Bundesministerium
des Innern
und für Heimat

Lernpfad

Datenschutz in der öffentlichen Verwaltung

Fortbildungsangebot der BAköV mit Zertifikat
unter Mitwirkung des Bundesbeauftragten für den
Datenschutz und die Informationsfreiheit

Brühl / Rheinland Dezember 2021
Version 1.0

Dieser Lernpfad wurde von der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat (BAköV) erstellt. Er ersetzt den bis 2021 verwendeten Leitfaden „Datenschutz in der öffentlichen Verwaltung“. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat am Lernpfad mitgewirkt. Die Inhalte dieses Lernpfads dürfen ausschließlich in Absprache mit der BAköV verwendet werden.

Herausgeber:

Bundesakademie für öffentliche Verwaltung
im Bundesministerium des Innern und für Bau
Willy-Brandt-Str. 1
50321 Brühl

Telefon: 0228 / 99 629-0
02232 / 929-0

E-Mail: poststelle@bakoev.bund.de

Internet: https://www.bakoev.bund.de
https://www.ifosbund.de
https://lernplattform.intranet.bund.de
https://digitalakademie.bund.de

Inhaltsverzeichnis

1 Warum eine systematische Qualifizierung im Datenschutz wichtig ist und wie Sie Ihren eigenen Lernpfad finden

Mit dem Wirksamwerden der EU-Datenschutzgrundverordnung (EU-DSGVO) am 25. Mai 2018 hat der behördliche Datenschutz einen enormen Impuls bekommen. Dieser Impuls geht allerdings mit steigenden Praxisanforderungen einher. Die Komplexität im Datenschutz ist nicht zuletzt durch die voranschreitende behördliche Digitalisierung gestiegen. Denn in den meisten Fällen werden bei Digitalisierungsmaßnahmen personenbezogene Daten verarbeitet, was eine datenschutzrechtliche Bewertung erfordert. Ohne systematische Qualifizierung, die auch die Besonderheiten in der öffentlichen Verwaltung im Blick hat, ist es schwer, diesen Herausforderungen zu begegnen.

Um die oft komplexen Fragen angemessen beantworten zu können, sind neben juristischen verstärkt auch technische Kenntnisse erforderlich. Hinzu kommen Managementkompetenzen und zahlreiche Berührungen zu angrenzenden Fachgebieten wie der Informationssicherheit. Das Anforderungsprofil im Datenschutz ist damit genauso komplex wie der Datenschutz selbst.

Die im behördlichen Datenschutz beschäftigten Kolleginnen und Kollegen - zum Beispiel als Datenschutzbeauftragte - weisen in der Regel sehr unterschiedliche Qualifikationen vor. Volljuristinnen und Volljuristen sowie Verwaltungswirtinnen und Verwaltungswirte sind ebenso vertreten wie Beschäftigte mit informationstechnischen Hintergründen. Nicht selten fehlt den Juristinnen und Juristen oder den Verwaltungswirtinnen und Verwaltungswirten das technische Know-How. IT-Beschäftigten fehlen hingegen oft die rechtlichen Aspekte des Datenschutzes. Andere Beschäftigte kommen aus Disziplinen wie den Wirtschaftswissenschaften oder den Sozialwissenschaften. Einige haben einen ausgeprägten Verwaltungsbezug, öfter aber auch Erfahrungen aus der Privatwirtschaft. Es gibt Beschäftigte mit langjähriger Erfahrung in der Bundesverwaltung, aber außerhalb des behördlichen Datenschutzes. Demgegenüber haben neue Beschäftigte in der Bundesverwaltung hin und wieder bereits wichtige Datenschutzerfahrungen in der Privatwirtschaft sammeln können. Die Qualifikationslage im behördlichen Datenschutz ist damit sehr heterogen und es gilt, Standardkompetenzen zu vermitteln, damit der behördliche Datenschutz in der Bundesverwaltung ein möglichst einheitlich hohes Niveau erreichen kann.

Um diesem Auftrag gerecht zu werden, hat die Bundesakademie unter Mitwirkung von Kolleginnen und Kollegen des Bundesbeauftragten für

den Datenschutz und die Informationsfreiheit im Jahr 2021 einen praxis- und bedarfsorientierten **Lernpfad für Datenschutz in der öffentlichen Verwaltung** entwickelt. Der Lernpfadentwicklung ging mit einer Modernisierung des Fortbildungsangebots der BAköV einher, die die Aspekte Hybridisierung der Lernformate, Digitalisierung, Modularisierung, Nachhaltigkeit und Flexibilisierung zum Gegenstand hatte. Auf Basis moderner methodisch-didaktischer Erkenntnisse und unter Berücksichtigung digitaler Lernformate haben wir ein Gesamtkonzept entwickelt, das in seinen jeweiligen modularen Bausteinen eine nachhaltige Maximierung des Lernerfolgs verspricht. Dabei berücksichtigen wir die äußerst heterogenen Ausgangslagen in puncto individueller Qualifikation und individueller Fortbildungsbedarf. Dies ermöglicht je nach persönlicher Situation einen individuellen Einstieg in den Lernpfad und damit eine eigene „Lernreise“ durch den Datenschutz.

Für alle Ebenen sehen wir Angebote vor: Für Einsteigende, Erfahrene und Fortgeschrittene. Die Nachhaltigkeit des Lernerfolgs gewährleisten wir durch verschiedene Angebote zur Vertiefung und zum Erfahrungsaustausch, aber nicht zuletzt durch unsere Zertifikate „Datenschutzbeauftragte in der öffentlichen Verwaltung“ und „Operativer Datenschutz in der öffentlichen Verwaltung“.

Jede Beschäftigte und jeder Beschäftigte kann quasi so lange auf ihrem bzw. seinen Lernpfad unterwegs sein, wie es der jeweilige Fortbildungsbedarf erfordert. Die digitalen Formate ermöglichen uns zudem, Kolleginnen und Kollegen zu adressieren, denen z.B. aus Gründen familiärer Verpflichtungen eine Präsenzveranstaltung in der Vergangenheit nicht möglich war. Wo aus methodischen und didaktischen Gründen der Mehrwert von Präsenzen indes größer ist, haben wir diesen Aspekt beispielsweise in Erfahrungsaustauschen gestärkt. So konnten wir einen Lernpfad entwickeln, auf dem für jede und jeden etwas dabei ist.

Für dieses Angebot haben wir neben unserer langjährigen Fortbildungserfahrungen im Bereich des Datenschutzes auch Anregungen aus dem Kreis der Teilnehmenden unserer Veranstaltungen berücksichtigt. Allen, die insofern mitgewirkt haben, - allen voran den Kolleginnen und Kollegen aus dem BfDI - möchten wir an dieser Stelle herzlich danken. Denn Fortbildung ist keine Einbahnstraße. Sie lebt vom gemeinsamen Erfahrungsaustausch und kann sich so stetig weiterentwickeln, genauso wie wir gemeinsam den hier vorliegenden Lernpfad stetig weiterentwickeln werden. Wir freuen uns, Sie damit auf ihrem individuellen „Datenschutzweg“ begleiten zu können. Gerne beraten wir Sie, um den für Sie richtigen Weg durch den Datenschutz zu finden. Sprechen Sie uns einfach an!

Die jeweils aktuelle Version des Lernpfads ist unter www.bakoev.bund.de veröffentlicht.

Wir wünschen Ihnen viel Freude auf Ihrem Lernpfad.

Ihre Lehrgruppe 5

2 Ziele

Anliegen dieses Lernpfades ist es, Beschäftigte der Bundesverwaltung:

- in den relevanten Bereichen des Datenschutzes nachhaltig zu sensibilisieren und fortzubilden;
- für die Tätigkeiten als Datenschutzbeauftragte oder im Bereich des operativen Datenschutzes in der öffentlichen Verwaltung zu befähigen, zu zertifizieren und permanent fortzubilden.

Das Fortbildungsangebot richtet sich in erster Linie an Beschäftigte der Bundesverwaltung.

3 Anforderungsprofile

Die Anforderungsprofile für die öffentliche Verwaltung sind je nach Tätigkeit unterschiedlich und können spezifische Ausprägungen haben. Dies berücksichtigend basiert der Lernpfad auf folgendem gestuften Anforderungskonzept:

3.1 Einstieg: Basiskompetenzen (Basissensibilisierung)

Alle Bundesbeschäftigen müssen grundsätzlich über allgemeine Basiskompetenzen verfügen, um in Zusammenhängen des Datenschutzes möglichst souverän agieren zu können. Dies umfasst im Wesentlichen folgende Aspekte:

- Erkennen personenbezogener Daten.
- Kenntnis der allgemeinen Rechtsgrundlagen der EU-DSGVO und des BDSG und deren Praxisbezug.
- Bedeutung der Datensicherheit.
- Erkennen von potentiellen Risiken.
- Rollenverständnis zu Datenschutzbeauftragten, Verantwortlichkeit und Auftragsverarbeitung.
- Rechte betroffener Personen.
- Kennen von geeigneten Maßnahmen technischer und organisatorischer zum Schutz personenbezogener Daten.
- Grundkenntnisse über Meldeprozesse.

3.2 Nächster Schritt: Vertiefung und Aufbaukompetenzen

Je nach behördlicher Funktion sind (u.a. für Führungskräfte) vertiefende oder aufbauende Kompetenzen erforderlich, um das behördliche Datenschutzniveau zu steigern. Hierzu zählen im Wesentlichen:

- Ausgeprägtere Kenntnis der wesentlichen Rechtsgrundlagen.
- Kennen wichtiger technischer und organisatorischer Datensicherheitsmaßnahmen.
- Kenntnis und Anwenden der datenschutzrechtlichen Risikobewertung.
- Ausgeprägtere Kenntnis von Auftragsverarbeitungen und Verantwortlichkeiten
- Kenntnis und Anwenden des Verzeichnisses von Verarbeitungstätigkeiten;
- Grundkenntnisse Datenschutzfolgenabschätzung.
- Kenntnis und Anwendung von Meldeprozessen.

3.3 Spezialkompetenzen

Einige Bundesbeschäftige müssen über vertiefte Spezialkompetenzen verfügen, um in komplexen Zusammenhängen des Datenschutzes, souverän agieren zu können, u.a.

- Personalbeschäftigte
- Personalvertretungen
- Beschaffungsstellen
- Organisation
- Innerer Dienst
- IT-Beschäftigte
- Digitalisierungsbeauftragte
- IT-Sicherheitsbeauftragte
- Sicherheits-, Strafverfolgungs- und OWiG-Beschäftigte

3.4 Datenschutzbeauftragte

Die EU-DSGVO fordert von Datenschutzbeauftragten ein hohes Maß an Fachwissen und Management-/Kommunikationskompetenz. Dies betrifft alle Bereiche des behördlichen Datenschutzes, damit Datenschutzbeauftragte ihren Beratungs- und Überwachungsaufgaben nach der EU-DSGVO entsprechen können. Die Kompetenzanforderungen erreichen hier ein sehr hohes Niveau, dass auch Spezialwissen umfasst.

3.5 Operativer Datenschutz

Ebenfalls hohe Anforderungen in puncto Fachwissen und Managementkompetenz sind an Beschäftigte des operativen Datenschutzes gestellt. Sie haben alle behördlichen Datenschutzanforderungen – wenngleich sie nicht für alles verantwortlich sind - aus Sicht der verantwortlichen Stelle im Blick und sind damit ein wesentlicher Baustein des behördlichen

Datenschutzmanagements. Die Kompetenzanforderungen erreichen hier ebenfalls ein sehr hohes Niveau, dass auch Spezialwissen umfasst.

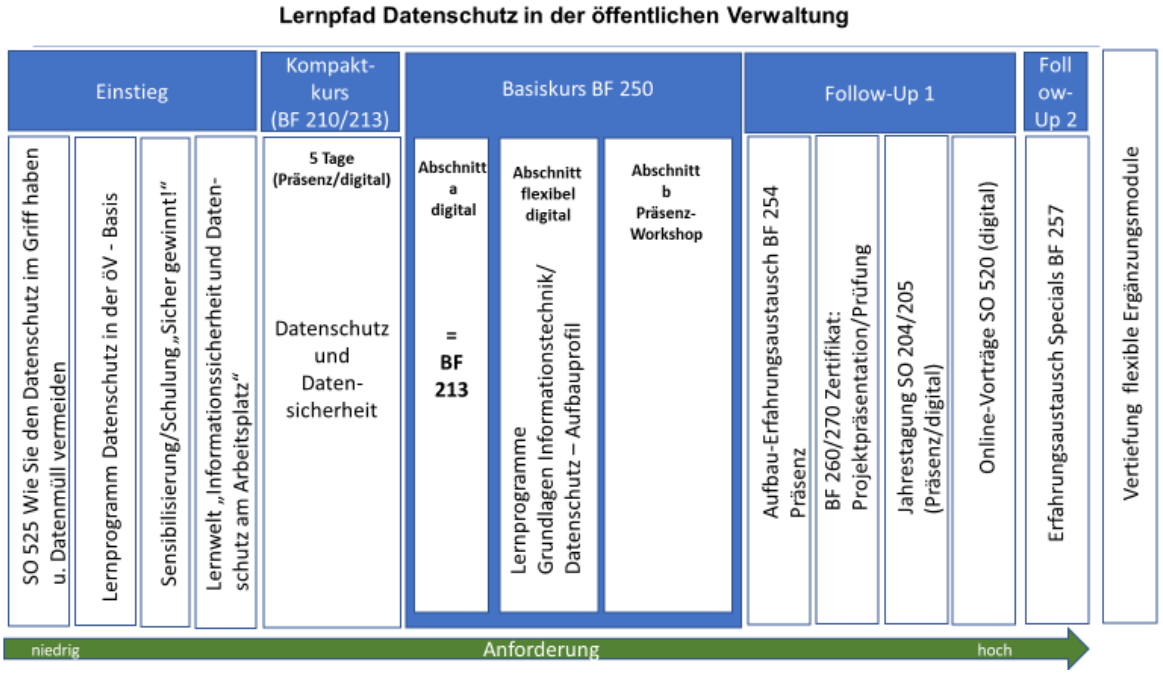
Diese Anforderungsprofile findet ihren Niederschlag im Angebot der BAköV.

4 Überblick zum Lernpfad

Dieser Lernpfad geht davon aus, dass die Aufgaben mit Datenschutzbezug innerhalb der öffentlichen Verwaltung vielfältig sind und das Tätigkeiten laufbahnübergreifend wahrgenommen wird. Ebenfalls wird berücksichtigt, dass hinsichtlich des Wissensstandes, des Aufgabenfeldes bzw. zukünftigen Einsatzgebietes sowie der Erfahrungen, unterschiedliche Voraussetzungen eingebracht werden. Die Gestaltung der Fortbildung muss deshalb flexibel sein und den individuellen Vorkenntnissen, Berufserfahrungen und Aufgabenfeldern Rechnung tragen. Daher ist das Fortbildungsangebot modular und flexibel aufgebaut. Wir ermöglichen Ihnen damit das Erstellen eines individuellen Lernpfads (Auswahl der zu besuchenden Veranstaltungen).

Für die Entscheidung über den individuellen Fortbildungsweg besteht die Möglichkeit, sich von der BAköV in einem Interview beraten zu lassen. Die BAköV stellt auch einen Selbsteinschätzungstest im Fortbildungsportal des Bundes zur Verfügung.

Eine Gesamtübersicht zum Lernpfad können Sie der nachstehenden Übersicht entnehmen:



Beschreibung:
Die Abbildung zeigt, dass Sie je nach eigener Qualifikation auf allen Anforderungsebenen flexibel einsteigen können. Niemand „muss“ alle Ebenen absolvieren. Weitere Informationen zu den JAP-Nummern (z.B. BF 250) finden Sie in IFOS Bund (www.ifosbund.de). Nachstehend erläutern wir Ihnen die verschiedenen Ebenen des Lernpfads:

4.1 Einstieg Basisfortbildung

Zum Einstieg in das Thema „Datenschutz in der öffentlichen Verwaltung“ und zu Erlangung erster Basiskenntnisse empfehlen wir neben dem Basis-Lernprogramm im Fortbildungsportal des Bundes, zu dem auch ein Abschlusstest verfügbar ist, den Besuch des Kurses SO 525, indem Sie auch lernen, dass Datenschutz nachhaltig sein kann und sollte. Beide Elemente haben das Ziel, erste Grundlagen für die praxiskonforme Anwendung des Datenschutzes zu entwickeln.
Zudem bieten wir Ihnen zum Einstieg neben der Lernwelt „Informationssicherheit und Datenschutz am Arbeitsplatz“ (IDAP) im Fortbildungsportal des Bundes Seminare und Webinare aus dem Rahmenvertrag „Sicher gewinnt!“ an. Alle Einstiegs-Elemente haben das Ziel, erste Grundlagen für die praxiskonforme Anwendung des Datenschutzes zu entwickeln. Die Inhalte können zielgruppenspezifisch adressiert werden (u.a. IT-Beschäftigte, Führungskräfte).

1	Lernprogram Datenschutz in der öffentlichen Verwaltung - Basis	**Online**	**120 Min**
2	SO 525: Wie Sie den Datenschutz im Griff haben und Datenmüll vermeiden Kurs für Einsteigende zur Basissensibilisierung	**Online**	**2 Tage**
3	Lernwelt „Informationssicherheit und Datenschutz am Arbeitsplatz“	**Online**	**120 Min**
4	Seminare/Webinare der Initiative Sicher gewinnt! zur Basissensibilisierung	**Online**	**180 Min**

4.2 Aufbau und Vertiefung von Grundlagen

Grundkenntnisse können mit dem 5-tägigen Kurs „Datenschutz und Datensicherheit“ - BF 210 (Präsenz) und BF 213 (inhaltsgleich, aber digital) stärker ausgeprägt und vertieft werden. Die inhaltlichen Module können Sie der nachstehenden Übersicht entnehmen.

Modul	Inhalt	Format	Tag
1	Allgemeine Grundlagen: • Grundrechtsdimension des Datenschutzes • Definition: Personenbezogene Daten, besondere Kategorien • Zielsetzung, Anwendungsbereiche und Regelungsgehalte der EU-DSGVO bzw. des BDSG sowie Spezialgesetze • Datenschutzgrundsätze • Verbotsprinzip und Rechtsgrundlagen • Rechtsfolgen von Datenschutzverstößen (inkl. Fehlermanagement) • Anonymisierung/Pseudonymisierung • Zulässigkeit der Datenübermittlung • Abgrenzung des Datenschutzes zur Informationsfreiheit und zur Informationssicherheit • Organisation der Datenschutzkontrolle	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**1**
2	Grundlagen zu Verantwortlichkeiten und Auftragsverarbeitung • Behördliches Datenschutzmanagement • Folgen für die Auftragsverarbeitung	**Online-Vortrag mit Praxisbeispielen und interaktiven Gruppenübungen, Vorstellung im Plenum**	**2**
3	Behördliche Datenschutzbeauftragte • Rechte und Pflichten für behördliche Datenschutzbeauftragte • Aufgaben/Anforderungen an behördliche Datenschutzbeauftragte und Schnittstellen zu anderen Bereichen und Beauftragte	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**2**
4	Rechte für betroffene Personen	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**3**
5	Grundzüge des Beschäftigtendatenschutz, insb. • Rechtsgrundlagen • Personalaktenrecht • Besonderheiten im öffentlichen Dienst • Mitbestimmung • Private Nutzung von Telekommunikationseinrichtungen	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**3**
6	Grundzüge praxisrelevante Themen im Datenschutz, insb. • Verarbeitungsverzeichnis • Datenschutz-Folgenabschätzung • Verzeichnis von Verarbeitungstätigkeiten • Videoüberwachung • Betrieb von Internetseiten • Versand von Newslettern • Grenzüberschreitender Datenverkehr • Schulungs- und Sensibilisierungsmaßnahmen	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen, Übungen mit Vorstellung im Plenum**	**4**

7	Grundlagen Datensicherheit und Informationssicherheit • Überblick über technische und organisatorische Datenschutzmaßnahmen nach der EU-DSGVO und dem BDSG, • Grundzüge des IT-Grundschutzes und des Informationssicherheitsmanagements	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen, Übungen mit Vorstellung im Plenum**	**5**

4.3 Datenschutzbeauftragte und Beschäftigte des operativen Datenschutzes

Für Datenschutzbeauftragte und Beschäftigte des operativen Datenschutzes, die über ein hohes Maß an Datenschutzkenntnis verfügen müssen, bieten wir den Kurs „Datenschutzmanagement in der öffentlichen Verwaltung“ - BF 250 an. Der Titel des Kurses soll keineswegs zum Ausdruck bringen, dass Datenschutzbeauftragte Teil verantwortlicher Stellen sind, wie dies bei Beschäftigten im administrativen/operativen Datenschutz der Fall ist. Allerdings arbeiten beide Zielgruppen in der Praxis sehr eng zusammen und die Beratungs- und Überwachungskompetenz der Datenschutzbeauftragten trägt zu einem hohen Datenschutzniveau im behördlichen Datenschutzmanagement bei. Letztlich geht es bei beiden Zielgruppen auch um die Ausprägung von Managementkompetenzen, was den Titel des Kurses ausmacht. Es hat sich gezeigt, dass ein gemeinsames Lernen dieser beiden Zielgruppen zielführend für die behördliche Zusammenarbeit im Datenschutz ist. Aus diesem Grund adressiert dieser Kurs beide Zielgruppen.

Inhaltlicher Gegenstand des Kurses ist das Handbuch „Datenschutzbeauftragte in der öffentlichen Verwaltung“, dass die BAköV unter Mitwirkung des BfDI seit vielen Jahren anbietet, stetig aktualisiert und den Teilnehmenden zur Verfügung stellt. Die Inhalte des Handbuchs sind Gegenstand der Zertifizierungsprüfung (vgl. Ziff. 6.4). Aus diesem Grund wird der Kurs Zertifikatsinteressierten empfohlen.

Der in seinen Lernformaten „hybride“ BF 250 besteht aus drei Teilen, die flexibel belegt werden können:

- Webinar: Datenschutz und Datensicherheit (=BF 213) – Abschnitt a
- Lernprogramme „Informationstechnik“ und „Datenschutz in der öffentlichen Verwaltung -Aufbau“ (Fortbildungsportal des Bundes) – Flexible unverbindliche Selbstlernphase

a. Datenschutzmanagement in der öffentlichen Verwaltung – Abschnitt b

Die inhaltlichen Module können Sie der nachstehenden Übersicht entnehmen.

4.3.1.1 Webinar: Datenschutz und Datensicherheit (=BF 213) – Abschnitt a

Zur Vermeidung von Wiederholungen an dieser Stelle, schauen Sie sich bitte die Inhalte oben zum BF 210/BF 213 an. Dieser Kurs wird im ersten Abschnitt des BF 250 inhaltsgleich, allerdings im digitalen Format angeboten. Damit möchten wir die Attraktivität des Gesamtkurses steigern. Interessierte Beschäftigte müssen nicht – wie noch vor 2022 – drei komplette Wochen vom Dienstort weg. Das digitale Format erhöht an dieser Stelle die Flexibilität wesentlich.

Der Kurs hat das Ziel Grundlagen zu entwickeln oder vorhandenes Wissen aufzufrischen. Der Kurs bietet sich daher auch für Beschäftigte, die schon vor einigen Jahren mit Datenschutzthemen zu tun hatten, deren Grundkenntnisse aber z.B. nach Rechtsänderungen nicht mehr aktuell sind.

Ziele: Entwicklung von Grundlagen oder Auffrischung vorhandener Kenntnisse

4.3.1.2 Lernprogramme „Informationstechnik“ und „Datenschutz in der öffentlichen Verwaltung - Aufbau“ (Fortbildungsportal des Bundes)

Auch die zweite Woche des BF 250 findet online statt, was die Flexibilität des Gesamtkurses um einen weiteren Baustein erhöht. Interessierte Beschäftigte können in dieser zweiten Woche je nach Lernbedarf zwei Lernprogramme im Fortbildungsportal des Bundes im Rahmen einer freien Selbstlernphase absolvieren. Das Lernprogramm „Informationstechnik“ adressiert Beschäftigte, die bislang über wenig technisches Know-How verfügen. Die Ziele der zweiten Woche sind die Lernvertiefung und Lernergänzung der Grundlagenthemen aus dem ersten Abschnitt. Je nach Bedarf können einzelne Module oder das ganze Programm absolviert werden. Beschäftigten (u.a. aus Ländern und Kommunen), die keinen Zugang zum Fortbildungsportal des Bundes haben, wird das Selbststudium mit dem Handbuch empfohlen. Auch Bundesbeschäftigte können je nach Bedarf hiervon Gebrauch machen. Diese Woche ist allerdings unverbindlich

und kann flexibel zum Selbststudium genutzt werden. Sie kann nicht über IFOS gebucht werden.

Ziele: Vertiefung der Lerninhalte (Empfehlung für behördliche Datenschutzbeauftragte und Beschäftigte im operativen/administrativen Datenschutz, Freiwillig für Beschäftigte mit Datenschutzbezug)

Modul	Inhalt	Format	Tag
1	Lernprogramm Grundlagen Informationstechnik	**Online**	**1**
2	Lernprogramm Datenschutz in der öffentlichen Verwaltung – Aufbaumodul	**Online**	**2**

4.3.2 Datenschutzmanagement in der öffentlichen Verwaltung – Abschnitt b

Der dritte Abschnitt (=Abschnitt b in IFOS) stellt einen wichtigen Praxisbaustein dar. Hier geht es darum, dass Ihre theoretischen Kenntnisse in der behördlichen Praxis angewandt werden. Dieser Abschnitt hat Workshop-Charakter und wendet sich in erster Linie an Datenschutzbeauftragte und Beschäftigte des operativen Datenschutzes, die die Zertifikate „Behördliche Datenschutzbeauftragte in der öffentlichen Verwaltung“ oder „Operativer Datenschutz in der öffentlichen Verwaltung“ anstreben. Aber auch Beschäftigte, die dieses Ziel nicht haben, können sich in diesem Abschnitt den „Praxisschliff“ holen. Die Grundlagenkenntnisse werden in jedem Fall vorausgesetzt, damit – von Ausnahmen abgesehen – die Zeit effektiv für die Erarbeitung praxiskonformer Ergebnisse genutzt werden kann. Wir sind der Meinung, dass dieser Abschnitt in Präsenz stattfindet, damit auch der Erfahrungsaustausch neben dem gemeinsamen Entwickeln von Praxishilfen optimiert wird. Die Inhalte dieses Abschnitts können Sie der nachfolgenden Übersicht entnehmen.

Ziele: Praxisvertiefung für behördliche Datenschutzbeauftragte und Beschäftigte im operativen/administrativen Datenschutz

Modul	Inhalt	Format	Tag
1	Aufbau eines behördlichen Datenschutzmanagementsystems: Entwicklung eines behördlichen Datenschutzkonzepts/einer behördlichen Datenschutzleitlinie unter ständiger Anleitung	**Vortrag, Workshop, Übungen und Präsentationen im Plenum**	**1**
2	Entwicklung einer Auftragsverarbeitungsvereinbarung unter ständiger Anleitung Abgrenzung zur Vereinbarung nach Art. 26 DSGVO	**Vortrag, Workshop, Übungen und Präsentationen im Plenum**	**2**

3	Entwicklung einer datenschutzkonformen Behördenwebseite unter ständiger Anleitung	**Workshop, Übungen und Präsentationen im Plenum**	**2**
4	Entwicklung eines Schulungs- und Sensibilisierungskonzepts	**Workshop, Übungen und Präsentationen im Plenum**	**3**
5	Datenschutz und Datensicherheit Mindeststandard Protokollierung/ Grundschutzbaustein CON.3 zur Datensicherung Gemeinsame Übung mit IT 486 (Informationssicherheit/Datenschutz) zur Protokollierung und zur Datensicherung unter ständiger Anleitung	**Vortrag, Workshop, Übungen und Präsentationen im Plenum**	**3**
6	Entwicklung eines Meldeprozesses	**Workshop, Übungen und Präsentationen im Plenum**	**4**
7	Entwicklung eines Prozesses für Aufkunftsansprüche	**Workshop, Übungen und Präsentationen im Plenum**	**4**
8	Datenschutzfolgenabschätzung	**Workshop, Übungen und Präsentationen im Plenum**	**5**
9	Erfahrungsaustausch offene Fragen	**BfDI-Sprechstunde**	**5**
	Hinweise zur Erstellung der Projektarbeit und zur Zertifizierung Datenschutz-Beauftragte in der öffentlichen Verwaltung	**Vortrag**	**5**

4.4 Follow-Up 1: Nachhaltigkeit des Lernerfolgs

Um die Nachhaltigkeit des Lernerfolgs zu steigern, sieht unser Lernpfad im Anschluss an die Basis-Qualifizierung verschiedene Etappen zur Lernvertiefung, zum Erfahrungsaustausch und zur stärkeren Ausprägung von Basiskompetenzen vor. Diese Etappen sind im Wesentlichen durch verschiedene Erfahrungsaustausche – allen voran das am Europäischen Datenschutztag (28. Januar) jährlich stattfindenden Datenschutzforum[1] – sowie die Projektpräsentation und Prüfung zum Erwerb der Zertifikate „Datenschutzbeauftragte in der öffentlichen Verwaltung“ und „Operativer Datenschutz in der öffentlichen Verwaltung“ geprägt. Auch hier gilt das Flexibilisierungsprinzip: Alles kann - nichts muss! Für Datenschutzbeauftragte ist das Zertifikat zudem ein ausgezeichneter Beleg für das erforderlicher Fachwissen nach der EU-DSGVO, weshalb wir dieses Zertifikat für diese Zielgruppe empfehlen. Weitere Bausteine dieses Follow-Ups zur Basisqualifizierung sind anlassbezogene Online-Vorträge, um der thematischen Aktualität Rechnung zu tragen, sowie im BF 254 ein

[1] Das Datenschutzforum hat 2021 die seit 2014 angebotene Jahrestagung der behördlichen Datenschutzbeauftragten abgelöst.

Erfahrungsaustausch für Teilnehmende des BF 250. Dieser Austausch hat das Ziel, dass die Teilnehmenden des BF 250 noch einmal in der gleichen Zusammensetzung zusammenkommen, um sich über ihre praktischen Erfahrungen im Anschluss an die Basisqualifizierung auszutauschen. Hiermit entsprechen wir einem Wunsch aus dem Kreis unserer Teilnehmenden. Freuen Sie sich auf ein Wiedersehen, denn so macht Lernen noch mehr Spaß! Der nachfolgenden Übersicht können Sie noch einmal alle Bausteine dieses ersten Follow-Ups entnehmen.

Modul	Inhalt	Format	Tag
1	**SO 204/ SO 205 Datenschutzforum** **Aktuelle Themen und Erfahrungsaustausch**	2 Tage in Präsenz oder ein Tag digital	**1-2**
2	**Zertifikat: Projektpräsentation/Prüfung BF 260/BF 270**	Präsentation mit Abstract.	**1-2**
3	**Erfahrungsaustausch BF 254 (ca. 6 Monate später, nur für TN BF 250)** Vertiefung des Basiskurses	2 Tage in Präsenz	**1-2**
4	**Online-Vorträge SO 520: Anlass bezogen**	90 Minuten Digital	

Ausführlichere Hinweise zur Zertifizierung haben wir Ihnen unter Ziff. 6 zusammengestellt.

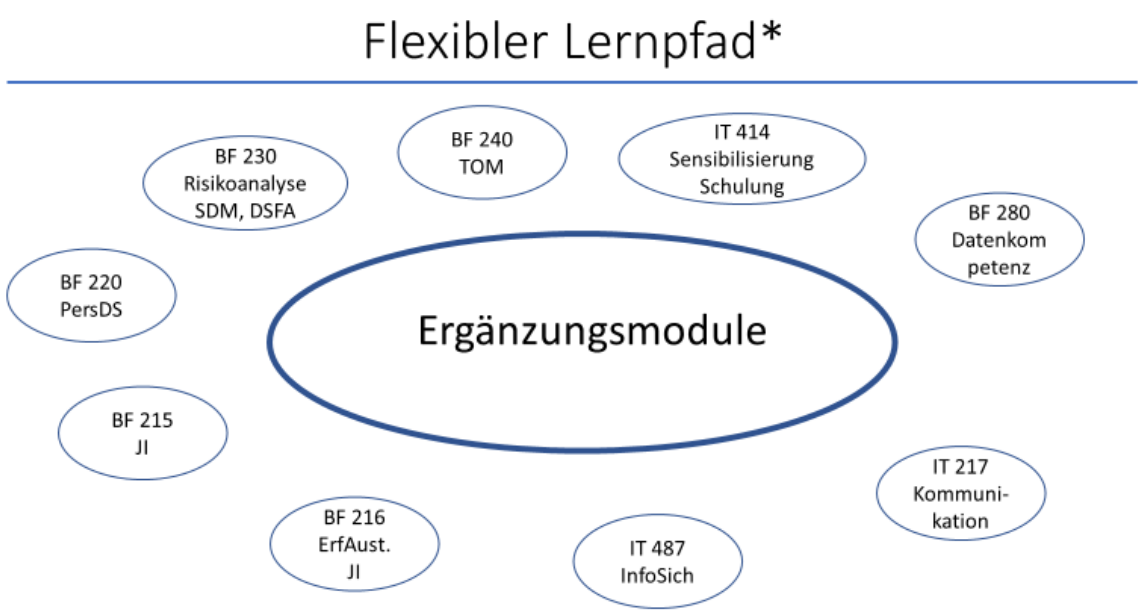
4.5 Follow-Up 2: Spezialfortbildung für Fortgeschrittene

In unseren Kursen haben wir die Erfahrung gemacht, dass Fortgeschrittene ein spezielles Follow-Up benötigen, dem mit den bisherigen Stufen des Lernpfads nicht zufriedenstellend entsprochen werden kann. Hierfür ist ein eigenes Angebot erforderlich, das die Grundlagen voraussetzt und auf einem hohem Wissenstand und sehr ausgeprägten Praxiserfahrungen aufsetzt. Gemeinsam mit dem BfDI bieten wir deshalb die sog. „Specials“ an. Dabei handelt es sich um eine Präsenzveranstaltung, die dem erweiterten Erfahrungs- und Wissensaustausch dient. Es werden insgesamt fünf Themenkomplexe mit hoher Praxisbedeutung behandelt. Eine Übersicht finden Sie hier:

Modul	Inhalt	Format	Tag
1	Datenschutz-Specials BF 257 – Vertiefung für Fortgeschrittene (gemeinsam mit dem BfDI)	Präsenz **Modul 1: AV und Verant-wortlichkeit** **Modul 2: DS und Be-schaffungen** **Modul 3: Drittstaaten** **Modul 4: Auskunftsan-spruch** **Modul 5: Technik, DSFA, Datensicherheit**	**1-2**

4.6 Flexible Ergänzungsmodule

Der Datenschutz in der öffentlichen Verwaltung hat viele Facetten und ist dabei so bunt, wie die verschiedenen Verwaltungsbereiche. Hieraus folgen verschiedene flexible Fortbildungsbedarfe in unterschiedlichen Zielgruppen, für die wir flexible Ergänzungsmodule bereithalten. Eine Übersicht zu diesen Ergänzungsmodulen, die im Lernpfad unabhängig von den zuvor vorgestellten Kursen belegt werden können, finden Sie nachstehend:



*Auszug. Eine vollständige Übersicht finden Sie im Lernpfad

Modul	Inhalt	Format	Tag
1	IT 217 – fachübergreifende Kommunikation in IT-Projekten-	(Präsenz/digital)	**1 Tag**
2	BF 230/235 Risikobewertung nach der DSGVO am Beispiel einer Datenschutzfolgenabschätzung nach dem Standarddatenschutzmodell	(Präsenz/digital)	**2 Tage**
3	IT 414 Sensibilisierung Effektiv und fair: Nachhaltig schulen und sensibilisieren im Datenschutz und der Informationssicherheit	Digital	**2 Tage**
4	BF 240/245 Technische und organisatorische Maßnahmen nach der DSGVO	(Präsenz/digital)	**2 Tage**
5	BF 280 Data Literacy – Datenkompetenz in der öffentlichen Verwaltung	(Präsenz/digital)	**2 Tage**
6	IT 487/497 Informationssicherheit in der öffentlichen Verwaltung – Basis kompakt	(Präsenz/digital)	**5 Tage**
7	BF 220/225 Personaldatenschutz – Rechtliche Grundlagen	(Präsenz/digital)	**3 Tage**
8	BF 215/217 Datenschutz im Bereich JI/3. Teil des BDSG	(Präsenz/digital)	**1 Tag/ 0,5 Tage**
9	BF 216/218 Datenschutz im Bereich JI/3. Teil des BDSG - Erfahrungsaustausch	(Präsenz/digital)	**1 Tag/ 0,5 Tage**

Weitere Ergänzungen dieser Module können Sie der nachstehenden Auswahl am BAköV-Angebot zum Kompetenzerwerb in anderen Bereichen entnehmen, die auch für den behördlichen Datenschutz hilfreich sein können. Ausführlichere Inhalte halten wir für Sie in IFOS-Bund unter ifosbund.de bereit:

- **FP 100 Verständliches Schreiben - Mehr Erfolg durch gute Texte**
- **BF 500 Notfallmanagement etablieren, umsetzen und steuern**
- **FÜ 270 Teams zielorientiert leiten**
- **FÜ 330 Changemanagement: Veränderungsprozesse aktiv gestalten**
- **FÜ 640 Steuerung von Veränderungsprozessen**
- **FÜ 400 Arbeit organisieren und Zeit managen für Führungskräfte**
- **IT 320 Grundlagen Digitales Management in der öffentlichen Verwaltung**
- **IT 205/206 Besondere Rahmenbedingungen für IT-Projekte in der Bundesverwaltung**
- **IT 234/230 Das V-Modell XT Bund – Basis**
- **IT 484/485 Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung - Grundlagen und Anwendung**
- **IT 540 Barrierefreie PDF-Dokumente erstellen - Grundlagen**
- **IT 600 Grundlagenwissen für Systemadministratoren in der öffentlichen Verwaltung**
- **IT 607 IT-Sicherheitsaspekte in heterogenen Netzen**
- **IT 630 Daten- und Informationssicherheit beim Einsatz mobiler Geräte**
- **IT 680 Computer-Forensik in Theorie und Praxis**
- **KO 240/21 Kommunikation mit Vorgesetzten**
- **KO 300 Erfolgreich verhandeln**
- **KO 1XX kommunizieren und kooperieren“**
- **KO 340 Argumentieren, überzeugen, Feedback geben“**
- **MD 330 Grundlagen- und Aufbauseminar: Lehren lernen**
- **OR 160 Personalbedarfsermittlung**
- **OR 270 Wissensmanagement - Theoretischer Überblick und individuelle Anwendung**
- **OR 520 Risiko- und Krisenmanagement in Projekten**
- **SE 150 Arbeit organisieren und Zeit managen**
- **SE 220 Resilienz - Widerstandskraft und Flexibilität stärken**
- **SE 240 Kreative Problemlösungen im Arbeitsalltag**

Darüber hinaus bietet die BAköV das Thema „Datenschutz“ auch als **Querschnittsthema für spezifische Zielgruppen** an (vgl. hierzu auch Ziff. 3.3, u.a. als integriertes Thema in entsprechenden Grundlagenkursen oder in Form von spezifischen Online-Vorträgen). Dieses Angebot wird z.T. aktuell noch entwickelt und kann daher noch nicht vollständig abgebildet werden. Mit diesem Angebot möchte die BAköV einen Beitrag leisten, um den Datenschutz als Querschnittsthema weiter zu entwickeln. Entsprechende Angebote werden in IFOS veröffentlicht.

4.7 Angebote der Digitalakademie des Bundes

Darüber hinaus bietet die Digitalakademie des Bundes als Teil der BAköV weitere Angebote, mit denen Sie sich digital qualifizieren können. Schauen Sie doch einfach mal unter www.digitalakademie.bund.de vorbei und genießen Sie die eine oder andere Lernreise durch die Welt der Digitalisierung. Wir wünschen Ihnen hierbei viel Freude!

5 Fortbildung in der öffentlichen Verwaltung

Die Fortbildung ist modular aufgebaut und beinhaltet die Möglichkeit der individuellen Gestaltung abhängig von dem konkreten Bedarf an Fortbildung der Teilnehmenden.

Alle in der Zielgruppe genannten Beschäftigten der Bundesverwaltung sind nach vorheriger Anmeldung der Behörde zur kostenfreien Teilnahme berechtigt. Die Anmeldung muss durch die Fortbildungsstelle in IFOS-BUND zusätzlich erfolgen.

5.1 Interviewberatung und Selbsteinschätzungstest

Zur Überprüfung Ihrer Kenntnisse im Vorfeld der Fortbildung besteht die Möglichkeit einer Interviewberatung bei der BAköV. Diese ist freiwillig und kann jederzeit wiederholt werden. Zudem bietet die BAköV im Fortbildungsportal des Bundes einen elektronischen Selbsteinschätzungstest für Sie an.

5.2 Lernprozessbegleitung

Sie haben die Möglichkeit, die Lernprozessbegleitung der BAköV in Anspruch zu nehmen. Die Lernprozessbegleitung der BAköV steht zur Auskunft und Beratung, sowohl für die Fortbildungsbeauftragten als auch für die Teilnehmenden zur Verfügung. Die Lernprozessbegleitung berät Sie bei der Erstellung Ihres individuellen Lernpfads, koordiniert und steht Ihnen als Ansprechperson für weitere Qualifizierungen zur Verfügung.

6 Zertifizierung

Für den Erwerb der BAköV-Zertifikate erarbeiten Sie ein Projekt innerhalb ihrer Behörde bzw. dem Aufgabenbereich. Dieses Projekt stellen Sie in einem Präsentationsworkshop vor. Die Zertifizierungen schließen Sie mit einer Prüfung ab. Ihr Zertifikat ist 5 Jahre gültig. Die Verlängerung Ihres Zertifikats ist nur über eine vorgegebene, zu erreichende Punktzahl möglich (siehe unten). Für die Zertifizierung gilt die Zertifizierungsordnung der BAköV.

6.1 Fachliche Begleitung

Das Thema und der Plan der Projektarbeit für die Zertifizierung wird mit der fachlichen Begleitung besprochen und bestätigt. Die Aufgabe der fachlichen Begleitung ist es, die eigenständige Auswahl und Durchführung des Projektes zu unterstützen. Die Begleitung unterstützt bei der Festlegung der Themenauswahl (Projektaufgabe), begleitet den Erstellungsprozess einer konzeptionellen Projektarbeit über ein

behördenspezifisches Thema und ggf. die Präsentation. Die Begleitung sollte vorzugsweise bei der eigenen Behörde erfolgen, um im Idealfall eine hohe Nähe der Projektarbeit zum Arbeitsfeld der Nachhaltigkeit herzustellen. Bei Bedarf kann auch eine Begleitung durch den BfDI angefragt werden. Die Entscheidung darüber wird vom Kandidaten bzw. von der Kandidatin getroffen.

6.2 Projektarbeit

Im praktischen Teil der Zertifizierung soll ein Projekt in der jeweiligen Behörde bearbeitet werden. Der Praktische Teil sollte begleitend stattfinden (behördenintern oder mit einer externen Unterstützung) und das Thema sollte den eigenen oder zukünftigen Aufgabenbereich betreffen bzw. daraus hervorgehen. Dies kann sowohl eine Vorlage für Entscheidungen der Hausleitung, die Aufbereitung fachlicher Themen aus dem Bereich Datenschutz als auch neue bzw. bevorstehende Projekte umfassen. Anliegen ist es, die Tätigkeit zu unterstützen bzw. die Erstellung von Dokumenten zu begleiten. Zur Bestätigung des Projektthemas wird der Antrag „Plan der Projektarbeit“ von der BAköV genehmigt und mit dem BfDI abgestimmt. Der Umfang des Projektes wird mit der fachlichen Begleitung besprochen und die reine Dokumentation sollte ca. 5-10 Seiten (ohne Deckblatt, Inhaltsverzeichnis, Literatur-/Quellenverzeichnis etc.) umfassen. Im Anhang dieses Lernpfades ist eine Übersicht von Themenvorschlägen enthalten.

Projektarbeit	Dauer
Auf der Grundlage der modularen Inhalte dieses Konzepts und den Anforderungen aus dem Aufgabenbereich ist ein überschaubares Projekt innerhalb der Behörde zu absolvieren.	Ca. 20 Stunden

Hinweis:

Die positive Beurteilung eines Projekts ersetzt nicht eine vollständige QS, ein (Zertifizierungs-)Audit oder sonstige genaue Überprüfungen des zugehörigen vollständigen Projektes.

6.3 Projektpräsentation

Die Präsentation der Projektarbeit erfolgt in einem behördenübergreifenden Workshop. Die Abgabe der Arbeit muss spätestens **drei Wochen** vor dem Workshop erfolgen. Eine elektronische Abgabe an die Mailadresse (lg5@bakoev.bund.de) ist möglich. Alle Teilnehmenden präsentieren ihre Projektarbeit und führen mit dem Teilnehmenden ein Gespräch darüber. Dieses Gespräch wird - die Präsentation eingeschlossen

- jeweils einen Zeitraum von etwa 30 Minuten beanspruchen. Der Workshop wird von der BAköV moderiert.

6.4 Prüfung

Abschließendes Element der Zertifizierung ist die Prüfung. Diese findet vor Ort bei der BAköV statt (an einer Online-Lösung wird noch gearbeitet). In 120 Minuten müssen 100 Fragen basierend auf dem Handbuch „Datenschutzbeauftragte in der öffentlichen Verwaltung“ beantwortet werden. Es handelt sich um einen Multiple-Choice-Test, bei dem mehrere Antworten zu einer Frage richtig sein können. 75 % der Antworten müssen richtig erkannt werden.

6.5 Zertifikatserhalt

Zur Erhaltung der Qualifikation wird eine kontinuierliche Fortbildung benötigt, die alle Aspekte Ihres Aufgabenbereichs umfasst und sowohl auf eine Erweiterung der fachlichen als auch der sozialen Kompetenzen abzielt. Die Fortbildung zum Kompetenzerhalt wird überwiegend durch Veranstaltungen der BAköV ermöglicht. Zum Erhalt oder zur jeweiligen Verlängerung des Zertifikats werden verschiedene Maßnahmen angeboten, die insbesondere im hier vorgestellten Lernpfad beschrieben sind. Auch die flexiblen Ergänzungsmodule zählen hierzu. Zudem besteht die Möglichkeit, eigene Vortrags- oder Dozierendentätigkeit im Bereich des Datenschutzes anerkennen zu lassen.

Punktesystem für den Erhalt des Zertifikats:

Innerhalb von 5 Jahren müssen 50 Punkte erreicht werden. Die zweimalige Teilnahme am „Datenschutzforum“ innerhalb dieses Zeitraums ist Bedingung.

Die Punkte sind über folgende Maßnahmen zu erreichen	**Punkte**
Teilnahme am Datenschutzforum	15
Teilnahme an anderen Veranstaltungen der BAköV aus den Bereichen des Datenschutzes.	13
Teilnahme an anderen Veranstaltungen der BAköV	12
Vortragstätigkeit bzw. Dozierendentätigkeit im Rahmen von Schulungen, Kongressen, usw. (Anerkennung nach Absprache mit der BAköV)	10
Teilnahme an Online-Vorträgen der BAköV	5

Teilnahme an Fortbildungsangeboten von externen Anbietern und Kongressen im Bereich Datenschutz. (Anerkennung nur nach Absprache mit der BAköV)	8
Teilnahme an anderen Fortbildungsangeboten von externen Anbietern (Anerkennung nur nach Absprache mit der BAköV)	5

Hinweis:

Die Punktetabelle gilt ab dem 1.1.2022. Zertifikate, die in den 5 Jahren vor diesem Stichtag erworben wurden, werden auf der Basis des bis zum 31.12.2021 erforderlichen Werts von 40 Punkten verlängert. Die Übergangszeit geht damit bis zum 31.12.2026. Mit der Punkteerhöhung verfolgen wir das Ziel, die für die Praxis erforderliche Qualifizierung zu intensivieren und nachhaltiger zu gestalten.

Die Zertifikatsverlängerung ist nur auf schriftlichen Antrag möglich. Der Antrag soll 3 Monate vor Ablauf des Zertifikats vorliegen.

7 ANHANG

- Zertifizierungsordnung
- Themenvorschläge für die Projektarbeit
- Empfehlungen zur Anfertigung der Projektarbeit
- Empfehlungen zur Vorbereitung der Präsentation
- Formulare
    - Plan der Projektarbeit – Antrag
    - Änderungs- / Ergänzungsmitteilung
    - Antrag: Zertifikatsverlängerung

7.1 Zertifizierungsordnung vom 1. Januar 2022

I. Allgemeines

§ 1: Geltungsbereich

Diese Zertifizierungsordnung gilt für die Qualifizierung von Datenschutzbeauftragten in der öffentlichen Verwaltung und von Beschäftigten im operativen behördlichen Datenschutz oder im behördlichen Wissensmanagement (z.B. hauptamtlich Lehrende). Sie regelt die Zertifizierung dieser Zielgruppen.

§ 2: Zweck der Zertifizierung

Die Zertifizierung dient dem Nachweis der erforderlichen Fachkunde für die in § 1 genannten Zielgruppen. Nach erfolgreicher Präsentation der Projektarbeit und der Prüfung erhalten die Absolventinnen bzw. Absolventen ein Zertifikat, durch das bescheinigt wird, dass sie aus Sicht der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern und für Heimat (BAköV) in Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) die notwendigen Kenntnisse und Fähigkeiten besitzen, um insbesondere die in § 1 genannten Tätigkeiten auszuüben.

§ 3: Zulassung zur Fortbildungsmaßnahme

Berechtigt zur Teilnahme an der in § 1 dieser Zertifizierungsordnung genannten Fortbildungsmaßnahme und Zielgruppen sind Beschäftigte der öffentlichen Verwaltung aus dem höheren, gehobenen und mittleren Dienst.

§ 4: Fortbildungsinhalt und -dauer

(1) Die in § 1 dieser Zertifizierungsordnung genannte Fortbildungsmaßnahme ist modular aufgebaut und beinhaltet die Möglichkeit der individuellen Gestaltung abhängig von dem konkreten Bedarf an Fortbildung der Teilnehmenden.

(2) Zur Vorbereitung auf die Projektarbeit und die Prüfung sollten die Teilnehmenden grundsätzlich die Fortbildungsmaßnahme BF 250 „Datenschutzmanagement in der öffentlichen Verwaltung“ gemäß des

BAköV-Lernpfades „Datenschutz in der öffentlichen Verwaltung“ absolvieren

II. Projektarbeit, Projektpräsentation und Prüfung

§ 5: Projektarbeit

Die Teilnehmenden müssen eine Projektarbeit zu einem für den Datenschutz der öffentlichen Verwaltung relevanten Thema erstellen. Dabei können sie sich seitens ihrer Behörde oder einer anderen externen Stelle begleiten lassen. Die Projektarbeit sollte einen geschätzten Mindestarbeitsaufwand von etwa 20 Stunden erfordern.

Über die Projektarbeit erstellen die Teilnehmenden eine schriftliche Dokumentation von ca. 5 bis 10 Seiten, die eine Erläuterung aller wesentlichen Bestandteile des Projekts enthält, und bestätigen gegenüber der BAköV mit eigener Unterschrift unter der Dokumentation, dass die Projektarbeit von ihr bzw. ihm tatsächlich und eigenverantwortlich durchgeführt wurde.

§ 6: Projektpräsentation

(1) Voraussetzung für den Erhalt des Zertifikats nach § 9 dieser Zertifizierungsordnung ist eine 20 Minuten umfassende Präsentation der Projektarbeit gem. § 5.

(2) Die BAköV bewertet die Projektarbeit und die Präsentation in Abstimmung mit dem BfDI. Die Bewertung kann „bestanden“ oder „nicht bestanden“ lauten. Kriterien für die Bewertung sind neben der Eigenständigkeit der Erarbeitung, die überzeugende Anwendung der einschlägigen Rechtsnormen und Gerichtsentscheidungen sowie die Praxistauglichkeit der Arbeit. Empfehlungen des BfDI und/der Datenschutzkonferenz der unabhängigen Aufsichtsbehörden aus Bund und Ländern sind zu berücksichtigen. Zur Praxistauglichkeit der Arbeit zählen die praxiskonforme Ergebnisorientierung für das jeweilige behördliche Umfeld, Nachvollziehbarkeit der Ausführungen, Überzeugende Vermittlung der zentralen und wesentlichen Arbeitsergebnisse, die Beachtung von geschlechtergerechter Sprache, die Angabe von Quellen und moderne Präsentationstechniken, die auch die Anforderungen aus Behindertengleichstellungsrecht beachten. Die Arbeit gilt als bestanden, wenn die vorgenannten Kriterien überwiegend erfüllt werden. Hierfür legt

die BAköV in Abstimmung mit dem BfDI folgende Punktewerte zu Grunde:

5 Punkte: Umfassend erfüllt

4 Punkte: Weit überwiegend erfüllt

3 Punkte: Überwiegend erfüllt

2 Punkte: zum Teil erfüllt

1 Punkt: zu einem geringen Teil erfüllt

0 Punkte: nicht erfüllt

(3) Die BAköV kann die Teilnehmenden in Abstimmung mit dem BfDI zur einmaligen Überarbeitung der Projektarbeit in einem angemessenen Zeitraum bitten.

§ 7: Prüfung

(1) Die Abschlussprüfung dauert 120 min.
(2) Gegenstand der Prüfung sind die Inhalte aus der jeweils aktuellen Fassung des Handbuchs „Datenschutzbeauftragte in der öffentlichen Verwaltung“, das zur Vorbereitung auf die Prüfung zur Verfügung gestellt wird.
(3) Die Abschlussprüfung findet in Form eines schriftlichen Multiple-Choice-Verfahrens statt (Abschlusstest).
(4) Die Abschlussprüfung ist nicht öffentlich.

§ 8: Bewertung

(1) Eine Differenzierung nach Noten findet bei der Bewertung der Prüfungsleistung nicht statt. Die Prüfung gilt vielmehr nur als „bestanden“ oder „nicht bestanden“. Die Prüfung gilt als bestanden, wenn mindestens 75 Prozent der möglichen Punktzahl erreicht werden.
(2) Die Abschlussprüfung kann einmal wiederholt werden. Die Wiederholung soll in der Regel innerhalb von zwölf Monaten nach dem erfolglosen Versuch stattfinden.
(3) Die Prüfungsleistung gilt als nicht bestanden, wenn Teilnehmende zu einem Prüfungstermin ohne triftige Gründe nicht erscheinen oder nach Beginn der Prüfung ohne triftige Gründe von der Prüfung zurücktreten oder die Prüfungsleistung nicht vor Ablauf der Prüfung erbracht wird.

(4) Die für den Rücktritt oder das Versäumnis geltend gemachten Gründe müssen der BAköV unverzüglich schriftlich angezeigt und glaubhaft gemacht werden. Bei Krankheit kann die Vorlage eines ärztlichen Attestes verlangt werden. Erkennt die BAköV die Gründe an, so kann die Zulassung zu der entsprechenden Prüfungsleistung erneut beantragt werden.

(5) Versuchen Teilnehmende, das Ergebnis der Prüfungsleistung durch Täuschung oder Benutzung nicht zugelassener Hilfsmittel zu beeinflussen, gilt die betreffende Prüfungsleistung als nicht bestanden. Wer den ordnungsgemäßen Ablauf der Prüfung stört, kann von der jeweiligen Aufsicht, in der Regel nach Abmahnung, von der Fortsetzung der Prüfungsleistung ausgeschlossen werden; in diesem Fall gilt die betreffende Prüfungsleistung als nicht bestanden. Die Gründe für den Ausschluss sind aktenkundig zu machen.

(6) Erfolgt ein Ausschluss von der weiteren Erbringung der Prüfungsleistung, können Teilnehmende verlangen, dass die Entscheidung der BAköV überprüft wird. Dies gilt entsprechend bei Feststellungen gemäß Satz 1.

III. Zertifikat

§ 9: Zertifikat

(1) Nach der erfolgreichen Prüfung wird möglichst innerhalb von zwei Wochen ein Zertifikat ausgestellt.

(2) Das Zertifikat ist vom Präsidenten der Bundesakademie oder seiner Vertretung zu unterzeichnen. Das Zertifikat trägt das Datum des Tages, an dem die Prüfung erfolgte.

(3) Das Zertifikat hat eine Gültigkeitsdauer von fünf Jahren, beginnend mit dem Tag der Prüfung.

(4) Die Gültigkeitsdauer verlängert sich auf schriftlichen Antrag für die Zeit einer Inanspruchnahme von Elternzeit nach dem Bundeselterngeld- und Elternzeitgesetz und Zeiten eines Beschäftigungsverbots nach dem Mutterschutzgesetz sowie für Zeiten einer Betreuung oder Pflege eines pflegebedürftigen Angehörigen nach dem Pflegezeitgesetz und dem Familienpflegezeitgesetz in dem Umfang, in dem eine

Erwerbstätigkeit nicht erfolgt ist, höchstens jedoch für die Zeit von fünf Jahren.

(5) Eine Verlängerung des Zertifikats erfolgt, wenn die Zertifikatsinhaberin bzw. Zertifikatsinhaber im Zeitraum der Gültigkeitsdauer durch den Besuch einschlägiger Fortbildungsveranstaltungen auf Grundlage der Tabelle in Ziff. 6.5 des Lernpfads „Datenschutz in der öffentlichen Verwaltung“ 50 Punkte erreicht, zweimal das Datenschutzforum besucht und sie/er im Zeitpunkt der Zertifikatsverlängerung zur Zielgruppe nach § 1 zählt oder für die Übernahme eine dieser Aufgaben vorgesehen ist. Wenn Teilnehmende die erforderliche Punktzahl nicht erfüllen und auch keine Verlängerung nach Abs. 4 in Betracht kommt, können sie zur Zertifikatsverlängerung die Prüfung erneut ablegen. Die Zertifikatsverlängerung ist nur auf schriftlichen Antrag möglich. Der Antrag soll 3 Monate vor Ablauf des Zertifikats vorliegen.

§ 10: Ungültigkeit von Prüfungen

(1) Haben Teilnehmende im Rahmen der Projektarbeit getäuscht und wird diese Tatsache erst nach der Aushändigung des Zertifikats nach § 9 dieser Zertifizierungsordnung bekannt, so kann die BAköV in Abstimmung mit dem BfDI nachträglich die Zertifizierung für nicht bestanden erklären.

(2) Das unrichtige Zertifikat nach § 9 dieser Zertifizierungsordnung ist einzuziehen und gegebenenfalls neu zu erteilen.

§ 11: Rechtsmittel

Gegen die Entscheidungen der BAköV ist die Beschwerde möglich. Sie ist innerhalb von vier Wochen nach Bekanntgabe der Entscheidung bei der BAköV schriftlich einzureichen. Diese entscheidet in Abstimmung mit dem BfDI über die Beschwerde.

IV. Abschlussvorschriften

§ 12: Datenschutzerklärung

(1) Die im Zusammenhang mit dieser Zertifizierungsordnung zur Verfügung gestellten personenbezogenen Daten werden ausschließlich zum Zweck der erforderlichen Zertifikatsverwaltung einschließlich aller mit der Durchführung der Abschlussprüfung zusammenhängenden erforderlichen Maßnahmen verwendet. Rechtsgrundlage ist Art. 6 Abs. 1 lit. e EU-DSGVO i.V.m. § 3 BDSG. Im Übrigen gilt die

Datenschutzerklärung der BAköV, die unter www.bakoev.bund.de/datenschutz eingesehen werden kann.

(2) Die personenbezogenen Daten werden bei der BAköV aufbewahrt. 10 Jahre nach der letztmaligen Entscheidung über das Bestehen oder Nichtbestehen der Prüfung oder einer Zertifikatsverlängerung werden die Daten vernichtet.

§ 13: Inkrafttreten und Veröffentlichung

Diese Zertifizierungsordnung tritt am 1. Januar 2022 in Kraft.

7.2 Themenvorschläge für die Projektarbeit

Aus allen Gebieten des behördlichen Datenschutzes können Themen für Projektarbeiten formuliert werden. Die nachfolgende Übersicht enthält lediglich Beispiele:

Themenvorschlag 1:
Erstellen Sie für Ihre Behörde ein Datenschutzkonzept. Die Erarbeitung eines vollständigen Datenschutzkonzepts ist im Rahmen der Projektarbeit nicht möglich. Daher sollte eine überblickartige Inhaltsangabe erfolgen und auf drei Beispielkapitel eingegangen werden. Es ist ein Inhaltsverzeichnis für ein vollständiges Datenschutzkonzept zu erstellen. Es ist zu begründen, warum diese Aspekte Gegenstand eines Datenschutzkonzeptes sind. Bei der Erarbeitung der drei Beispielskapitel kann unter anderem auf folgende Aspekte eingegangen werden:

- Umfang und Verarbeitung der zu verarbeitenden personenbezogenen Daten unter Berücksichtigung besonderer Datenarten
- Rechtsgrundlage der Verarbeitung beziehungsweise Zweckbindung der Datenverarbeitung
- Einhaltung von Datensparsamkeit und Datenvermeidung
- Recht auf Auskunft, Berichtigung etc. von betroffenen Personen
- Regelung der Verantwortlichkeiten im Datenschutz
- Vertragliche Regelungen einer Auftragsverarbeitung
- Bestellung und Aufgaben einer bzw. eines Datenschutzbeauftragten
- Prozess zur Aktualisierung des Datenschutzkonzepts sowie Berücksichtigung der Auswirkungen auf andere Dokumente

Themenvorschlag 2:
Erstellen Sie für Ihre Behörde ein Sensibilisierungs- und Schulungskonzept zum Datenschutz und erstellen Sie einen Fragebogen zu einem ausgewählten Themenbereich (zum Beispiel Passwortschutz, Internet, Installation von Programmen, gesetzliche oder sonstige regulatorische Vorschriften). Das Sensibilisierungs- und Schulungskonzept zum Datenschutz sollte beispielsweise folgende Aspekte enthalten:

- Definition der Zielgruppe für die Sensibilisierungsmaßnahmen, Bedarfs-ermittlung
- Definition der Schulungen für die jeweiligen Zielgruppen (zum Beispiel Grundsensibilisierung, anwenderorientierte Schulungen)
- Art und Weise der Durchführung (zum Beispiel Vorträge, Webbasiertes Training, Bereitstellung von Inhalten über das Intranet

oder sonstige (elektronische) Verzeichnisse, Newsletter) sowie Maßnahmenauswahl
- Art und Weise der Aufrechterhaltung zur Beschäftigtensensibilisierung
- Einsetzbare Werkzeuge
- Akzeptanz bei den Beschäftigten
- Evaluation der Sensibilisierungs- und Schulungsmaßnahmen (zum Beispiel Bewertungsbögen zur Verbesserung der Qualität)

Themenvorschlag 3:
Erstellen Sie eine allgemeingültige Prozessbeschreibung zur Durchführung von Datenschutz-Folgenabschätzungen. Führen Sie eine Datenschutz-Folgenabschätzung anhand eines selbst gewählten Beispiels Ihrer Behörde (Video, Zutrittskontroll- oder Zeiterfassungssysteme, Telekommunikationsanlage, elektronische Personalakte, ERP-System etc.) durch und dokumentieren Sie diese. Inhalte sind z.B.:

- Entwickeln Sie einen standardisierten Prozess zur Durchführung einer Datenschutz-Folgenabschätzung, der beispielsweise folgende Aspekte beinhaltet: Informationsbeschaffung, Mitbestimmungsrechte des Personalrats, Meldewege, Wichtige Sicherheitsanforderungen an die jeweilige automatisierte Verarbeitung, Dokumentation
- Erstellen Sie eine Vorlage zur Durchführung einer Datenschutz-Folgenabschätzung durch die bzw. den Datenschutzbeauftragten.

Themenvorschlag 4:
Erstellen Sie eine allgemeingültige Prozessbeschreibung zur Erstellung von Verzeichnissen für Verarbeitungstätigkeiten. Erstellen Sie ein Verzeichnis für Verarbeitungstätigkeiten anhand eines selbst gewählten Beispiels Ihrer Behörde (zum Beispiel Videoüberwachung, Zutrittskontroll- oder Zeiterfassungssysteme, Telekommunikationsanlage, elektronische Personalakte, ERP-System etc.). Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Entwickeln Sie einen standardisierten Prozess zur Erstellung eines Verzeichnisses für Verarbeitungstätigkeiten.
- Entwickeln Sie eine Arbeitsanweisung und eine Vorlage zur Erstellung eines Verzeichnisses für Verarbeitungstätigkeiten.

Themenvorschlag 5:
Erstellen Sie eine Dienstanweisung zur Nutzung von E-Mail- und Internet am Arbeitsplatz. Erläutern Sie hierbei die mit der E-Mail- und Internetnutzung verbundenen Risiken und deren Lösungsansätze. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Notwendigkeit der Dienstanweisung unter Beachtung der rechtlichen Anforderungen (zum Beispiel Telekommunikationsgesetz)
- Umfang der Nutzung (Erlaubnis, Verbot oder Duldung der privaten Nutzung)
- Regelung zum Herunterladen von Internetinhalten
- Umgang mit und Informationspflichten über den Einsatz von Cookies
- Regelungen zur Verwendung von Spam-Filtern
- Kontrollbefugnisse des Arbeitgebers
- Einbeziehung des Personalrats
- Technische und organisatorische Maßnahmen (zum Beispiel Verschlüsselung, elektronische Signaturen)
- Hinweispflichten zur Protokollierung
- Zeigen Sie Schnittstellen zu anderen behördeninternen Dokumenten auf.

Themenvorschlag 6:
Erstellen Sie eine Dienstanweisung zum Umgang mit mobilen Endgeräten (zum Beispiel Laptops, Tablets, Handys, Smartphones). Erläutern Sie hierbei die mit dem Umgang mobiler Endgeräte verbundenen Risiken und deren Lösungsansätze. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Notwendigkeit der Dienstanweisung unter Beachtung der rechtlichen Anforderungen
- Umfang der Nutzung
- Umgang mit mobilen Endgeräten außerhalb der Diensträume (zum Beispiel VPN, WLAN)
- Speicherung von Dokumenten
- Einhaltung technischer und organisatorischer Anweisungen zum Datenschutz und zur Datensicherheit (zum Beispiel Virenschutz, Verschlüsselung)

Themenvorschlag 7:
Erstellen Sie einen standardisierten Prozess für die Einbeziehung externer Dienstleisterinnen oder Dienstleister zur Verarbeitung personenbezogener Daten im Auftrag der Behörde („Auftragsverarbeitung“). Im

Rahmen der Projektarbeit kann am Beispiel „Rechenzentrumsbetrieb“ auf folgende Aspekte eingegangen werden:

- Definition gesetzlicher Anforderungen
- Vor- und Nachteile zur Auslagerung an Externe
- Zulässigkeitsprüfung zur Einbeziehung von Auftragnehmenden
- Sorgfältige Auswahl von Auftragnehmenden sowie Überprüfung der Einhaltung von Datenschutzmaßnahmen (zum Beispiel Zertifizierungsmöglichkeiten)
- Es ist das Risikopotential zu beschreiben sowie technische und organisatorische Maßnahmen zu entwickeln, die den Schutz personenbezogener Daten sicherstellen.

Themenvorschlag 8:
Prüfen Sie die Voraussetzungen zur Auftragsverarbeitung anhand des Beispiels „Cloud Computing“ und erstellen Sie in diesem Zusammenhang eine Checkliste zur Verwendung bei geplanten Outsourcing-Projekten. Die Projektarbeit sollte z.B. folgende Aspekte umfassen:

- Definition gesetzlicher Anforderungen
- Zulässigkeitsprüfung zur Einbeziehung von Externen
- grenzüberschreitender Datentransfer bei Cloud Computing
- Berücksichtigung von IT-Sicherheitsstandards und anderer Regelungswerke
- Sorgfältige Auswahl von Externen sowie Überprüfung der Einhaltung von Datenschutzmaßnahmen (zum Beispiel Zertifizierungsmöglichkeiten)

Themenvorschlag 9:
Erstellen Sie einen Fragebogen zur Durchführung von Erst- und Folgekontrollen im Rahmen der Auftragsverarbeitung. Erläutern Sie Ihre Herangehensweise zur Durchführung von Erst- und Folgekontrollen bei Externen. Der Fragebogen sollte z.B. folgende Aspekte beinhalten:

- Definition der Ziele zur Verwendung eines standardisierten Fragebogens-Kontrollfragen zu technischen und organisatorischen Maßnahmen
- Erläutern Sie Ihre Vorgehensweise, wenn bei Dienstleistenden keine angemessenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit getroffen wurden.

Themenvorschlag 10:
Erläutern Sie mögliche Risiken bei einer Datenübermittlung an öffentliche und nicht-öffentliche Stellen anhand eines selbst gewählten Beispiels. Gehen Sie darüber hinaus auf die technischen und organisatorischen Maßnahmen ein, die diesen Risiken entgegenwirken und eine

sichere Datenübermittlung gewährleisten. Die Projektarbeit sollte z.B. folgende Aspekte enthalten:

- Prüfung der Zulässigkeitsvoraussetzungen einer Datenübermittlung an eine andere öffentliche Stelle
- Prüfung der Zulässigkeitsvoraussetzungen einer Datenübermittlung an eine nicht-öffentliche Stelle
- Folgen unzulässiger Datenübermittlung an Dritte
- Entwickeln Sie eine allgemeingültige Dienstanweisung zur Datenübermittlung an öffentliche und nicht-öffentliche Stellen.

Themenvorschlag 11:
Erstellen Sie einen Auditplan zur Überprüfung datenschutzrechtlicher Anforderungen in Ihrer Behörde und führen Sie auf dieser Grundlage ein Datenschutzaudit durch. Der Auditplan sollte z.B. folgende Aspekte enthalten:

- Auditrahmendaten
- Gegenstand sowie Kontrollziele des Datenschutzaudits
- Zielsetzung des Datenschutzaudits
- Erforderliche Dokumentation
- Auditbericht
- Mängelbehebung, Folgemaßnahmen und Abschluss
- Auditstandards
- Gehen Sie bei der Durchführung des Datenschutzaudits mindestens auf folgende Aspekte ein:
    - Überprüfung der technischen und organisatorischen Maßnahmen gemäß den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
    - Zusammenspiel mit anderen Prüf- beziehungsweise Kontrollinstanzen (zum Beispiel IT-Sicherheitsrevision)

Themenvorschlag 12:
Entwickeln Sie eine Vorgehensweise bei der Einführung einer automatisierten Datenverarbeitung anhand des Beispiels „elektronische Personalakte“. Im Rahmen der Projektarbeit sind besondere Gefährdungen zu analysieren und eine Schwachstellenanalyse aus datenschutzrechtlicher Sicht durchzuführen. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Gesetzliche Grundlagen
- Umfang der Nutzung •Mitwirkungsrechte beziehungsweise -pflichten
- Bewertung der Angemessenheit technischer und organisatorischer Maßnahmen zum Datenschutz
- Protokollierung und Löschung von Daten

Themenvorschlag 13:
Erstellen Sie eine Dienstanweisung zum datenschutzgerechten Löschen beziehungsweise zur Vernichtung von Datenträgern (zum Beispiel Papier, elektronische Daten/Datenträger). Gehen Sie hierbei auf etwaige Risiken ein und erläutern Sie die Lösungen. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Notwendigkeit der Dienstanweisung unter Beachtung der rechtlichen Anforderungen
- Technische und organisatorische Maßnahmen zum Datenschutz
- Einbeziehung externer Dienstleistender
- Hinweispflichten zur Protokollierung
- Zeigen Sie Schnittstellen zu anderen behördeninternen Dokumenten auf.

Themenvorschlag 14:
Definieren Sie die technischen und organisatorischen Maßnahmen eines selbst gewählten Beispielverfahrens Ihrer Behörde (zum Beispiel Video, Zutrittskontroll- oder Zeiterfassungssysteme, TK-Anlage, elektronische Personalakte) und bewerten Sie die Angemessenheit der technischen und organisatorischen Maßnahmen.
Die Projektarbeit sollte z.B. folgende Aspekte enthalten:

- Bewertung der Angemessenheit von Schutzmaßnahmen gemäß BSI IT-Grundschutz sowie anderer relevanter Standards
- Analyse besonderer Gefährdungen und Risiken aus datenschutzrechtlicher Sicht

Themenvorschlag 15:
Erstellen Sie eine Vorgehensweise zum Umgang mit Betroffenenrechten in Ihrer Behörde. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Rechtliche Grundlagen
- Überblick über den Umgang mit Betroffenenrechten
- Einbeziehung der/des Datenschutzbeauftragten beziehungsweise anderer relevanter Gremien (zum Beispiel Personalrat)
- Kommunikations- und Meldewege
- Dokumentation
- Umgang mit Anfragen der/des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen der Geltendmachung von Betroffenenrechten
- Folgen nicht ordnungsgemäßer Umsetzung von Betroffenenrechten

Themenvorschlag 16:
Erstellen Sie einen allgemeingültigen Prozess zum Umgang mit Datenschutzverstößen in Ihrer Behörde. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Rechtliche Grundlagen
- Überblick über den Umgang mit Datenschutzverstößen
- Einbeziehung der/des Datenschutzbeauftragten beziehungsweise anderer relevanter Gremien
- Kommunikations- und Meldewege innerhalb der Behörde
- Fehlermanagement
- Meldepflichten gegenüber Aufsichtsbehörden sowie Rechtsfolgen bei Nichtbeachtung etwaiger Meldepflichten
- Dokumentation des Datenschutzverstoßes

Themenvorschlag 17:
Identifizieren Sie für einen von Ihnen selbst gewählten Geschäftsprozess beziehungsweise ein Fachverfahren (zum Beispiel Arbeitszeiterfassung) vorhandene Risiken und definieren geeignete Maßnahmen. Gehen Sie dabei insbesondere auf den Schutzbedarf personenbezogener Daten ein. Dokumentieren Sie Ihre Ergebnisse und Vorgehensweise z.B. wie folgt:

- Identifikation und Dokumentation der zum Geschäftsprozess/Fachverfahren gehörenden Risiken in Bezug auf Informationen, Anwendungen und der vorliegenden Informationstechnik
- Definition der Schutzbedarfskategorien in Anlehnung an die Vorgaben des BSI- IT-Grundschutzes unter Beachtung typischer Schadensszenarien
- Definition geeigneter technischer und organisatorischer Maßnahmen

Themenvorschlag 18:
Stellen Sie wesentliche Grundlagen eines Zugriffs- und Berechtigungskonzepts im Rahmen der Einstellung, Versetzung oder des Ausscheidens von Beschäftigten in Ihrer Behörde dar. Erläutern Sie mögliche Risiken bei der Berechtigungsvergabe sowie beim Entzug von Berechtigungen. Die Projektarbeit sollte beispielsweise folgende Aspekte enthalten:

- Definition der Zielsetzung eines Berechtigungskonzepts
- Beschreibung wesentlicher Inhalte eines Berechtigungskonzepts
- Funktionstrennung („Vier-Augen-Prinzip“)
- Werkzeuge zur Berechtigungsverwaltung

- Applikationsspezifische Berechtigungsverwaltung
- Überprüfung der Berechtigungen
- Antrags- und Freigabeprozess
- Stellen Sie mögliche Risiken dar und gehen Sie auf angemessene technische und organisatorische Maßnahmen ein, die die Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten sicherstellen.

Hinweis:

Die positive Beurteilung einer Projektarbeit ersetzt nicht eine vollständige QS, ein (Zertifizierungs-)Audit oder sonstige genaue Überprüfungen des zugehörigen vollständigen Projektes.

7.3 Hinweise und Empfehlungen zur Durchführung und Betreuung der Projektarbeiten

Zielsetzung

- Sie sollen mit der Projektarbeit dokumentieren,
  - dass sie im Tätigkeitsbereich des behördlichen Datenschutzes selbstständig konzeptionell arbeiten und
  - die Arbeitsergebnisse dann überzeugend vermitteln, bzw. präsentieren können.

  Eine solche management- und kommunikationsorientierte Aufgabe ist wesentlicher Bestandteil im Aufgabenfeld eines/einer Datenschutzbeauftragten und im Bereich des operativen Datenschutzes.

  Nach der Benennung der fachlichen Begleitung für die Betreuung der Projektarbeit soll die Initiative bei der Erstellung der Projektarbeit immer von der Kandidatin bzw. dem Kandidat ausgehen. Die fachliche Begleitung sollte hinzugezogen werden, wenn fachliche Fragestellungen oder Unsicherheiten auftreten.

Inhalt

- Das Thema der Arbeit kann grundsätzlich frei gewählt werden. Es wird empfohlen, ein Thema aus den Vorschlägen dieses Lernpfades zu wählen. Wenn ein Thema aus diesem Lernpfad in Inhalt und Umfang geändert behandelt werden soll, muss dies im Projektplan dargestellt werden.
- Ob ein Thema für eine Projektarbeit akzeptiert werden kann, entscheidet die BAköV in Abstimmung mit dem BfDI nach Eingang des Projektplanes.
- Es empfiehlt sich, die Inhalte der geplanten Arbeit (auch nach Genehmigung des Projektes) am Anfang mit der fachlichen Begleitung abzustimmen. Insbesondere, wenn ein eigenes Thema gewählt wurde, sollte diese Abstimmung erfolgen. Bei den vorgegebenen Themen im Konzept sind Inhalte in Form von Unterpunkten z.T. schon näher spezifiziert.

Umfang

- Der minimale zeitliche Aufwand der Projektarbeit sollte bei etwa 20 Stunden liegen. Abhängig von der Komplexität des Themas und einer ggfs. vorhandenen Vorarbeit, auf der aufgesetzt wird, kann und darf der Gesamtaufwand höher sein.
- Im Einzelfall sind die Ressourcen (mit der fachlichen Begleitung) im Vorfeld abzuschätzen und evtl. zu prüfen, ob der Aufwand (auch für die fachliche Begleitung) vertretbar ist.

- Für die Aufwendungen der fachlichen Begleitung ist etwa ein Personentag vorgesehen (ohne Teilnahme an der Abschlusspräsentation). Es erscheint sinnvoll, ca. zwei Stunden in die Planung und Abstimmung der Inhalte am Anfang zu investieren. Die weitere Zeit sollte für Rückfragen bzw. Abnahme der Arbeit aufgewendet werden.
- In dem zeitlich begrenzten Rahmen einer solchen Arbeit können nicht immer alle Aspekte eines Themas vollständig bearbeitet werden. In einem solchen Fall sollen nicht behandelte bzw. tangierende Aspekte aufgeführt werden.

Aufbau der Arbeit (ca. 5 bis 10 Seiten, ohne Deckblatt und Verzeichnisse)

1. Anliegen / Einleitung (knappe Beschreibung)
   z. B. Einordnung der Arbeit in den behördlichen Datenschutz; Anlass für die Wahl des Themas; Vorgehensweise bei der Bearbeitung
2. Gliederung
3. Text, Abbildungen, Übersichten etc.
4. Zusammenfassung
5. Nachweise, Literatur
6. Eidesstattliche Erklärung

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Arbeit tatsächlich, eigenverantwortlich und nur unter Zuhilfenahme der ausgewiesenen Hilfsmittel angefertigt habe. [Ort], den [Datum] [Unterschrift] Vorname Name

Inhalt des Deckblattes

- Name, Vorname
- Behörde
- Thema
- fachliche Begleitung (Nennung nur mit Zustimmung)
- Zeitraum der Anfertigung

Umfang

ca. 5 - 10 Seiten (exklusive Deckblatt, Inhaltsverzeichnis usw.) - Schrift 12 pt (z. B. Times New Roman, Arial)

Termine

- Nach der Anmeldung zur Fortbildung ist eine baldige Entscheidung für ein Thema zu treffen.
- Besprechung der Arbeit mit der fachlichen Begleitung.
- Vorlage der Arbeit spätestens 3 Wochen vor der Projektpräsentation bei der BAköV. Eine elektronische Abgabe ist möglich.
- Vorbereitung der Präsentation und wenn erforderlich Unterlagen für die anderen Teilnehmenden. Achtung die Präsentationszeit beträgt 20 Minuten. Eine zeitliche Überziehung oder eine deutliche Unterschreitung sind zu vermeiden.

7.4 Empfehlungen zur Vorbereitung der Präsentation

Im Rahmen eines Präsentationsworkshops wird die Projektarbeit vorgestellt. An diesem Erfahrungsaustausch nehmen weitere Kandidatinnen und Kandidaten teil, welche die Projektarbeit abgeschlossen haben. Neben der Präsentation und dem Gespräch wird damit eine Plattform für den weiteren Erfahrungsaustausch geöffnet.
Die Projektarbeit wird in einer 20minütigen Präsentation vorgestellt. Zusätzlich sind 10 Minuten für das Gespräch vorgesehen. Eine wesentliche Aufgabe bei der Präsentation besteht darin, die zentralen und wesentlichen Arbeitsergebnisse der Zuhörerschaft überzeugend zu vermitteln.

Die Darstellung sollte sich an folgenden Inhalten orientieren:

- Erläuterung der Projektarbeit und Einordnung in die Agenda/Leitlinie der Behörde.
- Darlegung der Vorgehensweise (fachliches Vorgehen; Absprachen etc.).
- Zusammenfassung der Ergebnisse und wichtige Erfahrungen für die weitere Arbeit.
- Als Modellfall kann man sich z.B. vorstellen, dass man die Aufgabe hat, seiner Behördenleitung in zwanzig Minuten einen Datenschutzaspekt überzeugend darzustellen, um eine Entscheidung herbeizuführen. (Nicht empfehlenswert wären z.B. weitschweifige oder zu technische Darstellungen in dieser kurzen Zeit.)

Mit der Präsentation und dem Gespräch wird fachliches Wissen, der Lernerfolg und Fähigkeit der Einordnung in die Gesamttätigkeit aufgezeigt.

Hinweise für Präsentationen
Im Rahmen Ihrer Tätigkeit ist immer wieder eine Präsentation von Vorhaben oder Ergebnissen erforderlich. Es empfiehlt sich, für die Präsentation elektronische Medien zu nutzen. Folgende Hinweise haben sich bewährt:

Titel*	**Text**	**Aufzählungstext**
Folientitel auf eine Zeile beschränken	alle Texte sauber formatieren	maximal sechs Aufzählungen pro Folie
Folientitel treffend zum Inhalt wählen	nur Abkürzungen verwenden, die die Zuhörer kennen	je Aufzählungspunkt maximal zwei Zeilen
jeder Folie ihren eigenen aussagekräftigen Titel geben	eine serifenlose Schrift verwenden (20 pt, Überschriften 32 pt, Tabellen 16 pt)	kurze und klare Formulierungen der Aufzählungspunkte mit Hilfe von Verben
auf einen einheitlichen Sprachstil achten	kein Blocksatz, keine Silbentrennung	unnötige Substantive vermeiden

Bilder/Grafiken	**Layout**	**Gliederung**
auf erklärende Funktion achten, keine Dekoration	klare Strukturen schaffen	wiederkehrende Symbole verwenden (Pfeile, Häkchen --)
mit der Farbauswahl harmonisieren	Verwirrendes entfernen oder anpassen	nicht mehr als zwei Gliederungsebenen nutzen
einheitlichen Stil beachten	wichtige Elemente hervorheben	Schrittfolgen deutlich nummerieren
Überzeugungskraft überprüfen	zusammengehörige Elemente gleich gestalten	alle Texte ausreichend gliedern

Die Präsentation bzw. Grundthesen werden an die Teilnehmenden der Veranstaltung weitergegeben. Bei allen Inhalten sind das Urheberrecht und die Barrierefreiheit zu beachten.

* Die vorstehende Übersicht wurde mit freundlicher Genehmigung entnommen: Grundwald, Stefan; Freitag, Thoralf; Witt-Schleuer, Detlef: Zertifizierung im IT-Weiterbildungssystem. Hannover 2005, S. 127

7.5 Formulare (werden von der BAköV noch ergänzt)

Plan der Projektarbeit

Änderungs-/Ergänzungsmitteilung

Antrag: Zertifikatsverlängerung