diesem Dokument sollen Verantwortlichen auf Ebene der Landes- und Kommunalverwaltung und weiteren Beteiligten als Hilfestellung und Orientierung dienen. Dabei ist zu beachten, dass die einzelnen datenschutzrechtlich relevanten Punkte je nach Anforderung und konkreter Ausgestaltung des jeweiligen Online-Dienstes auch an anderer Stelle in einer ggf. abweichenden Struktur dokumentiert werden können. So ist es etwa möglich, den datenschutzrechtlichen Anforderungen durch eine Dokumentation in einem einzigen Dokument zu entsprechen oder mehrere Dokumente vorzusehen, die untereinander Verweisungen enthalten. In jedem Fall ist sicherzustellen, dass zumindest die in dieser Orientierungshilfe dargestellten Punkte in der Dokumentation enthalten sind und angemessen behandelt werden.

Die Ausführungen in diesem Dokument erheben keinen Anspruch auf Vollständigkeit. Es bedarf für jeden Online-Dienst einer Einzelfallprüfung, in deren Ergebnis ggf. weitere Unterlagen zu erarbeiten oder inhaltliche Änderungen geboten sind.

2 Zusammenwirken mit dem Themenfeldführer

In der Regel werden große Teile der Dokumentation zum Nachweis der Erfüllung datenschutzrechtlicher Anforderungen bereits vom Themenfeldführer und ggf. dessen Dienstleister(n) erarbeitet und der nachnutzenden Stelle zur Verfügung gestellt. Soweit dies nicht der Fall ist und Unterlagen nicht ausschließlich Besonderheiten des Landesrechts (z.B. aus dem Brandenburgischen Datenschutzgesetz – BbgDSG) oder der nachnutzenden Stelle abbilden, wird empfohlen, vor der eigenen Erstellung eines Nachweises auf den Themenfeldführer zuzugehen und ihn um eine Ergänzung seiner Vorarbeiten und Dokumente zu bitten.

Vom Themenfeldführer zur Verfügung gestellte Unterlagen sind von der nachnutzenden Stelle auf Plausibilität und erforderliche Anpassungen zu prüfen und ggf. fortzuschreiben. Einige Nachweise sind jedoch von der nachnutzenden Stelle selbst zu erstellen (z.B. zur Festlegung lokaler technischer und organisatorischer Maßnahmen). Soweit dies möglich erschien, haben wir diese in den nachfolgenden Punkten kenntlich gemacht. Letztendlich ist der jeweilige datenschutzrechtlich Verantwortliche (hier: die nachnutzende Stelle) für die Einhaltung und den Nachweis der Datenschutzkonformität zuständig.

3 Datenschutzkonzept

3.1 Grundsätzliches

Zum Nachweis der datenschutzkonformen Nutzung eines EfA-Online-Dienstes, der personenbezogene Daten verarbeitet, dient in der Regel ein **Datenschutzkonzept**. Es umfasst alle Aussagen, Beschreibun-

[1] Siehe hierzu auch „Eine datenschutzrechtliche Einordnung von Portallösungen und Fachanwendungen in der OZG-Umsetzung" BMI 15.01.2021 unter https://leitfaden.ozg-umsetzung.de/display/OZG/Arbeitshilfen

gen, Teildokumente usw., die für die Nachweisführung erforderlich sind. Das Datenschutzkonzept bietet sich als das führende Dokument zur datenschutzrechtlichen Dokumentation für den zu betrachtenden Online-Dienst an und kann auf andere Unterlagen verweisen, anstatt diese zu wiederholen.

Das Datenschutzkonzept dokumentiert in aussagekräftiger und stets aktueller Form den Ist-Zustand der Erfüllung der datenschutzrechtlichen Anforderungen durch den Verantwortlichen und ggf. einbezogene Dienstleister (Auftragsverarbeiter) bei der Einführung sowie während der Nutzung des Online-Dienstes. Es ist bei Bedarf fortzuschreiben und anzupassen, z.B. bei Änderungen der Rechtsgrundlagen, der Kategorien verarbeiteter Daten oder betroffener Personen, der technischen Implementierung oder der Risiken für Rechte und Freiheiten von Personen.

Das Datenschutzkonzept soll die Verantwortlichen bei der Erfüllung ihrer **Rechenschaftspflicht** gemäß Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO unterstützen. Es kann gleichzeitig als Arbeitsmittel dienen, eine stetige Verbesserung des Datenschutzniveaus zu erreichen.

3.2 Beschreibung des Online-Dienstes

Zunächst empfiehlt sich, den betreffenden Online-Dienst abstrakt darzustellen. Dies dient zum einen dem grundsätzlichen Verständnis sowie der Nachvollziehbarkeit, bildet aber auch jeweils Rahmen und Anhaltspunkte für die nachfolgenden datenschutzrechtlichen Betrachtungen. Insbesondere soll dadurch deutlich werden, welche spezifischen Punkte in welcher Tiefe aus datenschutzrechtlicher und technischer Sicht nachfolgend zu betrachten sind.

Im Rahmen einer initialen Beschreibung des Online-Dienstes bietet sich eine überblicksartige Darstellung zum Hintergrund und zu den Grundlagen der umgesetzten Verwaltungsleistung an. Die **Zwecke der Verarbeitung** sind zu beschreiben (inklusive der Zweckbestimmung, Zweckabgrenzung sowie bspw. die zur Gewährleistung der Zweckbindung getroffenen Maßnahmen). Durch eine angemessene Dokumentation der Verarbeitungszwecke kann dem Erfordernis des Art. 5 Abs. 1 lit. b DS-GVO nachgekommen werden, wonach personenbezogene Daten ausschließlich für festgelegte, eindeutige und legitime Zwecke verarbeitet werden dürfen. Die Beschreibung soll auch ermöglichen, die für die Erreichung der Zwecke unbedingt erforderlichen Daten zu bestimmen und so dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO zu entsprechen.

Weiterhin empfiehlt es sich, die Verarbeitung der personenbezogenen Daten in verschiedene Verarbeitungstätigkeiten bzw. Verarbeitungsschritte zu unterteilen und diese einzeln zu beschreiben. Den Verarbeitungsschritten sind die jeweils **verarbeiteten Daten und Datenflüsse** sowie die **Beteiligten** (z.B. Antragsteller, Behörden, ggf. Dienstleister etc.) zuzuordnen.

Darüber hinaus ist in der abstrakten Beschreibung des Online-Dienstes auch die verwendete **technische Infrastruktur** im Überblick darzustellen. Hierbei können z.B. wesentliche IT-Systeme wie Server oder Clients, deren örtliche Zuordnungen sowie Verbindungen über Rechnernetze aufgenommen werden. Aus der Darstellung lassen sich oft erste Hinweise zur Festlegung technischer und organisatorischer Maßnahmen ableiten.

Während die Verarbeitungszwecke, die einzelnen Schritte, die Daten und Datenflüsse sowie zentrale technische Komponenten in der Regel vom Themenfeldführer umfassend beschrieben werden, können bei der Darstellung der lokalen technischen Infrastruktur Besonderheiten der jeweiligen Stelle der Landes- oder Kommunalverwaltung zu beachten und zu ergänzen sein.

3.3 Datenschutzrechtliche Verantwortlichkeit und Auftragsbeziehungen

Im Kontext der Nachnutzung von EfA-Online Diensten sind regelmäßig mehrere Stellen in verschiedenen Funktionen beteiligt. Ein entsprechend hoher Stellenwert kommt der Klärung und Abgrenzung der datenschutzrechtlichen Verantwortung nach Art. 4 Nr. 7 DS-GVO sowie der Identifizierung von Auftragsbeziehungen nach Art. 4 Nr. 8 DS-GVO zu.

Datenschutzrechtlich Verantwortlicher ist gem. Art. 4 Nr. 7 DS-GVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über **Mittel und Zwecke der Verarbeitung** personenbezogener Daten entscheidet. Die Beurteilung, wer über die Mittel und Zwecke der Datenverarbeitung bestimmt, orientiert sich dabei an der tatsächlichen Verarbeitung. Bei der Nachnutzung von EfA-Online-Diensten kommt im Ergebnis regelmäßig eine datenschutzrechtliche Verantwortlichkeit einer einzelnen Stelle (zuständige Behörde) oder eine getrennte Verantwortlichkeit mehrerer beteiligter Stellen nacheinander oder eine gemeinsame Verantwortlichkeit mehrerer Stellen nach Art. 26 DS-GVO zum Tragen.[2] Soweit eine getrennte Verarbeitung mehrerer Stellen im Sinne einer sog. „Verarbeitungskette“ vorliegt, sind die getrennten Verantwortlichkeitsbereiche im Datenschutzkonzept darzulegen. Kommt man zu einer gemeinsamen Verantwortlichkeit, so müssen die jeweiligen Einflussmöglichkeiten aller beteiligten Stellen auf die Mittel und Zwecke der Verarbeitung sowie die unterschiedlichen Pflichten zur Erfüllung der datenschutzrechtlichen Anforderungen (z.B. hinsichtlich der Betroffenenrechte) in einer Vereinbarung gemäß Art. 26 Abs. 1 DS-GVO beschrieben werden.

Eng im Zusammenhang mit der Verantwortlichkeit steht auch die Frage der **Auftragsverarbeitung**. Bei einer Auftragsverarbeitung wird ein Dritter (häufig ein IT-Dienstleister) streng weisungsgebunden als Auftragnehmer für den bzw. die Verantwortlichen tätig. Der Auftragsverarbeiter stellt in dieser Konstellation gerade keinen weiteren Verantwortlichen im datenschutzrechtlichen Sinne dar, so dass es keiner separaten Rechtsgrundlage für sein Tätigwerden für im Rahmen des Auftragsverarbeitungsverhältnisses vorgenommene Datenverarbeitungsmaßnahmen bedarf. Er muss aber korrekt und datenschutzkonform über einen **Auftragsverarbeitungsvertrag** (AVV) eingebunden werden. Die in einem AVV zu regelnden Inhalte sind dabei Art. 28 Abs. 3 DS-GVO zu entnehmen. Auf ein Muster eines AVV wird in der Anlage verwiesen. Auch Unterauftragnehmer sind nach den Vorschriften des Art. 28 DS-GVO vertraglich zu binden (in der Regel durch den ersten Auftragnehmer).

Bei der Formulierung des AVV ist auf konkrete Angaben zu Gegenstand und Dauer sowie zu Art und Zweck der Verarbeitung, zu den im Auftrag verarbeiteten Daten und den betroffenen Personen sowie zu den Rechten und Pflichten der Vertragsparteien zu achten. Dies kann auch in einer Anlage zum Vertrag geschehen.

Weiterhin ist eine Verarbeitung im Auftrag des Verantwortlichen nur zulässig, wenn der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass die gesamte Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der Betroffenen gewährleistet. Insofern muss vor der Einführung eines Verfahrens **eine Prüfung der Geeignetheit des Auftragsverarbeiters** erfolgen – diese kann bei EfA-Online-Diensten und zentraler Auftragsverarbeitung auch der Themenfeldführer vornehmen. Ebenso bedeutsam ist die **Kontrolle des Auftragsverarbeiters** durch den Verantwortlichen nach der Verfahrenseinführung. Auf die Erfordernisse des Art. 28 Abs. 3 lit. h DS-GVO wird hingewiesen.

3.4 Zulässigkeit der Verarbeitung

Essenziell ist darüber hinaus auch der **Rechtmäßigkeitsvorbehalt** gemäß Art. 5 Abs. 1 lit. a DS-GVO als weiterer datenschutzrechtlicher Grundsatz. Danach ist eine Verarbeitung personenbezogener Daten

2 Die Verantwortlichkeit kann im Übrigen auch per Gesetz oder Verordnung festgelegt sein. Dies gilt z.B. für die IT-Basiskomponenten nach § 11 BbgEGovG i.V.m. der zugehörigen Rechtsverordnung.

nur zulässig, wenn sie auf eine tragfähige Rechtsgrundlage gestützt werden kann. Eine solche liegt vor, wenn die betroffene Person ausdrücklich in die Verarbeitung ihrer Daten eingewilligt hat oder eine Rechtsvorschrift die Verarbeitung erlaubt. Hieraus folgt das Erfordernis, im Datenschutzkonzept eines EfA-Online-Dienstes die **Rechtsgrundlagen** für die Verarbeitung der personenbezogenen Daten eindeutig zu benennen. Es empfiehlt sich, die jeweiligen Rechtsgrundlagen getrennt nach Datenkategorien sowie Verarbeitungsschritten anzugeben. Sie sind darüber hinaus möglichst genau, d.h. durch Angabe der konkreten Norm in dem Gesetz oder der Verordnung, darzustellen.

Im Zusammenhang mit EfA-Online-Diensten der öffentlichen Verwaltung kommen regelmäßig die Rechtsgrundlagen nach Art. 6 Abs. 1 lit. c und lit. e DS-GVO in Verbindung mit einer konkreten fachgesetzlichen Regelung oder einer datenschutzrechtlichen Auffangvorschrift wie § 5 Abs. 1 BbgDSG in Betracht. Ein Rückgriff auf die Einwilligung der betroffenen Personen nach Art. 6 Abs. 1 lit. a DS-GVO wird insbesondere für Pflichtaufgaben nicht nur nicht empfohlen: Es muss in diesem Fall auch stets mit dem Widerruf der Einwilligung gerechnet werden, wonach die entsprechenden personenbezogenen Daten zu löschen wären.

In der Regel wird der Themenfeldführer die zutreffenden Rechtsgrundlagen für einen EfA-Online-Dienst getrennt nach Verarbeitungsschritten und Datenkategorien dokumentieren (z.B. tabellarisch). Bewährt hat sich auch, in derselben Darstellung die Speicher- bzw. Löschfristen für die personenbezogenen Daten anzugeben und so die Voraussetzungen für die Beachtung des datenschutzrechtlichen Grundsatzes der Speicherbegrenzung aus Art. 5 Abs. 1 lit. e DS-GVO (z.B. durch technische Löschverfahren) zu schaffen. Falls bezüglich der Rechtsgrundlagen oder der Speicherfristen landesrechtliche Besonderheiten zu beachten sind, müssen diese durch die nachnutzende Stelle ergänzt werden.

3.5 Gewährleistung der Rechte betroffener Personen

Die Rechte betroffener Personen, deren personenbezogene Daten in einem EfA-Online-Dienst verarbeitet werden, sind in Art. 12 bis 22 DS-GVO festgelegt. Mögliche Ausnahmeregelungen, z.B. in §§ 10 ff. BbgDSG, sind zu beachten.

Die Gewährleistung der Betroffenenrechte erfordert von dem Verantwortlichen zunächst die Erfüllung der **Informationspflichten** nach Art. 13, 14 DS-GVO. Diese sollen der betroffenen Person ermöglichen, u.a. die jeweils verarbeiteten personenbezogenen Daten, die Verarbeitungszwecke, die Rechtsgrundlagen, die datenschutzrechtlich zuständigen Verantwortlichen, mögliche Datenempfänger bzw. Datenquellen sowie Speicherfristen zu kennen. Die Informationen dienen der Herstellung der Transparenz der Datenverarbeitung im Sinne des Datenschutzgrundsatzes aus Art. 5 Abs. 1 lit. a DS-GVO. In der Regel wird ein Themenfeldführer für den von ihm entwickelten EfA-Online-Dienst die Informationen nach Art. 13, 14 DS-GVO als Muster bereitstellen. Die nachnutzende Stelle hat zu prüfen, ob Anpassungsbedarf besteht, und das Dokument ggf. fortzuschreiben. Dies kann z.B. die Angaben zum Verantwortlichen, zu Datenempfängern oder zu Speicherfristen betreffen. Der Anlage ist ein Verweis auf ein Muster zur Erfüllung der genannten Informationspflichten zu entnehmen.

Weitere wesentliche Rechte betroffener Personen sind die **Rechte auf Auskunft** (Art. 15 DS-GVO), auf **Berichtigung** (Art. 16 DS-GVO), auf **Löschung** (Art. 17 DS-GVO), auf **Einschränkung der Verarbeitung** (Art. 18 DS-GVO), auf **Datenübertragbarkeit** (Art 20 DS-GVO) und auf **Widerspruch** (Art. 21 DS-GVO). Verantwortliche sind verpflichtet, betroffenen Personen diese Rechte zu gewähren, sie hierbei ggf. zu unterstützen und gesetzliche Fristen (in der Regel ein Monat, s. Art. 12 Abs. 3 DS-GVO) einzuhalten. Dies erfordert, innerhalb der Behörde entsprechende Prozesse vorzusehen (z.B. zur Prüfung der Anspruchsvoraussetzungen, Beteiligung von Organisationseinheiten, Beratung durch den bzw. die Datenschutzbeauftragte, Einbeziehung der Leitung). Die Prozesse sollten dokumentiert und die Einhaltung kontrolliert werden. Es liegt in der Natur der Sache, dass Themenfeldführer für EfA-Online-Dienste in

diesen Punkten nur wenig Unterstützung leisten können und die Aufgaben in der Regel durch die nachnutzenden Stellen in eigener Verantwortung zu erfüllen sind.

3.6 Ermittlung von Risiken und Schutzbedarf

Zur Bestimmung geeigneter und angemessener technischer und organisatorischer Maßnahmen gemäß Art. 24, 25 und 32 DS-GVO ist zunächst eine Ermittlung und Bewertung der Risiken für Rechte und Freiheiten der betroffenen Personen vorzunehmen. In diesem Kontext wird häufig auch der Begriff Schutzbedarfsfeststellung genutzt.

Ein **Risiko** kann durch ein Ereignis entstehen, dass selbst einen Schaden für betroffene Personen darstellt oder zu einem solchen Schaden führen kann. Hierbei sind die Schwere des Schadens und die Eintrittswahrscheinlichkeit des Ereignisses von Bedeutung. Im Allgemeinen sind für die Bestimmung der Risiken systematisch mögliche Schäden (z.B. Diskriminierung, finanzielle Verluste, gesellschaftliche Nachteile, Hinderung an der Ausübung von Rechten), deren auslösende Ereignisse (z.B. unbefugte Offenlegung oder Änderung von Daten, Verlust von Daten, unberechtigte Profilbildung, zweckfremde Datenverarbeitung) sowie Risikoquellen (z.B. Hacker, Verantwortlicher, Beschäftigte, höhere Gewalt) zu ermitteln. Durch eine Abschätzung der möglichen Schadenshöhe und der Eintrittswahrscheinlichkeit für jedes Schadensszenario erfolgt anschließend eine **Klassifizierung der Risiken** z.B. in die Stufen gering, normal, hoch. Das Gesamtrisiko einer Verarbeitung bestimmt sich nach dem höchsten Teilrisiko.

Aus dem Risiko, das von einer Verarbeitung personenbezogener Daten ausgeht, ergibt sich der **Schutzbedarf** für die betroffenen Personen. Geringe und normale Risiken resultieren in einem normalen Schutzbedarf, hohe Risiken in einem hohen Schutzbedarf. In der Praxis und aus Sicht der Informationssicherheit hat sich seit vielen Jahren bewährt, den Schutzbedarf hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit anhand der Sensibilität der verarbeiteten Daten und der Verarbeitungsprozesse zu betrachten. Die Sicht des Datenschutzes stellt die betroffenen Personen in den Fokus und ergänzt spezifische Schutzziele wie etwa die Transparenz der Verarbeitung, die Ausübung von Betroffenenrechten oder die strenge Zweckbindung. Die Ergebnisse der Beurteilung können deshalb von den rein informationssicherheitsbezogenen Resultaten abweichen.

Die Ermittlung der Risiken und des Schutzbedarfs wird bei EfA-Online-Diensten in der Regel durch den Themenfeldführer durchgeführt. Eine nachnutzende Stelle sollte ergänzend immer prüfen, ob durch lokale Besonderheiten Beurteilungen anders ausfallen oder zusätzliche Risiken entstehen.

3.7 Schwellwertanalyse und Datenschutz-Folgenabschätzung

Im Rahmen der **Schwellwertanalyse** ist zu prüfen, ob von der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen ausgeht und deshalb eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich ist. Wichtige Anhaltspunkte sind neben dem Text von Art. 35 Abs. 1 und 3 DS-GVO die entsprechenden Kriterien des Europäischen Datenschutzausschusses[3], die Positiv-Listen der Datenschutzaufsichtsbehörden nach Art. 35 Abs. 4 DS-GVO[4] sowie die Ergebnisse der Ermittlung und Bewertung der Risiken (s.o. Abschnitt 3.6).

3 Leitlinien zur Datenschutz-Folgenabschätzung des Europäischen Datenschutzausschusses (WP 248 rev.01), https://ec.europa.eu/newsroom/article29/items/611236

4 Listen von Verarbeitungstätigkeiten nach Art 35 Abs. 4 DS-GVO der LDA Brandenburg, https://www.lda.brandenburg.de/lda/de/datenschutz/auslegungshilfen-der-landesbeauftragten/

Ziel einer **Datenschutz-Folgenabschätzung** (DSFA) ist es letztlich, die identifizierten Risiken durch geeignete und angemessene technische und organisatorische Maßnahmen auf ein vertretbares Maß abzusenken. Gemäß Art. 35 Abs. 7 DS-GVO sind im Rahmen einer DSFA die geplanten Verarbeitungsvorgänge und der Zweck der Verarbeitung systematisch zu beschreiben, die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug zum Zweck sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen darzustellen.

Es ist zu erwarten, dass Themenfeldführer auch die Schwellwertanalyse und ggf. die Datenschutz-Folgenabschätzung für einen EfA-Online-Dienst durchführen und beides den nachnutzenden Stellen zur Verfügung stellen. Diese müssen ihrerseits prüfen, ob sie die Einschätzungen in den Unterlagen teilen und ob durch lokale Besonderheiten wie spezifische landesrechtliche Regelungen oder individuelle technische Gegebenheiten eine Anpassung und Fortschreibung erforderlich ist.

3.8 Technische und organisatorische Maßnahmen, Sicherheitskonzept

Um die Einhaltung der Datenschutzanforderungen bei der Verarbeitung sicherzustellen und dies nachweisen zu können, sind anschließend gemäß Art. 24, 25 und 32 DS-GVO die **technischen und organisatorischen Maßnahmen** einschließlich ihrer Umsetzung zu dokumentieren. Adressaten der genannten Normen sind sowohl der datenschutzrechtlich Verantwortliche als auch beteiligte Auftragsverarbeiter. Diese sind u.a. verpflichtet, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste zu gewährleisten. Sie müssen bei der Festlegung und Umsetzung der Sicherheitsmaßnahmen z.B. die Art und den Umfang, die Umstände und Zwecke der Datenverarbeitung, die Risiken für die Rechte und Freiheiten der betroffenen Personen sowie den Stand der Technik berücksichtigen. Nach § 4 Abs. 1 Nr. 2 BbgDSG sind die Maßnahmen in einem Sicherheitskonzept darzustellen.

Die Art und Weise der Dokumentation kann sehr unterschiedlich sein: Für manche Verarbeitungen wird ein einziges, einheitliches Sicherheitskonzept erarbeitet, meist findet man in der Praxis jedoch eine Reihe von separaten Teilkonzepten, auf die aus einem Rahmendokument verwiesen wird. Besonders wichtig sind in diesem Zusammenhang Konzepte z.B. zu Rollen und Berechtigungen, zu kryptografischen Verfahren, zur Datensicherung, zur Protokollierung, zur Änderung und zur Löschung von Daten. Die technischen Konzepte werden ergänzt durch organisatorische Festlegungen, häufig in Form von Dienstanweisungen und ggf. Dienstvereinbarungen. Wichtig ist, dass alle Maßnahmen regelmäßig und anlassbezogen überprüft, bewertet und hinsichtlich ihrer Wirksamkeit evaluiert werden (vgl. Art. 32 Abs. 1 lit d DS-GVO). Auch hierfür sollte es entsprechende Konzepte geben.

Wesentliche Festlegungen zu technischen und organisatorischen Maßnahmen werden in der Regel vom Themenfeldführer eines EfA-Online-Dienstes getroffen. Falls eine Verarbeitung durch einen externen Auftragsverarbeiter erfolgt, muss dieser die Umsetzung der Maßnahmen gewährleisten und die Verpflichtung ggf. auch auf seine Unterauftragnehmer übertragen. Der Abschluss eines bzw. mehrerer Verträge zur Auftragsverarbeitung gemäß Art. 28 DS-GVO ist in diesem Fall erforderlich.

Allerdings ist darauf hinzuweisen, dass häufig weitere technische und organisatorische Maßnahmen in der Verantwortungssphäre der nachnutzenden Stelle umzusetzen sind. Diese können sich z.B. auf lokale Netz- oder Clientkomponenten beziehen, die zentral bereitgestellte Serverdienste nutzen. Auf Sicherheitsmaßnahmen für diese lokalen Komponenten hat der Themenfeldführer keinen Einfluss. Gleiches gilt für lokale organisatorische Festlegungen etwa zu Zuständigkeiten oder zur Vergabe von Rollen und Berechtigungen. Ebenso wird zu erwarten sein, dass entsprechend den örtlichen Gegebenheiten Regelungen zur Gewährleistung der Betroffenenrechte (z.B. auf Auskunft oder Berichtigung) oder zur Erfüllung der Pflichten bei Datenschutzverletzungen (z.B. Meldung an Aufsichtsbehörde, Information betroffener Personen) zu treffen sind. Insofern muss eine nachnutzende Stelle immer prüfen, welche er-

gänzenden technischen und organisatorischen Maßnahmen sie zusätzlich zu den im Sicherheitskonzept des Themenfeldführers dokumentierten Maßnahmen lokal festzulegen und umzusetzen hat.

3.9 Verzeichnis von Verarbeitungstätigkeiten und datenschutzrechtliche Freigabe

Gemäß Art. 30 DS-GVO ist der Verantwortliche verpflichtet, ein **Verzeichnis von Verarbeitungsverzeichnissen** (VVT) zu führen. In diesem sind alle Verarbeitungstätigkeiten nach festgelegten Kriterien zu beschreiben – also auch EfA-Online-Dienste. Die Mindestanforderungen der Beschreibung ergeben sich aus Art. 30 Abs. 1 DS-GVO.

In der Regel haben Behörden eine Mustervorlage für das VVT. Auch in der Anlage wird auf ein solches Muster verwiesen. Eine nachnutzende Stelle kann diese Mustervorlage verwenden, um Angaben zu dem jeweiligen EfA-Online-Dienst, die sie vom Themenfeldführer erhält, dort nach den lokalen Vorgaben für das eigene VVT einzutragen. Alternativ kann sie den vom Themenfeldführer in der Regel bereitgestellten Eintrag für das VVT direkt dem eigenen Verzeichnis hinzufügen. In jedem Fall sind erforderliche Anpassungen vorzunehmen, etwa zum Verantwortlichen und zum lokalen Datenschutzbeauftragten.

Neben den bisher dargestellten datenschutzrechtlichen Anforderungen insbesondere aus der Datenschutz-Grundverordnung sind auch **landesspezifische Besonderheiten** z.B. nach dem Brandenburgischen Datenschutzgesetz zu beachten. Sie konkretisieren die vorgenannten Rechenschaftspflichten. Insbesondere muss an die in § 4 Abs. 1 BbgDSG geregelte Notwendigkeit einer **schriftlichen Freigabe** durch den Verantwortlichen (z.B. Leiter der Behörde) vor Produktivsetzung des EfA-Online-Dienstes oder bei wesentlichen Änderungen gedacht werden. Die Freigabeerklärung ist dem VVT beizufügen. Auf ein entsprechendes Muster wird in der Anlage verwiesen. Die Erfüllung dieser landesspezifischen Anforderung kann nur durch die nachnutzende Stelle erfolgen und wird entsprechend nicht vom Themenfeldführer berücksichtigt.

4 Anlagen

Im Folgenden werden einige Verweise auf Veröffentlichungen im Internet zur Unterstützung der Nachnutzung von EfA-Online-Diensten zusammengestellt. Insbesondere wurden Unterlagen aufgenommen, die als Muster dienen können.

zu 3.3 – Datenschutzrechtliche Verantwortlichkeit und Auftragsbeziehungen

- LDA Brandenburg: Formulierungshilfe für einen Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO, https://www.lda.brandenburg.de → Datenschutz → Auslegungshilfen der Landesbeauftragten → Auftragsverarbeitung
- Ministerium des Innern und für Kommunales des Landes Brandenburg: Muster für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO, https://mik.brandenburg.de → Ministerium → Akteneinsicht und Datenschutz → EU-Datenschutz-Grundverordnung Anwendungshinweise → Anlage 8

zu 3.5 – Gewährleistung der Rechte betroffener Personen

- Ministerium des Innern und für Kommunales des Landes Brandenburg: Muster zur Erfüllung der Informationspflichten nach Art. 13 und 14 DS-GVO, https://mik.brandenburg.de → Ministerium → Akteneinsicht und Datenschutz → EU-Datenschutz-Grundverordnung Anwendungshinweise → Anlage 7a und 7b

zu 3.7 – Schwellwertanalyse und Datenschutz-Folgenabschätzung

- Datenschutzkonferenz: Kurzpapiere Nr. 5 (Datenschutz-Folgenabschätzung) und Nr. 18 (Risiken für die Rechte und Freiheiten natürlicher Personen), https://www.datenschutzkonferenz-online.de → Kurzpapiere
- LDA Brandenburg: Listen von Verarbeitungsvorgängen, für die eine DSFA erforderlich ist, https://www.lda.brandenburg.de → Datenschutz → Auslegungshilfen der Landesbeauftragten → Datenschutz-Folgenabschätzung

zu 3.9 – Verzeichnis von Verarbeitungstätigkeiten und datenschutzrechtliche Freigabe

- Datenschutzkonferenz: Muster für Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs.1 DS-GVO und Hinweise, https://datenschutzkonferenz-online.de → Anwendungshinweise → 2018 → Hinweise zum Verzeichnis der Verarbeitungstätigkeiten, Muster für Verantwortliche
- Ministerium des Innern und für Kommunales des Landes Brandenburg: Muster für eine Freigabe-erklärung nach § 4 Abs. 1 BbgDSG, https://mik.brandenburg.de → Ministerium → Akteneinsicht und Datenschutz → EU-Datenschutz-Grundverordnung Anwendungshinweise → Anlage 5