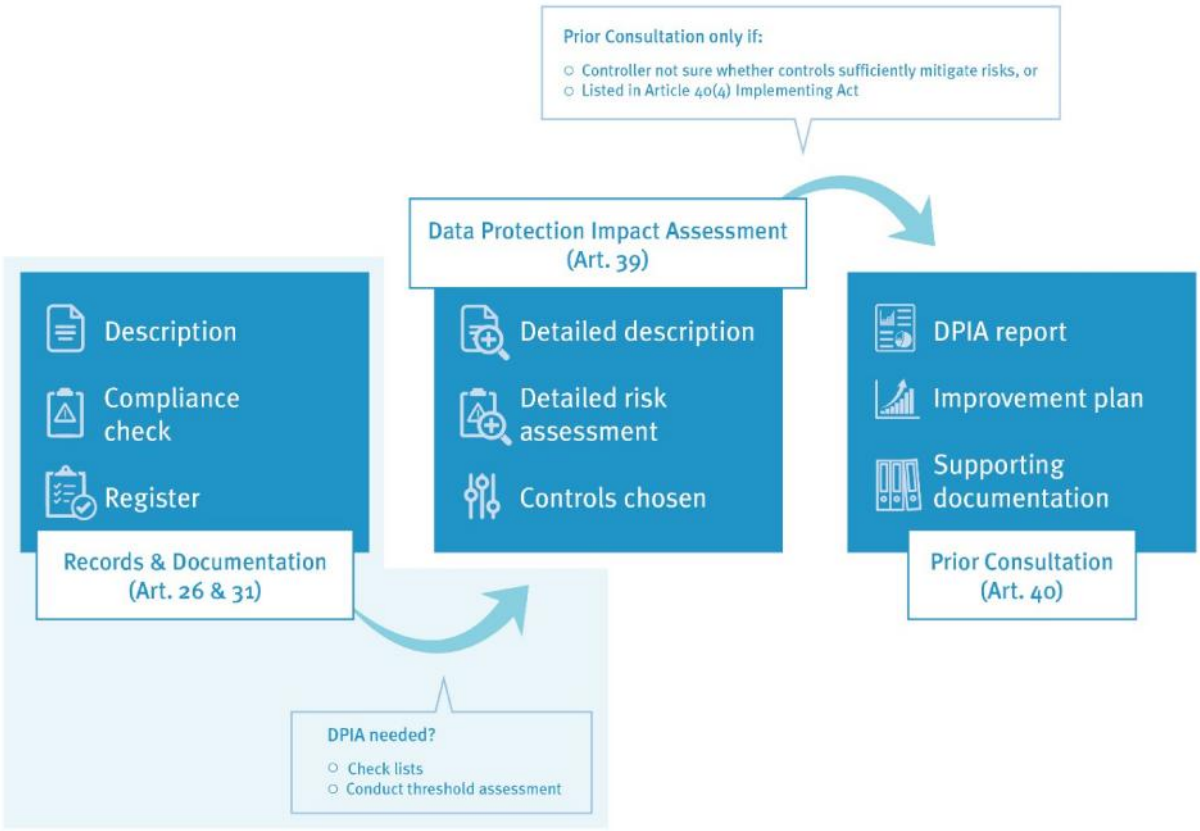
DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE (EDSB)

# Rechenschaftspflicht in der Praxis Teil I: Verzeichnisse, Register und Erfordernis einer Datenschutz-Folgenabschätzung


v1.3 Juli 2019




| | |
|---|---|
| Prior Consultation only if: | Vorherige Konsultation nur, wenn: |
| Controller not sure whether controls sufficiently mitigate risks, or<br>Listed in Article 40 (4) Implementing Act | Verantwortlicher nicht sicher, ob Kontrollmaßnahmen ausreichen, oder<br>im Durchführungsrechtsakt gemäß Artikel 40 Absatz 4 aufgelisteter Fall |
| Data Protection Impact Assessment (Art. 39) | Datenschutz-Folgenabschätzung (Artikel 39) |
| Description | Beschreibung |
| Compliance check | Compliance-Kontrolle |
| Register | Registrierung |
| Records & Documentation (Art. 26 &31) | Verzeichnisse und Dokumentierung (Artikel 26 und 31) |
| Detailed description | Ausführliche Beschreibung |
| Detailed risk assessment | Ausführliche Risikobewertung |
| Controls chosen | Ausgewählte Maßnahmen |
| DPIA report | DSFA-Bericht |
| Improvement plan | Verbesserungsplan |
| Supporting documentation | Dazugehörige Unterlagen |
| Prior Consultation (Art. 40) | Vorherige Konsultation (Artikel 40) |
| DPIA needed? | DSFA erforderlich? |
| Check lists | Checklisten |
| Conduct threshold assessment | Schwellenwertanalyse durchführen |

## Inhaltsverzeichnis



## Abbildungsverzeichnis

# 1. Einleitung und Gegenstand von Teil I

Als die für einen Prozess im Geschäftsbereich zuständige Person sind Sie der Durchführungsverantwortliche aufseiten des für die Verarbeitung Verantwortlichen und damit zur Führung von „Verzeichnissen“ verpflichtet (Artikel 31 der Verordnung (EU) 2018/1725; im Folgenden: Verordnung[1]), und zwar jeweils ein Verzeichnis für jeden personenbezogene Daten betreffenden Verarbeitungsvorgang Ihrer EU-Institution. Das bedeutet, dass Sie zum Beispiel ein „Verzeichnis“ für Auswahl- und Rekrutierungsverfahren führen müssen und ein weiteres für Verfahren im Zusammenhang mit der Bekämpfung von Mobbing.

Teil I des Toolkits zeigt, wie Sie diese Verzeichnisse und die dazugehörigen Unterlagen erstellen. Es wird auch gezeigt, wie man entscheidet, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist.

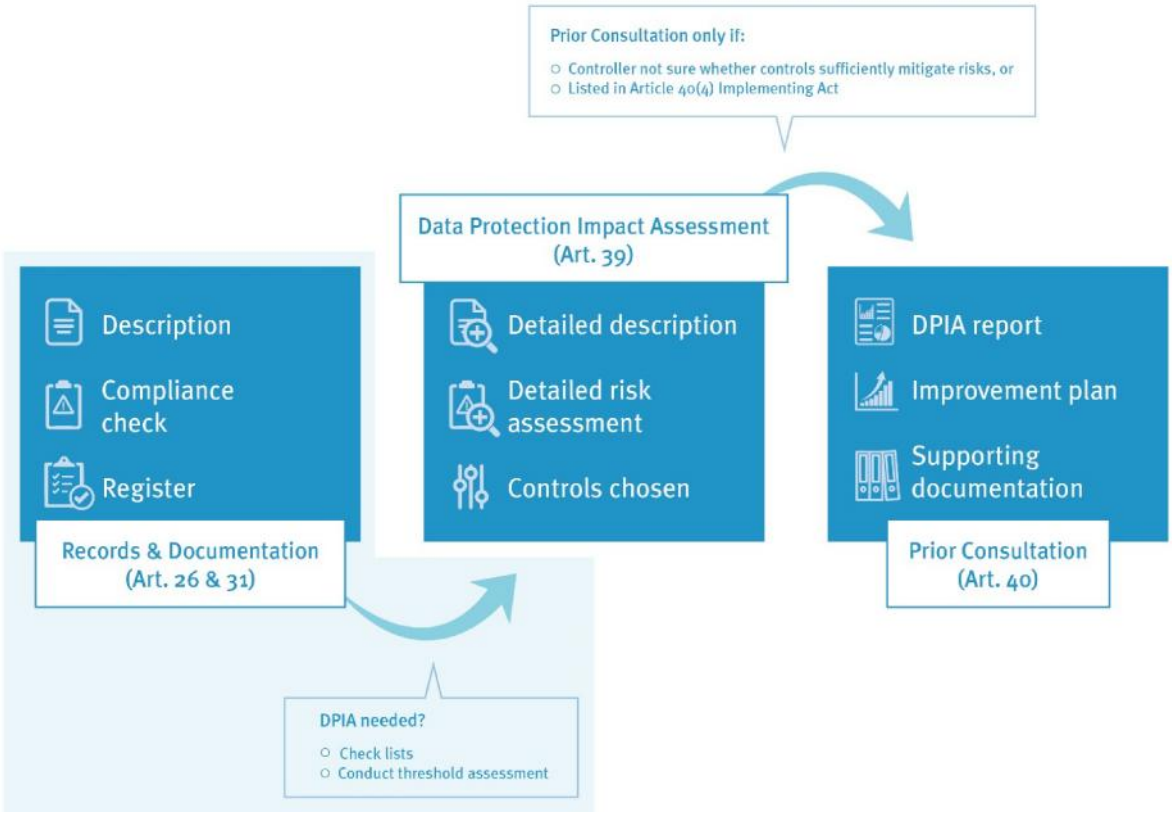



Abbildung 1: Gegenstand von Teil I

Dieser Teil gibt Orientierung darüber, wie man die Anforderungen, die die Verordnung an die Entwicklung neuer Geschäftsprozesse (in der Datenschutzterminologie: „Verarbeitungstätigkeiten“) stellt, erfüllt und die erforderliche Datenschutzdokumentation erstellt. Teil I behandelt folgende Aspekte, wobei es für die meisten dieser Aspekte auch Vorlagen gibt:

- wie man die eigenen Verarbeitungstätigkeiten dokumentiert;
- wem dabei welche Aufgaben zukommen;
- wie man feststellt, ob eine DSFA erforderlich ist;

[1] ABl. L 295/39 vom 21.11.2018.

- Verzeichnisse betreffende Vorschriften für den Übergang von der alten zur neuen Datenschutzverordnung für die EU-Institutionen.

Folgende Themen werden in Teil II behandelt:

- wie man DSFA durchführt;
- in welchen Fällen die Datenschutz-Folgenabschätzung dem Europäischen Datenschutzbeauftragten (EDSB) im Zuge der vorherigen Konsultation zuzusenden ist.

## 2. Verantwortlichkeiten – wer macht was?

Rechenschaftspflicht bedeutet, dass der für die Verarbeitung Verantwortliche dafür zuständig ist, sicherzustellen, dass alle Vorschriften eingehalten werden und die Vorschriftseinhaltung auch nachgewiesen werden kann. Im Falle der EU-Institutionen ist der für die Verarbeitung Verantwortliche in rechtlicher Hinsicht „das Organ oder die Einrichtung der Union oder die Generaldirektion oder sonstige Organisationseinheit, das beziehungsweise die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten bestimmt“[2]. In der Praxis liegt **die Rechenschaftspflicht für die Vorschriftseinhaltung bei der obersten Verwaltungsebene, wobei jedoch die Durchführungsverantwortung in der Regel auf einer niedrigeren Ebene liegt** („Durchführungsverantwortlicher aufseiten des für die Verarbeitung Verantwortlichen“ / „in der Praxis Verantwortlicher“). Vielfach wird es die im Geschäftsbereich zuständige Person sein, die der Durchführungsverantwortliche ist. **Als die für einen Prozess im Geschäftsbereich zuständige Person sind Sie die Person, die in erster Linie für die Compliance zuständig ist, wobei Ihnen der Datenschutzbeauftragte (DSB) assistiert** (und auch der Datenschutzkoordinator (DPK), falls Ihre EU-Institution einen solchen hat)[3].

Das **Führen angemessener Verzeichnisse ist Aufgabe des Verantwortlichen** (in der Praxis: Rechenschaftspflicht bei der obersten Verwaltungsebene, Durchführungsverantwortung bei der im Geschäftsbereich zuständigen Person)[4]. Der EDSB empfiehlt den EU-Institutionen dringend, ihre Verzeichnisse in einem **zentralen, vom DSB geführten, öffentlich zugänglichen Register** zu führen[5]. Die Rechenschaftspflicht für die Erstellung der Verzeichnisse und für deren Inhalt liegt beim Verantwortlichen. Bei der Erstellung der Verzeichnisse und dazugehörigen Unterlagen kann der DSB Ihnen helfen; es ist jedoch eine von Ihnen wahrzunehmende Aufgabe. Auch für die Prüfung, ob eine DSFA erforderlich ist, sind Sie als die im Geschäftsbereich zuständige Person verantwortlich – der DSB kann Ihnen dabei helfen, aber es ist Ihre Aufgabe, diese Prüfung vorzunehmen.

Die nachstehende RACI-Matrix[6] gibt einen Kurzüberblick über die verschiedenen Verantwortlichkeiten[7] bezüglich der Verzeichnisse. Bitte beachten Sie, dass dies ein

---

[2] Artikel 3 Absatz 1 Nummer 8 der neuen Verordnung.

[3] Es kann vorkommen, dass die im Geschäftsbereich zuständige Person auf Input von anderen angewiesen ist; zum Beispiel der Leiter einer Geschäftseinheit, für den die IT-Abteilung eine Anwendung entwickelt. Auch wenn die im Geschäftsbereich zuständige Person viele Informationen bei der IT-Abteilung einholen muss, liegt die Verantwortung für das System doch bei der im Geschäftsbereich zuständigen Person.

[4] Artikel 26 und 31 der Verordnung.

[5] Siehe auch die nachstehenden Abschnitte 3.3 und 3.5.

[6] RACI steht für „*responsible* (für die Durchführung verantwortlich), *accountable* (rechenschaftspflichtig), *consulted* (konsultiert), *informed* (informiert)“. Die RACI-Matrix bietet eine übersichtliche Darstellung der Verteilung von Aufgaben und Verantwortlichkeiten.

[7] „(Für die Durchführung) verantwortlich“ ist, wer verpflichtet ist, Handlungen vorzunehmen und Entscheidungen zu treffen, um vorgegebene Ergebnisse zu erzielen; „rechenschaftspflichtig“ ist, wer für Handlungen,

allgemeiner Überblick ist – je nachdem, um welche Verarbeitungsvorgänge es geht, müssen Sie unter Umständen weitere Teams einbeziehen, zum Beispiel das Rechtsreferat oder den Rechtsdienst Ihrer EU-Institution.

| | Verantwortlich | Rechenschaftspflichtig | Konsultiert | Informiert |
|---|---|---|---|---|
| Oberste Verwaltungsebene | | X | | |
| Im Geschäftsbereich zuständige Person | X | | | |
| DSB | | | X | |
| IT-Abteilung | | | X | |
| ggf. Auftragsverarbeiter | | | X | |

Abbildung 2: RACI-Matrix zum Prozess für Verzeichnisse/Unterlagen

Die oberste Verwaltungsebene ist dafür rechenschaftspflichtig, dass die Datenschutzvorschriften eingehalten werden. In der Praxis sind es jedoch zumeist die im Geschäftsbereich für bestimmte Prozesse Zuständigen, die den Hauptteil der Arbeit erledigen. Die im Geschäftsbereich zuständige Person muss unter Umständen andere Stellen hinzuziehen, sowohl interne (z. B. die IT-Abteilung) als auch externe (z. B. Auftragsverarbeiter oder Informationslieferanten); diese Stellen müssen konsultiert werden und erforderlichenfalls ihren Input liefern. In den meisten Fällen wird Ihre IT-Abteilung die technische Infrastruktur bereitstellen; sie wird sich auch am besten mit den die Informationssicherheit betreffenden Aspekten auskennen.

Last, not least, sollten Sie während des gesamten Verfahrens Ihren Datenschutzbeauftragten konsultieren, da er in Ihrer EU-Institution die zentrale Stelle für Datenschutzwissen ist. **Ihr behördlicher Datenschutzbeauftragter (DSB) kann bei Ihnen allem zur Seite stehen – wobei allerdings Verantwortung und Rechenschaftspflicht letztendlich beim Verantwortlichen liegen –** die DSB sind dazu da, den für die Verarbeitung Verantwortlichen bei ihrer Arbeit zu helfen, nicht jedoch dazu, die Arbeit für sie zu erledigen. Anhang 1 gibt für die in diesem Toolkit behandelten Schritte einen Überblick darüber, was von wem zu erledigen ist.

# 3. Dokumentierung Ihrer Verarbeitungsvorgänge

## 3.1 Was ist unter Verzeichnissen zu verstehen?

**Ihre Verarbeitungsvorgänge müssen Sie in „Verzeichnissen" dokumentieren. Falls Sie für bereits bestehende Verarbeitungsvorgänge Meldungen gemäß Artikel 25 der alten Verordnung vorgenommen haben, können Sie diese als Grundlage für Ihre Verzeichnisse verwenden.**

Entscheidungen und Erfolg einstehen muss; „konsultiert" ist, wer um Beiträge und Stellungnahmen gebeten wird; „informiert" ist, wer über die getroffenen Entscheidungen und das Verfahren auf dem Laufenden gehalten wird.

Als Durchführungsverantwortlicher aufseiten des für die Verarbeitung Verantwortlichen **müssen Sie für alle Ihre Verarbeitungstätigkeiten, die personenbezogene Daten betreffen, Verzeichnisse erstellen** – für die Newsletter Ihrer EU-Institution genauso wie für die Verarbeitungstätigkeiten im Zusammenhang mit der Personalauswahl, den Hauptaufgaben Ihrer Behörde, Verwaltungsuntersuchungen und Disziplinarverfahren. Verzeichnisse enthalten grundlegende Angaben zu den Verarbeitungsvorgängen: Wer ist verantwortlich? Was bezweckt die Verarbeitung? Welche Daten verarbeiten wir über welche Personen? Sie bilden die Grundlage Ihrer Datenschutzdokumentation und zählen zu dem, was sich der EDSB, wenn es um die Beurteilung Ihrer Einhaltung der Datenschutzvorschriften geht, als erstes ansieht.

Wenn es um ein neues Projekt geht, das noch nicht so weit vorangekommen ist, dass man schon ein Verzeichnis erstellen könnte, ist es **immer eine gute Idee, mit Ihrem Datenschutzbeauftragten zu sprechen**. Je früher Sie erkennen, dass Aspekte Ihrer geplanten Verarbeitungsvorgänge problematisch sind, desto leichter können Sie die Probleme beheben.

**Verzeichnisse sind nichts Neues:** Auch nach Artikel 25 der alten Verordnung (EG) 45/2001 waren Meldungen ähnlichen Inhalts an Ihren behördlichen Datenschutzbeauftragten vorgeschrieben. Sie können diese auch für die Erstellung Ihrer Verzeichnisse wiederverwenden. Die Angaben in den Verzeichnissen sind denen in den Datenschutzhinweisen / Datenschutzerklärungen, mit denen betroffene Personen über Ihre Verarbeitungsvorgänge informiert werden, sehr ähnlich. Die **Wiederverwendung der alten Texte** ist möglich.

In **Artikel 31 der neuen Verordnung** sind sämtliche Angaben aufgeführt, die das Verzeichnis enthalten muss:

a) Namen und Kontaktdaten des Verantwortlichen für die Verarbeitung (ggf. einschließlich der gemeinsam mit ihm Verantwortlichen), des Datenschutzbeauftragten und gegebenenfalls der Auftragsverarbeiter
*Wer ist zuständig? An wen können sich die Betroffenen wenden? Benutzen Sie funktionale Postfächer, nicht die persönlichen Postfächer der im Geschäftsbereich zuständigen Person und des Datenschutzbeauftragten (dies ist besser für die Geschäftskontinuität und lässt sich leichter aktualisieren)*[8]*. Schließlich ist es die Rolle in der Organisation, auf die es ankommt, nicht die Person, die diese Rolle gerade innehat. Wenn Sie personenbezogene Daten von einem Auftragsverarbeiter / Auftragnehmer verarbeiten, ist das anzugeben (z. B. bei IT-Dienstleistungen oder vor der Anstellung erfolgende Gesundheitsprüfungen, die extern erledigt werden); wenn Sie und eine andere EU-Institution oder eine andere Organisation gemeinsam Verantwortliche sind, ist das anzugeben (z. B. wenn zwei EU-Institutionen einen medizinischen Dienst gemeinsam nutzen).*

[8] In Artikel 31 der Verordnung ist hier vom „Namen" des Datenschutzbeauftragten die Rede, in den Artikeln 15 und 16 (wo es um die Pflicht zur Information betroffener Person geht) nur von den Kontaktdaten. Der Europäische Datenschutzbeauftragte ist der Ansicht, dass es hier nicht erforderlich ist, den Namen der natürlichen Person, die gerade der behördliche Datenschutzbeauftragte der jeweiligen EU-Institution ist, anzugeben – worauf es ankommt, ist, dass es für die betroffenen Personen eine Kontaktstelle in der Organisation gibt.

b) Zweck der Verarbeitung;
*Wozu erfolgt die Verarbeitung? Hier ist kurz anzugeben, was mit der Verarbeitung personenbezogener Daten erreicht werden soll; wenn Sie sich auf eine bestimmte Rechtsgrundlage stützen, ist diese ebenfalls anzugeben (z. B. im Falle von Verfahren, die Personalangelegenheiten betreffen, das Statut; die Ihrer EU-Institution durch das Unionsrecht zugewiesenen Aufgaben).*

c) Beschreibung der Kategorien betroffener Personen und der Daten über diese Personen, um deren Verarbeitung es geht;

*Wer ist betroffen? Welche Daten über diese Personen werden gespeichert? Wenn es verschiedene Datenkategorien für verschiedene Personenkategorien gibt, ist das zu erklären (im Falle von Ermittlungen z. B. Beschuldigte im Gegensatz zu Zeugen).*

d) die Kategorien von Empfängern, gegenüber denen die Daten offengelegt werden;

*Wer wird Zugang zu diesen Informationen haben (sowohl intern als auch extern)? Wer hat Zugang zu welchen Teilen der Daten? Anmerkung: Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags möglicherweise personenbezogene Daten erhalten (z. B. OLAF, EO, EDSB), brauchen nicht als Empfänger angegeben werden*[9].

e) Übermittlungen an ein Drittland oder an eine internationale Organisation unter Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie Dokumentierung geeigneter Garantien für die Übermittlung;

*Falls Sie Daten an solche Stellen übermitteln: Wer sind diese Stellen und wie stellen Sie sicher, dass diese Stellen die Daten rechtmäßig und nach Treu und Glauben verarbeiten (z. B. Auftragsverarbeiter im Drittland verwendet Standardvertragsklauseln)?*

f) die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

*Wie lange bewahren Sie die Informationen auf, ab wann läuft diese Frist? Geben Sie Ihre administrative Speicherungsfrist einschließlich Fristbeginn an; erforderlichenfalls ist zwischen verschiedenen Datenkategorien oder Personenkategorien zu differenzieren (z. B. beim Auswahlverfahren: Bewerber, die es auf die Reserveliste geschafft haben, und solche, die es nicht geschafft haben).*

g) wenn möglich, eine allgemeine Beschreibung der getroffenen Sicherheitsvorkehrungen.

*Welche Angaben dürfen Sie dazu machen, wie Sie die verarbeiteten Daten sichern? Hier geht es nicht um detaillierte Angaben zu Ihren Maßnahmen auf dem Gebiet der Informationssicherheit, sondern lediglich darum, eine allgemeine Beschreibung zu geben, die die Wirksamkeit der getroffenen Maßnahmen nicht beeinträchtigt.*

Im ersten Teil des **Formulars in Anhang 2**, in dem diese Punkte aufgeführt sind, sind auch Ausfüllanweisungen und ein Beispiel für ein Verzeichnis zu finden. Nur dieser erste Teil mit den **in Artikel 31 der neuen Verordnung aufgeführten Angaben unterliegt dem Öffentlichkeitserfordernis**, auf das nachstehend im Abschnitt 3.5 eingegangen wird.

[9] Siehe Artikel 3 Absatz 1 Nummer 13 der Verordnung; Näheres zu den entsprechenden Vorschriften der DSGVO ist Erwägungsgrund 31 der DSGVO zu entnehmen.

## 3.2 Vorschriftseinhaltung und Risikoprüfung

**Wenn Sie Ihre Verzeichnisse erstellen, sollten Sie die Gelegenheit nutzen, auch zu überprüfen, dass Ihr Verarbeitungsvorgang den Datenschutzvorschriften genügt. Sie müssen diese Vorschriften einhalten und die Vorschriftseinhaltung nachweisen können.**

Die Verzeichniserstellung ist ein **guter Zeitpunkt für die Überprüfung**, dass die Datenschutzvorschriften im Wesentlichen eingehalten werden, wofür die Verantwortlichen rechenschaftspflichtig sind. Die Verantwortlichen müssen Prozesse so gestalten, dass die Einhaltung der Vorschriften sichergestellt ist (siehe Artikel 4 Absatz 2 und 26 der Verordnung).

Der zweite Teil des Formulars im Anhang 2 enthält eine **kurze Checkliste** für die wichtigsten Vorschriften. Sie müssen die Verordnung einhalten und deren Einhaltung auch nachweisen können, wobei die durch die Verarbeitungsvorgänge verursachten Risiken zu berücksichtigen sind (Artikel 26 und Erwägungsgrund 38 der Verordnung). Dieses **Risikobewusstsein** ist eine der entscheidenden Änderungen gegenüber den alten Vorschriften: Sie müssen stets darüber nachdenken, wie sich die Verarbeitung auf diejenigen auswirken könnte, deren Daten Sie verarbeiten. Welche Auswirkung hat die Verarbeitung auf diese Personen? Werden die Personen dadurch beeinträchtigt? Diese Überlegungen sind sowohl für die planmäßige Verarbeitung als auch für den Fall, dass die Verarbeitung nicht ordnungsgemäß erfolgt, anzustellen. Dafür kann die Checkliste nützlich sein. Auch wenn sie nicht formell Teil des Verzeichnisses ist, zeigt sie doch, dass Sie die für den Datenschutz relevanten Auswirkungen der Verarbeitung bedacht haben.

Hier geht es um zwei grundlegende Aspekte: „Ist diese Verarbeitung rechtmäßig?“ und „Halten wir die Datenschutzgrundsätze ein?“ Die Vorlage in Anhang 2 enthält Ausfüllhinweise; genauere Angaben zum rechtlichen Hintergrund sind in Anhang 3 zu finden. Wenn Sie diese Compliance-Aspekte schon beim Erstellen und Dokumentieren der Verzeichnisse prüfen, wird Ihnen das die Vorschriftseinhaltung und deren Nachweise erleichtern („Rechenschaftspflicht“ in Artikel 4 Absatz 2).[10] Was die die Informationssicherheit betreffenden Aspekte der Datenschutz-Compliance angeht, ist sicherzustellen, dass Sie einen ordnungsgemäßen Prozess für das Informationssicherheits-Risikomanagement haben und Risikomanagementmaßnahmen vorsehen, die den durch die Verarbeitungsvorgänge verursachten Risiken angemessen sind.[11]

Am Ende der Compliance-Checkliste finden Sie auch einige Fragen, die Ihnen helfen festzustellen, ob Ihre Verarbeitungsvorgänge möglicherweise hohe Risiken bergen und deshalb eingehenderer Prüfung bedürfen. Sollten Sie eines dieser Kästchen angekreuzt haben, ist mit Ihrem Datenschutzbeauftragten Rücksprache zu nehmen – unter Umständen müssen Sie eine Datenschutz-Folgenabschätzung durchführen. Nähere Informationen zu Datenschutz-Folgenabschätzungen finden Sie in Teil II dieses Toolkits.

---

[10] Der Logik nach kommt erst die Compliance-Kontrolle und dann das Verzeichnis: Falls Sie feststellen, dass bestimmte Verarbeitungsvorgänge nicht rechtmäßig ausgeführt werden können, müssen Sie das Projekt aufgeben, in welchem Falle kein Verzeichnis erforderlich ist. In der Praxis ist es aber sinnvoll, das Verzeichnis vor der Compliance-Kontrolle zu erstellen: Es erleichtert die Lesbarkeit, wenn Sie erst beschreiben, was Sie tun (oder zu tun planen), und dann, warum Sie gerade auf diese Weise vorgehen und wie Sie sicherstellen, dass alle einschlägigen Vorschriften eingehalten werden.

[11] Genauere Angaben dazu sind einer Veröffentlichung des EDSB (Leitlinien für Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten (https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en)) sowie dem Rahmen für das Informationssicherheits-Risikomanagement (ISRM) Ihrer EU-Institution zu entnehmen.

## 3.3 Überprüfung der Verzeichnisse

**Es ist sicherzustellen, dass die Verzeichnisse stets die aktuellen Gegebenheiten der Verarbeitungsvorgänge widerspiegeln, auf die sie sich beziehen.**

Ihre Verzeichnisse müssen die Verarbeitungsvorgänge Ihrer EU-Institution realistisch wiedergeben. Sie müssen also **sicherstellen, dass die Verzeichnisse stets auf dem aktuellen Stand sind**. Wenn Sie Änderungen Ihrer Verarbeitungsvorgänge planen, ist zu prüfen, ob die Verzeichnisse aktualisiert werden müssen. Es ist sinnvoll, **diese Prüfung förmlich in Ihren Prozess für das Änderungsmanagement aufzunehmen**. Auch regelmäßige Überprüfungen, die unabhängig von geplanten Änderungen erfolgen, können sinnvoll sein, um bisher übersehene Veränderungen zu berücksichtigen.

## 3.4 Verzeichnisregister

Ihre EU-Institution muss diese Verzeichnisse schriftlich führen (was auch in einem elektronische Format erfolgen kann – Artikel 31 Absatz 3 der Verordnung) und auf Anfrage dem Europäischen Datenschutzbeauftragten zur Verfügung stellen (Artikel 31 Absatz 4). Artikel 31 Absatz 5 bestimmt, dass „die Organe und Einrichtungen der Union … ihre Verzeichnisse der Verarbeitungen in einem zentralen Register [führen], es sei denn, dies ist unter Berücksichtigung der Größe des Organs oder der Einrichtung der Union nicht sachgerecht."

**Der EDSB empfiehlt den EU-Institutionen dringend, ihre Verzeichnisse in einem zentralen, vom behördlichen Datenschutzbeauftragten geführten Register zu führen.**

Nach der alten Verordnung führten die EU-Institutionen ein zentrales Register. Aus praktischen Gründen spricht vieles dafür, diese Praxis beizubehalten:

- Das Register gibt einen schnellen Überblick über die Verarbeitungsvorgänge Ihrer Organisation, so dass diese Kontrolle darüber hat, was bei ihr geschieht;
- es erleichtert die Beantwortung von Verzeichnisse betreffenden Anfragen, sei es des EDSB oder anderer Interessenträger;
- es erleichtert Vergleiche zwischen Ihren Verzeichnisse, was wiederum die Qualitätskontrolle Ihrer Aufzeichnungen erleichtert;
- es hilft Ihrem Datenschutzbeauftragten bei seiner Aufgabe, die interne Anwendung der Verordnung sicherzustellen;
- es ist für Sie einfacher, herauszufinden, wie vergleichbare Verarbeitungsvorgänge in Ihrer Organisation bisher dokumentiert wurden, was wiederum die Verzeichniserstellung vereinfacht.

Der EDSB empfiehlt, diese Register von den Datenschutzbeauftragten der EU-Institutionen führen zu lassen, und zwar aus den folgenden Gründen:

- Der behördliche Datenschutzbeauftragte ist die zentrale Stelle für Datenschutzwissen – d. h. die erste Anlaufstelle, wenn Sie Fragen zur Einhaltung der Datenschutzvorschriften haben; wenn er alle Verzeichnisse zur Hand hat, wird er Ihre Fragen viel besser beantworten können.
- Wenn der behördliche Datenschutzbeauftragte einen Überblick über die Verarbeitungsvorgänge der Organisation hat, kann er besser beraten (z. B. dazu, wie andere Teile der Organisation ähnliche Angelegenheiten behandeln).

- Das Register gemäß Artikel 25 der alten Verordnung (EU) 45/2001, das dem Register gemäß Artikel 31 Absatz 5 der Verordnung in funktioneller Hinsicht entsprach, wurde vom behördlichen Datenschutzbeauftragten geführt. Wird diese Praxis beibehalten, sind weniger organisatorische Änderungen erforderlich.

Allerdings ist zu beachten, **dass auch wenn es der behördliche Datenschutzbeauftragte ist, von dem das Verzeichnisregister *geführt* wird, die Verantwortung für den *Inhalt* der Verzeichnisse doch weiterhin bei der EU-Institution als dem Verantwortlichen liegt (und damit bei Ihnen als dem Durchführungsverantwortlichen aufseiten des für die Verarbeitung Verantwortlichen)**.

Was die alten Vorschriften angeht, wurde von uns empfohlen, dass die behördlichen Datenschutzbeauftragten geplante Verarbeitungsvorgänge, die noch nicht so weit fortgeschritten waren, dass eine volle Meldung nach Artikel 25 (der Vorläufer zu den Verzeichnissen) erforderlich wäre, in einem „Inventar“ führen. An dieser Empfehlung halten wir fest, da ein solches „Inventar“ ein nützliches Planungsinstrument sein kann.

### 3.5 Öffentliche Zugänglichkeit der Verzeichnisse

Verzeichnisse sind ein wichtiges Instrument, wenn es darum geht, zu prüfen und zu dokumentieren, dass Ihre Organisation ihre Verarbeitungstätigkeiten unter Kontrolle hat. Gemäß Artikel 31 Absatz 5 der Verordnung machen die EU-Institution ihre Register öffentlich zugänglich.

**EU-Institutionen sind verpflichtet, Verzeichnisse im Sinne von Artikel 31 öffentlich zugänglich zu machen, vorzugsweise durch Veröffentlichung im Internet. Die Praxis, der viele EU-Institutionen für ihre Meldungen gemäß Artikel 25 der alten Verordnung folgten, wird damit fortgesetzt.**

Diese Veröffentlichung hat viele Vorteile, weil sie:

- zur Transparenz der EU-Institutionen[12] beiträgt;
- das Vertrauen der Öffentlichkeit stärkt;
- den Wissensaustausch unter den EU-Institutionen erleichtert.

**Bitte beachten Sie, dass dieses Öffentlichkeitserfordernis nur für Artikel-31-Verzeichnisse im strengen Sinne gilt (also nur für die in Artikel 31 Absatz 1 der neuen Verordnung aufgelisteten Punkte) und nicht für sonstige Dokumentationen, die Ihre EU-Institution haben mag.** Die Vorlage in Anhang 2 ist in mehrere Teile untergliedert, um es Ihnen einfacher zu machen, nur diejenigen Angaben zu veröffentlichen, zu deren Veröffentlichung Sie gemäß Artikel 31 verpflichtet sind.

## 4. Erforderlichkeit einer Datenschutz-Folgenabschätzung (DSFA)

### 4.1 Wann ist die DSFA-Durchführung zwingend vorgeschrieben?

Sie werden nicht für alle Verarbeitungsvorgänge eine DSFA durchführen müssen. Die Pflicht dazu besteht nur bei den Verarbeitungsvorgängen, die ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ bergen. Als Durchführungsverantwortlicher aufseiten des für

[12] Siehe auch Artikel 15 Absatz 1 AEUV.

die Verarbeitung Verantwortlichen ist die Durchführung der DSFA Ihre Aufgabe, bei der der behördliche Datenschutzbeauftragte Ihrer EU-Institution Ihnen Hilfe und Anleitung gibt.

**Eine DSFA ist durchzuführen, wenn Ihr Verarbeitungsvorgang mindestens eine der folgenden Voraussetzungen erfüllt:**

**(1) Er steht auf der vom EDSB herauszugebenden Liste der Arten riskanter Verarbeitungsvorgänge.**
**(2) Er hat nach Ihrer Schwellenwertanalyse voraussichtlich ein hohes Risiko zur Folge.**

Die neue Verordnung enthält mehrere nicht erschöpfende Listen, in denen Verarbeitungsvorgänge aufgeführt sind, bei denen eine DSFA erforderlich ist. Für die Fälle, die dort nicht aufgelistet sind, ist vorgesehen, dass Sie eine Abschätzung vornehmen. Um festzustellen, ob für Ihre geplanten Verarbeitungsvorgänge eine DSFA erforderlich ist, müssen Sie sich folgende Fragen stellen:

1. Ist der Verarbeitungsvorgang auf einer der vom EDSB gemäß Artikel 39 Absatz 4 erstellten Listen aufgeführt? Falls ja, ist eine DSFA durchzuführen.
2. Ist der Verarbeitungsvorgang auf einer der vom EDSB gemäß Artikel 39 Absatz 5 erstellten Listen aufgeführt? Falls ja, ist zu überprüfen, dass der Verarbeitungsvorgang tatsächlich unter die aufgeführten Arten von Verarbeitungsvorgängen fällt; ist dies der Fall, ist keine DSFA erforderlich.
3. Ist der Verarbeitungsvorgang auf keiner der beiden Listen aufgeführt, müssen Sie selbst eine Schwellenwertanalyse vornehmen, um festzustellen, ob eine DSFA erforderlich ist.

Artikel 39 der Verordnung bestimmt (Hervorhebung hinzugefügt):

> *„(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.*
>
> […]
>
> *(3) Eine Datenschutz-Folgenabschätzung nach Absatz 1 ist insbesondere in folgenden Fällen erforderlich:*
>
> > *(a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf eine automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkungen gegenüber natürlichen Personen entfalten oder diese in ähnlicher erheblicher Weise beeinträchtigen,*
> >
> > *(b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 10 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 11 oder*
> >
> > *(c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.“*

Dies ist, wie am Wort „insbesondere“ deutlich wird, eine **nicht erschöpfende** Aufzählung. Es mag auch andere Verarbeitungsvorgänge geben, die die Schwelle übersteigen und ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge haben. Für DSFA gemäß der DSGVO hat die Datenschutzgruppe nach Artikel 29 Leitlinien[13] herausgegeben (die inzwischen auch vom Europäischen Datenschutzausschuss gebilligt wurden), die auch Kriterien dafür enthalten, wann nach der DSGVO eine DSFA für einen Verarbeitungsvorgang erforderlich ist. **Die Schwellenwertanalyse hilft Ihnen, festzustellen, ob Ihre geplanten Verarbeitungsvorgänge diese Schwelle übersteigen.**

Absatz 4 desselben Artikels sieht vor, dass der **Europäische Datenschutzbeauftragte eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, erstellt und veröffentlicht**. Nach Absatz 5 desselben Artikels kann der Europäische Datenschutzbeauftragte auch eine Negativliste der Arten von Verarbeitungsvorgängen, für die keine Datenschutz-Folgenabschätzung erforderlich ist, erstellen. Diese Liste, die der Europäische Datenschutzbeauftragte am 16. Juli 2019 angenommen hat, ist in diesem Dokument als Anhang 5 wiedergegeben.

Nach Artikel 40 Absatz 4 der Verordnung kann die Kommission im Wege eines Durchführungsrechtsakts eine Liste der Arten von Verarbeitungsvorgängen Fälle festlegen, die vorheriger Konsultation bedürfen. Damit der Europäische Datenschutzbeauftragte auf diese Konsultation antworten kann, sollten Sie vorab eine DSFA durchgeführt haben. Sollte die Europäische Kommission solche Durchführungsrechtsakte erlassen, **werden wir die dort aufgeführten Verarbeitungsvorgänge unserer gemäß Artikel 39 Absatz 4 erstellten Liste hinzufügen**. Sie werden dann also nur eine einzige Liste abgleichen müssen.

Wenn Sie zu dem Schluss kommen, dass eine DSFA erforderlich ist, finden Sie die Informationen dazu in Teil II des Toolkits *Rechenschaftspflicht in der Praxis*.

Artikel 39 Absatz 9 der Verordnung sieht eine **Ausnahme** vom Erfordernis der Durchführung einer DSFA vor. Nach dem Artikel ist für Verarbeitungsvorgänge, die (1) auf einem Rechtsakt beruhen, in dem der konkrete Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge geregelt sind, und für die (2) bereits im Rahmen der allgemeinen Folgenabschätzung vor Erlass des vorgeschlagenen Rechtsakts eine DSFA erfolgte, keine DSFA erforderlich. Derartige Abschätzungen erfüllen nur dann die sich in der Verordnung vorgesehenen Anforderungen, wenn sie wesentlich detaillierter sind als die bisherigen Folgenabschätzungen für Legislativvorschläge. Kurz gesagt: Die derzeitigen Folgenabschätzungen im Gesetzgebungsverfahren der Union stellen einfach die Frage: „Ist dieser Vorschlag eine gute Idee?“[14], wohingegen die DSFA, die die EU-Institutionen durchführen müssen, die Frage beantworten soll: „Wie können wir diese uns übertragene Aufgabe unter Einhaltung der einschlägigen Vorschriften und unter Schutz der Privatsphäre erledigen?“.

Selbst wenn bereits bei der Vorschlagserarbeitung für die Rechtsgrundlage eine DSFA nach den Normen der Verordnung durchgeführt wurde, ist es sehr wahrscheinlich, dass vor Inkrafttreten eine Überprüfung erforderlich ist. Der Grund dafür ist, dass sich die erlassene Rechtsgrundlage möglicherweise in verschiedenen Punkten vom Vorschlag unterscheidet, und dass diese Unterschiede Auswirkungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz haben. Hinzu kommt, dass in der Regel nicht alle Gestaltungsentscheidungen, die

[13] Siehe http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[14] Hilfe bei der Beantwortung dieser Frage bietet, soweit es um Datenschutzaspekte geht, das vom EDSB herausgegebene Toolkit für die Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken.

sich auf Privatsphäre und Datenschutz auswirken, bereits durch die Rechtsgrundlage festgelegt werden. **In der Praxis stellen solche im Gesetzgebungsverfahren durchgeführten DSFA *allenfalls* die erste Iteration des DSFA-Prozesses dar.**

## 4.2 Positiv- / Negativlisten des Europäischen Datenschutzbeauftragten

**Wenn die Art von Verarbeitungsvorgang, den Sie implementieren möchten, auf der vom Europäischen Datenschutzbeauftragten gemäß Artikel 39 Absatz 4 der Verordnung erstellten Positivliste aufgeführt ist, müssen Sie eine DSFA durchführen.**

Die gemäß Artikel 39 Absätze 4 und 5 der Verordnung erstellten Listen finden Sie in Anhang 5. Die dort genannten Beispiele sind keine erschöpfende Darstellung.

Artikel 40 Absatz 4 der neuen Verordnung sieht vor, dass die Europäische Kommission im Wege eines Durchführungsrechtsakts eine Liste der Fälle festlegen kann, in denen die Verantwortlichen den Europäischen Datenschutzbeauftragten zu einer Verarbeitung zur Erfüllung einer vom Verantwortlichen im öffentlichen Interesse wahrgenommenen Aufgabe, unter anderem zur Verarbeitung personenbezogener Daten zu Zwecken des Sozialschutzes und der öffentlichen Gesundheit, konsultieren müssen. Derartige Durchführungsrechtsakte gelten dann für alle EU-Institutionen, nicht nur für die Europäische Kommission.

Damit der Europäische Datenschutzbeauftragte auf derartige Konsultationen antworten kann (siehe auch Teil II – Abschnitt 4), sollten Sie vorab eine DSFA durchführen. Bislang hat die Europäische Kommission keine solchen Durchführungsrechtsakte erlassen. **Sollte die Europäische Kommission dies jedoch tun, werden wir die betreffenden Arten von Verarbeitungsvorgängen unserer Liste gemäß Artikel 39 Absatz 4 hinzufügen**, um das Nachschlagen zu erleichtern.

## 4.3 Schwellenwertanalyse

**Eine Schwellenwertanalyse ist durchzuführen, wenn ein Verarbeitungsvorgang auf der Liste der Verarbeitungsvorgänge, für die die DSFA obligatorisch ist, nicht aufgeführt ist, Sie und/oder der Datenschutzbeauftragte Ihrer EU-Institution aber dennoch vermuten, dass er ein hohes Risiko bergen könnte; die Vorlage dafür ist in Anhang 5 beigefügt. Grundsätzlich sollten Sie, wenn mindestens zwei der Kriterien gegeben sind, eine DSFA durchführen. Die Schwellenwertanalyse ist zu dokumentieren.**

Wenn Ihre geplanten Verarbeitungsvorgänge auf keiner der beiden Listen stehen und Sie sich nicht sicher sind, ob eine DSFA erforderlich ist, sollten Sie Ihren behördlichen Datenschutzbeauftragten konsultieren und eine Schwellenwertanalyse durchführen. **Anhang 5 enthält eine Vorlage** für die Durchführung dieser Schwellenwertanalyse.

Diese Vorlage **beruht auf den Kriterien für die Arten von „wahrscheinlich ein hohes Risiko mit sich bringenden“ Verarbeitungsvorgängen, die von der Datenschutzgruppe nach Artikel 29 aufgestellt[15] und vom EDSA gebilligt wurden**, wobei einige Anpassungen im Hinblick auf den spezifischen Kontext von EU-Institutionen vorgenommen wurden. Da zum Beispiel im Beamtenstatut bereits erklärt wird, wie die Beurteilung der Beamten in den EU-Institutionen abläuft, hat der für die Verarbeitung Verantwortliche weniger Spielraum, was die Organisation und die rechtlichen Möglichkeiten der mit Entscheidungen unzufriedenen

[15] Siehe oben Fußnote 13.

Beamten angeht (weil z. B. Beschwerdeweg und Rechtsschutz bereits gesetzlich vorgegeben sind).

Mit der Vorlage wird abgefragt, ob die in Rede stehende Verarbeitung bestimmte Merkmale aufweist – ob es z. B. darum geht, Personen von Rechten, Vorteilen oder Verträgen auszunehmen, oder ob es um die Verarbeitung bestimmter Datenkategorien geht, etwa Gesundheitsdaten. Wenn dem so ist, ist detailliert anzugeben, auf welche Weise und aus welchen Gründen dies geschieht; in Grenzfällen sollten Sie auch angeben, warum das Kriterium Ihrer Ansicht nach nicht erfüllt ist. Die Kriterien, die über die in Artikel 39 Absatz 3 aufgeführten hinausgehen, beruhen auf der von der Artikel-29-Datenschutzgruppe vorgenommenen Auslegung der entsprechenden Vorschriften in der DSGVO. **Grundsätzlich sollten Sie, wenn mindestens zwei der Kriterien gegeben sind, eine DSFA durchführen.**

Die Abschätzung lässt sich jedoch nicht darauf reduzieren, einfach zu zählen, wie viele Kriterien erfüllt sind. Die Entscheidung ist kein Automatismus. Es kann durchaus vorkommen, dass auch für eine Verarbeitung, die nur eines der Kriterien erfüllt, eine DSFA erforderlich ist. In anderen Fällen ist dagegen vielleicht selbst dann keine DSFA nötig, wenn zwei oder mehr Kriterien gegeben sind. **Wenn Sie mindestens zwei Kriterien angekreuzt haben, jedoch denken, dass die Verarbeitung tatsächlich keine hohen Risiken für die betroffenen Personen zur Folge hätte, müssen Sie dies nach Rücksprache mit dem Datenschutzbeauftragten Ihrer EU-Institution, erklären.**

## 5. Was ist zu tun?

Die Verpflichtung, stets den Überblick über Ihre Verarbeitungsvorgänge zu behalten, ist nichts Neues. Auch nach Artikel 25 der alten Verordnung mussten Sie, als der Durchführungsverantwortliche aufseiten des für die Verarbeitung Verantwortlichen, Ihrem behördlichen Datenschutzbeauftragten alle Verarbeitungsvorgänge, die personenbezogene Daten betrafen, melden. Ihr Datenschutzbeauftragter hat diese in einem Register geführt, das allgemein zugänglich war.

**Für die Verzeichniserstellung können Sie auf Ihre vorhandenen Meldungen gemäß Artikel 25 der alten Verordnung zurückgreifen. Für neue Verarbeitungsvorgänge erstellen Sie die Verzeichnisse im Zuge Ihrer Entwicklungsarbeit.**

Die Meldungen können als Grundlage für die Verzeichniserstellung dienen (siehe dazu die Konkordanztabelle in Anhang 4). Für die bestehenden Verarbeitungsvorgänge können Sie Ihre vorhandenen Artikel-25-Meldungen in Verzeichnisse umwandeln. Wenn Ihre Meldungen auf dem aktuellen Stand sind, dürfte es nicht viel Mühe machen, daraus Verzeichnisse anzufertigen. Für neue Verarbeitungsvorgänge erstellen Sie die Verzeichnisse im Zuge Ihrer Entwicklungsarbeit.

In der **Verordnung ist keine Übergangszeit vorgesehen, abgesehen von den üblichen 20 Tagen nach der Veröffentlichung im Amtsblatt der EU**. Sie sollten Ihre Meldungen gemäß Artikel 25 schnellstmöglich umwandeln.

Falls Sie priorisieren müssen, sollten Sie mit den Verzeichnissen gemäß Artikel 31, die Ihre Verarbeitungsvorgänge mit höherem Risiko betreffen, beginnen. Die Compliance-Checkliste ist ein Tool, das Ihnen helfen soll, die Nachweise für die Begründung der von Ihnen gewählten Art der Datenverarbeitung vorlegen zu können.

# 6. Schlusswort

In Teil I des *Toolkits Rechenschaftspflicht in der Praxis* wurde praktische Anleitung dazu gegeben, wie Sie Verzeichnisse für Ihre Verarbeitungsvorgänge erstellen und herausfinden können, ob eine DSFA erforderlich ist. Für viele Verarbeitungsvorgänge werden Sie lediglich das Verzeichnis brauchen.

Als der Durchführungsverantwortlicher aufseiten des für die Verarbeitung Verantwortlichen bzw. die im Geschäftsbereich zuständige Person **müssen Sie alles Notwendige erledigen** – Sie tragen die Verantwortung dafür, dass die Datenschutzvorschriften eingehalten werden. Ihr behördlicher Datenschutzbeauftragter wird Ihnen Orientierung geben, doch die Verantwortung für die Auswahl und Implementierung der konkreten Maßnahmen zur Sicherstellung der Vorschriftseinhaltung liegt bei Ihnen.

**Verzeichnisse bilden die Grundlage Ihrer Datenschutzdokumentation.** Werden die Verzeichnisse nicht ordnungsgemäß geführt, kann dies mit Geldbußen gegen Ihre EU-Institution geahndet werden.[16] Wenn der Europäische Datenschutzbeauftragte prüft, ob Ihre EU-Institution ihren Datenschutzpflichten genügt, wird er sich mit Sicherheit Ihre Verzeichnisse ansehen. Auch wenn es in Ihrer EU-Institution Datenschutzverletzungen gibt, die Sie dem Europäischen Datenschutzbeauftragten melden müssen[17], werden wir nach den relevanten Verzeichnissen fragen.

Sie brauchen mit der Verzeichniserstellung nicht bei Null anzufangen, sondern können von den Meldungen ausgehen, die Sie schon nach der alten Verordnung machen mussten. Sie sollten die Meldungen schnell aktualisieren, da die Verzeichnisse die Grundlage Ihrer Datenschutzdokumentation bilden.

Verzeichnisse sind kein Selbstzweck, sondern dienen dem Nachweis, dass Sie bei der Gestaltung Ihrer Verarbeitungsvorgänge die Datenschutz-Compliance bedacht haben.

**Einige Verarbeitungsvorgänge mit höherem Risiko erfordern eine zusätzliche Prüfung.** Wenn Sie zu dem Schluss gelangen, dass für Ihren Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung (DSFA) nötig ist, so ist diese durchzuführen. Je nachdem, zu welchem Ergebnis die DSFA führt, kann es sein, dass auch eine „vorherige Konsultation“ des Europäischen Datenschutzbeauftragten nötig ist. Nähere Informationen zu alledem finden Sie in Teil II dieses Toolkits.

[16] Artikel 66 der Verordnung; ein Leitlinienentwurf ist den Datenschutzbeauftragten informationshalber zugeschickt worden.

[17] Artikel 37 der Verordnung; die vom Europäischen Datenschutzbeauftragten herausgegebenen Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten sind erhältlich unter: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-personal-data-breach-notification_en.

# Anhänge

## 1 Aufgabenverteilung

Die nachstehende Liste gibt einen Kurzüberblick über die Verteilung der Aufgaben: Was muss der für die Verarbeitung Verantwortliche / die im Geschäftsbereich zuständige Person tun, und wofür sind die Datenschutzbeauftragten zuständig?

Verantwortlicher / im Geschäftsbereich Zuständiger;

- Verzeichnis entwerfen;
- Fragen zur Compliance-Kontrolle beantworten;
- Prüfen, ob eine DSFA erforderlich ist.

Datenschutzbeauftragter:

- Feedback geben zum Entwurf des Verzeichnisses und zu sonstigen Entwürfen von Unterlagen;
- Verzeichnisregister führen;
- auf Konsultation durch Verantwortliche / im Geschäftsbereich Zuständige erwidern;
- als Verbindungsstelle zwischen EU-Institution und dem Europäischen Datenschutzbeauftragten fungieren.

Sonstige Funktionen (z. B. IT oder Rechtsabteilung)

- Unterstützung des Verantwortlichen / im Geschäftsbereich Zuständigen und des Datenschutzbeauftragten, falls erforderlich.

## 2 Checkliste für Verzeichnisse und Compliance

Nach Artikel 31 der neuen Verordnung müssen EU-Institutionen Verzeichnisse ihrer Veredelungsvorgänge führen. Diese Vorlage deckt zwei Aspekte ab:

1. obligatorische Verzeichnisse im Sinne von Artikel 31 der neuen Vorschriften (Empfehlung: öffentlich zugänglich)
2. Compliance-Kontrolle und Risikoprüfung (intern)

Die Überschrift und Teil 1 sollten öffentlich zugänglich sein; Teil 2 ist intern für die EU-Institution. In der dritten Spalte wird ein Beispiel für ein hypothetisches Verzeichnis für Badges und physische Zugangskontrolle in einer EU-Institution gegeben.

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | **Überschrift – Versions- und Referenznummer (Empfehlung: öffentlich zugänglich)** | | |
| 1. | Letzte Aktualisierung dieses Verzeichnisses | | 25/05/2018 |
| 2. | Referenznummer | Zur Nachverfolgung: Wenn Ihre EU-Institution ein zentrales Register führt, holen Sie beim Registerführer die Referenznummer ein. | EUI/Logistics/1.1 |
| | **Teil 1 – Verzeichnis gemäß Artikel 31 (besondere gesetzliche Verpflichtung zur Veröffentlichung – siehe Artikel 31 Absatz 5)** | | |
| 3. | Name und Kontaktdaten des für die Verarbeitung Verantwortlichen | So weit möglich, funktionale (nicht: persönliche) Postfächer verwenden – das spart Zeit bei der Aktualisierung der Verzeichnisse und dient der Geschäftskontinuität. | Für die Verarbeitung Verantwortlicher: EU-Institution, Europaplatz 1, Stadt, Mitgliedstaat, Kontakt: Direktor Logistik, EU-Institution fmb-logistics@eui.europa.eu |
| 4. | Name und Kontaktangaben des DSB | Dies ist ein vorausgefülltes Feld. | DSB, EU-Institution dpo@eui.europa.eu |
| 5. | Name und Kontaktangaben des für die Verarbeitung gemeinsam Verantwortlichen (gegebenenfalls) | Wenn Sie und eine andere EU-Institution oder eine andere Organisation gemeinsam Verantwortliche sind, ist das anzugeben (z. B. wenn zwei EU-Institutionen einen medizinischen Dienst gemeinsam nutzen). In diesem Fall ist darauf zu achten, dass Sie in der Beschreibung angeben, wer wofür zuständig ist und an wen man sich mit Fragen wenden kann. | Entfällt. |
| 6. | Name und Kontaktangaben des | Wenn Sie einen Auftragsverarbeiter (Auftragnehmer) | Entfällt. |

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | Auftragsverarbeiters (gegebenenfalls) | personenbezogene Daten verarbeiten lassen, ist das anzugeben (z. B. für 360°-Beurteilungen, outgesourcte IT-Dienstleistungen oder bei externer Erledigung vor der Anstellung erfolgender Gesundheitsprüfungen). | |
| 7. | Zweck der Verarbeitung | Knappe Darstellung, was erreicht werden soll; ggf. auch die spezifische Rechtsgrundlage angeben (z. B. im Falle von Auswahlverfahren das Statut der Beamten). | Sicherstellung der physischen Sicherheit des Gebäudes der EU-Institution durch Zugangskontrolle, sowohl allgemein als auch zu besonders sensiblen Bereichen innerhalb des Gebäudes (z. B. Archiven); Erfassung der Anzahl der Personen im Gebäude für Evakuierungszwecke; beides gestützt auf die Artikel X und Y der Entscheidung über die Sicherheit der EU-Institution. |
| 8. | Beschreibung der Kategorien von Personen, deren Daten [die EU-Institution] verarbeitet, sowie Auflistung der Datenkategorien | Wenn die Datenkategorien für verschiedene Personenkategorien verschieden sind, ist das zu erklären (im Falle von Verwaltungsuntersuchungen z. B. Verdächtige im Gegensatz zu Zeugen). | Wir verarbeiten die folgenden Daten jeder Person, an die ein Zugangs-Badge für Gebäude der EU-Institution ausgegeben wurde (d. h. Mitarbeiter und vor Ort tätige Auftragnehmer, nicht jedoch begleitete Besucher):<br>) Name und Foto [auf Badge aufgedruckt und zentral gespeichert];<br>) Verbindung zur EU-Institution [Mitarbeiter / Auftragnehmer, zentral gespeichert];<br>) Badge-Nummer [einzige im RFID-Tag auf dem Badge gespeicherte Information];<br>) Türen / Tore, für die Badge gilt [zentral gespeichert];<br>) Ende der Badge-Gültigkeit [auf Badge aufgedruckt und zentral gespeichert];<br>) beim Badge-Auflegen an Türen /Toren: Zeitstempel, Kennung von Tür / Tor, Badge-Nummer [zentral gespeichert]. |
| 9. | Fristen für die Speicherung der Daten | Angabe der für die EU-Institution geltenden Aufbewahrungsfristen für Verwaltungsdaten, mit Angabe des Fristbeginns; erforderlichenfalls zwischen verschiedenen Datenkategorien oder Personenkategorien zu differenzieren (z. B. beim Auswahlverfahren: Bewerber, die es auf die Reserveliste geschafft haben, und solche, die es nicht geschafft | Die Daten werden von uns ab Ablauf / Einziehung des Badge zwei Monate lang gespeichert; anderes gilt nur für Zugriffsprotokolle, die wir rollierend zwei Monate lang speichern. |

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | | haben). | |
| 10. | Datenempfänger | Wer in Ihrer EU-Institution hat Zugang zu den Daten? Wer außerhalb Ihrer EU-Institution hat Zugang?<br>Hinweis: Behörden, die unter Umständen im Rahmen einer bestimmten Untersuchung personenbezogene Daten erhalten (z. B. OLAF, EO, EDSB), brauchen nicht als Empfänger angegeben zu werden. | Der Sicherheitsbeauftragte der EU-Institution, zum Zwecke der Nachverfolgung und Untersuchung von Sicherheitsvorfällen.<br>Wachleute haben nur Zugang zur aktuellen Anzahl der Menschen im Gebäude (aggregierte Daten, keine personenbezogenen Daten). |
| 11. | Gibt es Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen? Falls ja: Wohin und mit welchen Garantien? | Z. B. an Auftragsverarbeiter in einem Drittland, unter Verwendung von Standardvertragsklauseln; an eine staatliche Behörde in einem Drittland, mit der die EU-Institution aufgrund einer Übereinkunft zusammenarbeitet. Mit Fragen zur Einholung der Garantien wenden Sie sich an den behördlichen Datenschutzbeauftragten. | Nein |
| 12. | Allgemeine Beschreibung der Sicherheitsvorkehrungen, soweit möglich. | Die von der EU-Institution getroffenen Sicherheitsvorkehrungen sind allgemein zu beschreiben, in einer Weise, die auch veröffentlicht werden könnte. | Daten von Badge-Inhabern und Zugriffsprotokollen werden von uns elektronisch in Systemen mit Zugangsbeschränkungen gespeichert, die durch die üblichen Sicherheitspraktiken der EU-Institution gesichert sind, die unserem nach ISO 27001 zertifizierten |
| | | | Informationssicherheitsmanagementsystem genügen. Die einzige elektronisch (im RFID-Tag) auf dem Badge gespeicherte Information ist die Badge-Nummer. Die Information kann nur in einem Abstand von bis zu 5 cm gelesen werden. |
| 13. | Nähere Informationen über die Ausübung Ihrer Rechte auf Auskunft, Berichtigung, Widerspruch und (ggf.) Datenübertragbarkeit finden Sie in der Datenschutzerklärung: | Streng genommen ist die Veröffentlichung der Datenschutzerklärung nicht Teil des Verzeichnisses; sie erhöht jedoch die Transparenz und verursacht keinen zusätzlichen Verwaltungsaufwand, weil es sie bereits gibt. | [Link zur Datenschutzerklärung] |
| | **Teil 2 – Compliance-Kontrolle und Risikoprüfung (intern)** | | |
| | **Compliance-Kontrolle (Artikel 4 und 5)** | | |
| 14. | Rechtsgrundlage und Erforderlichkeit | Hier (mindestens) eine der Bedingungen ankreuzen und | (a2) nicht spezifisch im Primär- oder Sekundärrecht der Union |

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | der Verarbeitung (siehe Artikel 5 der neuen Verordnung):<br><br>(a) erforderlich für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe, die durch Unionsrechtsakt übertragen wurde;<br><br>(a2) (a) gemäß Erwägungsgrund 17 Satz 2<br><br>(b) erforderlich zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt;<br><br>(c) erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist;<br><br>(d) Einwilligung;<br><br>(e) lebenswichtige Interessen. | erklären, warum die Verarbeitung dafür erforderlich ist. Beispiele:<br><br>(a) eine ihrer EU-Institution durch Rechtsakt übertragene Aufgabe, z. B. im Statut der Beamten vorgesehene Verfahren oder Aufgaben, die einer Agentur in ihrer Gründungsverordnung übertragen wurden. Bitte die Rechtsgrundlage genau angeben (z. B. Artikel X des Statuts der Beamten, so wie dieser durch Artikel Y der Durchführungsverordnung der EU-Institution implementiert wurde; „Statut der Beamten“ genügt nicht);<br><br>(a2) nicht alle Verarbeitungsvorgänge, die für die Arbeitsweise der EU-Institutionen erforderlich sind, sind ausdrücklich in Rechtsakten geregelt; Erwägungsgrund 17 stellt klar, dass sie dennoch hierdurch gedeckt sind, z. B. interne Mitarbeiterverzeichnisse, Zugangskontrolle;<br><br>(b) eine spezifische gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten (z. B. die in der Gründungsverordnung einer EU-Agentur vorgesehene Verpflichtung zur Veröffentlichung von Interessenerklärungen);<br><br>(c) dies kommt bei den EU-Institutionen selten vor;<br><br>(d) wenn jemand freiwillig und in informierter Weise eingewilligt hat (z. B. Fotoautomat bei einem Europatag, optionale Veröffentlichung von Fotos in internem Mitarbeiterverzeichnis);<br><br>(e) die Verarbeitung von Gesundheitsinformationen durch Ersthelfer, wenn die Person nicht einwilligen kann (z. B. bei einem Unfall). | erwähnt, jedoch für Schutz und Sicherheit von Personal, Gebäuden und Informationen erforderlich. Vgl. auch Artikel X und Y der Entscheidung 2017/XXXX über die Sicherheit der EU-Institution. |
| 15. | Zweckbestimmung | Haben Sie alle oben in Nr. 7 genannten Zwecke aufgeführt?<br><br>Sind die Zwecke konkret und ausdrücklich angegeben und rechtmäßig? Wenn die Informationen auch für andere Zwecke verarbeitet werden: Sind Sie sich sicher, dass diese anderen Zwecke nicht mit dem/den ursprünglichen Zweck(en) | Ja.<br><br>Die Überprüfung, dass nur befugte Personen Zugang zu den Gebäuden der EU-Institution haben, dient dazu, Schutz und Sicherheit unserer Mitarbeiter, Informationen und sonstigen Vermögenswerte zu gewährleisten. |

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | | unvereinbar sind? | Außerdem verwenden wir Zugangsprotokolle, um (zu Evakuierungszwecken) zu wissen, wie viele Personen sich gerade im Gebäude aufhalten.<br><br>Die Protokolle können im Einzelfall auch dazu verwendet werden, Vorfälle zu untersuchen (z. B. „Wer befand sich in dem Zeitraum, in dem die Akten verschwanden, im Archivraum?“), wobei dies gemäß den einschlägigen Verfahren geschieht (siehe Verzeichnis EUI-123.4 über Verwaltungsuntersuchungen), was nicht mit den ursprünglichen Zwecken unvereinbar ist.<br><br>Bei der Ausgabe des Badge weisen wir die Badge-Inhaber darauf hin (siehe Datenschutzerklärung). |
| 16. | Datenminimierung | Werden alle Daten, deren Erfassung geplant ist, wirklich gebraucht? Gibt es vielleicht welche, auf die man verzichten könnte? | Foto, Name und Ablaufdatum auf dem Badge sind erforderlich, damit die Wachleute Sichtkontrollen vornehmen können; die Badge-Nummer ist erforderlich für die Zugangskontrolle zu zugangsbeschränkten Bereichen und für die Einziehung von Badges.<br><br>Zugangsprotokolle (wer, wann, wo) sind erforderlich, um Vorfälle wie Diebstähle oder das Abhandenkommen von Unterlagen zu untersuchen. |
| 17. | Richtigkeit | Wie stellen Sie die Richtigkeit der von Ihnen verarbeiteten Informationen über Personen sicher? Wie berichtigen Sie unzutreffende Informationen? | Name und Foto erfassen wir direkt von der Person, die ein Badge beantragt. Die Uhren an den Zugangstoren sind synchronisiert. Badge-Inhaber können die Änderung von Name und Foto verlangen. |
| 18. | Speicherbegrenzung | Erklären Sie, warum Sie sich für die oben in Nummer 9 genannte(n) Speicherfrist(en) entschieden haben.<br><br>Genügen die Speicherfristen dem Grundsatz „so lange wie erforderlich, so kurz wie möglich“? Falls Sie nur einige der Informationen länger brauchen: Können Sie für die verschiedenen Informationen unterschiedliche Speicherfristen vorsehen? | Zwei Monate scheint für Zugangsprotokolle eine angemessene Frist, die die Untersuchung von Vorfällen (auch wenn diese, z. B. bei Diebstahl in Urlaubszeiten, nicht sofort entdeckt werden) ermöglicht, jedoch nicht zu lang bemessen ist.<br><br>Die Informationen über die Badge-Inhaber müssen solange, wie der Badge gültig ist, gespeichert werden. Indem wir sie über den Ablauf / die Einziehung des Badge hinaus weitere zwei Monate speichern, bleiben wir in der Lage, auch Vorfälle, die unter Umständen kürzlich ausgeschiedene Mitarbeiter |

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | | | betreffen, zu untersuchen (andernfalls wüssten wir nicht, um wessen Badge es sich handelte). |
| 19. | Transparenz: Wie informieren Sie die betroffenen Personen über die Verarbeitung? | Z. B. Datenschutzerklärungen auf Formularen, E-Mail-Mitteilungen; wenn Sie beabsichtigen, die betroffenen Personen nicht (oder erst nachträglich) zu informieren, müssen Sie sich an Ihren behördlichen Datenschutzbeauftragten wenden! | Datenschutzerklärung auf dem Badge-Antragsformular und kurzer Hinweis auf der Badge-Rückseite mit Link zur veröffentlichten Datenschutzerklärung. |
| 20. | Auskunftsrecht und sonstige Rechte der Personen, deren Daten verarbeitet werden | Wie können die betroffenen Personen die EU-Institution erreichen, wenn sie wissen möchten, welche Daten über sie gehalten werden, die Daten berichtigen, löschen oder sperren lassen oder der Verarbeitung widersprechen möchten? Wie werden Sie darauf reagieren? Wenn Sie denken, dass es Situationen geben könnte, in denen Sie zum Beispiel keine Auskunft würden geben wollen, sollten Sie das mit Ihrem behördlichen Datenschutzbeauftragten besprechen. | Siehe Datenschutzerklärung: E-Mail an logistics@eui.europa.eu; Wir werden darauf innerhalb der üblichen Fristen und nach den Verfahren erwidern, die in den Datenschutz-Durchführungsvorschriften der EU-Institution vorgesehen sind (Abschnitt Y der Entscheidung 2018/1234 der EU-Institution). |
| | **Feststellung eines hohen Risikos** | | |
| 21. | Geht es im relevanten Prozess um Folgendes:<br>J Gesundheitsdaten, (Verdacht auf) Straftaten oder sonstige als sensibel anzusehende Daten („besondere Datenkategorien“);<br>J Bewertung, automatisierte Entscheidungsfindung oder Profiling;<br>J Überwachung betroffener Personen;<br>J neue Technologie, die als starker Eingriff angesehen werden könnte. | Einige als riskant eingestufte Verarbeitungsvorgänge erfordern zusätzliche Schutzmaßnahmen und Dokumentierung. Wenn Sie einen dieser Punkte angekreuzt haben, sollten Sie sich zwecks näherer Informationen und Anleitung an Ihren behördlichen Datenschutzbeauftragten wenden. | Nein |
| | **Teil 3 – Verlinkte Dokumente (intern)** | | |
| 22. | (ggf.) Links zur | Wenn Sie eine Schwellenwertanalyse und/oder DSFA | Nicht zutreffend. |

| Nr. | Gegenstand | Erläuterung | Beispiel: Zugangskontrolle |
|---|---|---|---|
| | Schwellenwertanalyse und DSFA | durchgeführt haben, verweisen Sie hier darauf. | |
| 23. | Wo sind Ihre Maßnahmen auf dem Gebiet der Informationssicherheit dokumentiert? | Nach den Vorschriften Ihrer EU-Institution auf dem Gebiet der Informationssicherheit sind Sie höchstwahrscheinlich verpflichtet, Ihre Sicherheitsvorkehrungen zu dokumentieren; angemessene Informationssicherheit ist auch eine Datenschutzanforderung. Bitte tragen Sie einen Link zu den einschlägigen Dokumenten über die Informationssicherheit ein. | [Link zu Dokumenten über Informationssicherheit] |
| 24. | Sonstige verlinkte Dokumente | Bitte hier Links zu weiterer Dokumentation über diesen Prozess eintragen (z. B. Projektdokumentation, Handbücher). | [Links zum Konzept „Physische Sicherheit“ der EU-Institution] |

# 3 Eingehendere Erläuterungen zu den Vorlagen für Verzeichnisse / Compliance-Kontrolle

Die Vorlage in Anhang 1 enthält einige Erläuterungen und Ausfüllhinweise; in diesem Anhang finden Sie genauere Informationen zum rechtlichen Hintergrund. Diese sind in zwei Teile gegliedert: „Ist diese Verarbeitung rechtmäßig?“ und „Halten wir die Datenschutzgrundsätze ein?“

## Artikel 5 – Rechtmäßigkeit der Verarbeitung

Was die erste Frage angeht, so muss die Verarbeitung eine der in Artikel 5 der Verordnung genannten Bedingungen erfüllen. Hier müssen wir uns fragen: „Warum dürfen wir das überhaupt machen?“

*„Artikel 5 – Rechtmäßigkeit der Verarbeitung*

1. *Die Verarbeitung ist nur rechtmäßig, wenn und soweit mindestens eine der nachstehenden Bedingungen erfüllt ist:*
   a) *die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Organ oder der Einrichtung der Union übertragen wurde,*
   b) *die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt,*
   c) *die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen,*
   d) *die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben,*
   e) *die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.*
2. *Die Rechtsgrundlage für eine Verarbeitung gemäß Absatz 1 Buchstaben a und b wird im Unionsrecht festgelegt.“*

Meistens werden Sie **Unterabsatz a** als Rechtsgrundlage anführen. Beispiele hierfür sind Aufgaben, deren Wahrnehmung Ihrer Institution durch Unionsrechtsakt übertragen werden – wobei es sich um spezifische Aufgaben Ihrer EU-Institution handeln kann oder auch um Verwaltungsvorschriften, z. B. über Personalmanagement oder Beschaffung und Auftragsvergabe, die gemäß den Vorschriften über Personal und Finanzen erfolgen müssen. Diese spezifischen Rechtsgrundlagen können auch zusätzliche Vorgaben bezüglich einzelner Aspekte der Verarbeitung enthalten (z. B. zu Datenkategorien, Aufbewahrungsfristen usw.).

Gemäß Erwägungsgrund 22 Satz 2 der Verordnung schließt Unterabsatz a „die Verarbeitung personenbezogener Daten ein, die für die Verwaltung und die Arbeitsweise dieser Organe und Einrichtungen erforderlich sind“ (z. B. das Führen eines internen Mitarbeiterverzeichnisses). Dies ist auf dem Formular als (a2) erwähnt.

**Unterabsatz b** betrifft nur spezifische gesetzliche Verpflichtungen zur Verarbeitung personenbezogener Daten, z. B. die in den Gründungsverordnungen einiger EU-Agenturen vorgesehene Verpflichtung zur Veröffentlichung von Interessenerklärungen.[18]

[18] Die Unterabsätze a und b unterscheiden sich insofern, als es in Unterabsatz a um eine der EU-Institution übertragene Aufgabe geht, zu deren Wahrnehmung die Verarbeitung personenbezogener Daten erforderlich ist

**Unterabsatz c** bezieht sich auf eine Verarbeitung, die für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Davon machen die EU-Institutionen selten Gebrauch. Ein Beispiel aus dem Privatsektor wäre die Warenlieferung im Versandhandel: Die Lieferanschrift ist erforderlich, damit der Lieferant seinen Teil des Vertrags erfüllen kann (während es möglicherweise nicht erforderlich ist, sie noch über die Lieferung hinaus zu speichern).

**Unterabsatz d** bezieht sich auf Verarbeitungen, in die die betroffene Personen eingewilligt haben. Die Einwilligung muss freiwillig, in informierter Weise und für den bestimmten Fall erteilt werden.[19] Von dieser Rechtsgrundlage machen die EU-Institutionen nicht oft Gebrauch, weil ihre Verarbeitung personenbezogener Daten in der weit überwiegenden Zahl der Fälle unter den oben genannten Unterabsatz a fällt. Es gibt aber auch Beispiele dafür, dass sich EU-Institutionen auf eine Einwilligung stützen: z. B. für Newsletter-Abonnements oder für Fotoautomaten beim Europatag.

**Unterabsatz e** betrifft eine Verarbeitung, die erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, Ein Beispiel dafür wären von Sanitätern ergriffene medizinische Rettungsmaßnahmen nach einem Arbeitsunfall.

In manchen Fällen können Sie sich vielleicht für unterschiedliche Aspekte der Verarbeitung auf verschiedene Unterabsätze stützen. So ist zum Beispiel ein internes Mitarbeiterverzeichnis „für die Verwaltung und die Arbeitsweise“ Ihrer EU-Institution erforderlich, Mitarbeiterfotos sind es jedoch nicht. Sie können den Mitarbeitern die Möglichkeit anbieten, einzuwilligen und Fotos hochzuladen, Sie dürfen die Mitarbeiter jedoch weder zwingen noch unter Druck setzen.

## Artikel 4 – Datenschutzgrundsätze

Die Datenschutzgrundsätze in Artikel 4 bilden die Grundlage für die detaillierteren Vorschriften in der neuen Verordnung. Hier geht es um die Frage: „Auf welche Weise machen wir das?“

*„Artikel 4 – Grundsätze für die Verarbeitung personenbezogener Daten*

*1. Personenbezogene Daten müssen*

*a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“),*

*b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 13 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“),*

*c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“),*

---

(z. B. Beurteilungen von Mitarbeitern), während es in Unterabsatz b darum geht, dass Ihre EU-Institution eine spezifische Verpflichtung zur Verarbeitung personenbezogener Daten hat, die eindeutig im Unionsrecht geregelt ist, ohne den geringsten Spielraum hinsichtlich der Art und Weise der Durchführung (z. B. „Die Agentur ergreift Maßnahmen zur Prävention und Aufdeckung von Interessenkonflikten“ im Gegensatz zu „Die Interessenserklärung des Exekutivdirektors wird veröffentlicht“).

[19] Siehe Artikel-29-Datenschutzgruppe Opinion 15/2011 on consent (WP 187).

*d) sachlich richtig sein und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit"),*

*e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 13 verarbeitet werden („Speicherbegrenzung"),*

*f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").*

*2. Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht")."*

Bei jedem dieser Unterabsätze müssen Sie sich – unter Berücksichtigung der nachstehenden zusätzlichen Erläuterungen – fragen, ob Ihre EU-Institution diesen Anforderungen genügt:

Das Wort **„rechtmäßig"** in Unterabsatz a bezieht sich auf die oben zu Artikel 5 vorgenommene Prüfung.

In Unterabsatz a ist auch **„Transparenz"** erwähnt. Das bedeutet, dass Sie den betroffenen Personen sagen müssen, dass Sie deren personenbezogene Daten verarbeiten, sowie wozu und auf welche Weise die Verarbeitung erfolgt (was in den Artikeln 14 bis 16 näher angegeben ist). Dabei sind allerdings Beschränkungen möglich; man denke etwa an die ersten Phasen einer OLAF-Untersuchung. Wenn Sie die Daten direkt bei den betroffenen Personen erfassen (z. B. mit einem Fragebogen), teilen Sie die Informationen gleichzeitig mit. Wenn Sie sie anderswo erfassen, müssen Sie darüber nachdenken, wie Sie die betroffenen Personen informieren können. In der Regel wird es nicht genügen, einfach einen Datenschutzhinweis zu veröffentlichen, da Sie die betroffenen Personen damit nicht unbedingt erreichen. Nähere Informationen finden Sie in den Leitlinien des EDPS zu Artikel 14 bis 16 der Verordnung[20] sowie zu Artikel 25[21].

Teil der in Unterabsatz a genannten **Verarbeitung nach Treu und Glauben** ist auch, dass die Personen, deren Daten Sie verarbeiten, bestimmte Rechte haben, die sie bezüglich der Verarbeitung geltend machen können (und die in den Artikel 14 und 17 bis 24 der neuen Verordnung im Einzelnen angegeben sind); z. B. das Recht auf Auskunft über die über sie gespeicherten Daten, erforderlichenfalls deren Berichtigung oder, wenn die Daten rechtswidrig gespeichert werden, deren Löschung usw. Mehr darüber finden Sie in den Leitlinien zu den

[20] https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf.

[21] Den Datenschutzbeauftragten ist die Entwurfsfassung der internen Vorschriften im Sinne von Artikel 25 der Verordnung zur Information zugeschickt worden.

Rechten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten[22]. Außerdem bedeutet dies, dass Sie Ihre Systeme und Prozesse so gestalten müssen, dass Sie solche Anfragen ohne Weiteres beantworten können.

Der erste Teil von Unterabsatz b ist im Verzeichnis bereits durch das Feld **„Zweck“** abgedeckt. Dieser Grundsatz steht im Zusammenhang mit der Verarbeitung nach Treu und Glauben: Die Zwecke sind klar zu definieren, damit die betroffenen Personen wissen, womit sie rechnen müssen. Sie müssen also klar angeben, wozu Ihre EU-Institution die personenbezogenen Daten verarbeitet. Die strengen Regeln über die Weiterverarbeitung zielen darauf ab, bestimmte Situationen zu verhindern, etwa, dass Informationen dazu wiederverwendet werden, mit Repressalien gegen Whistleblower vorzugehen. Dabei ist zu beachten, dass die neue Verordnung nicht pauschal gestattet, sämtliche Daten für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke länger zu speichern. Sie müssen in jedem Einzelfall eine einschlägige Rechtsgrundlage für die Verarbeitung haben und die Erforderlichkeit und Verhältnismäßigkeit jeder Datenspeicherung prüfen. Außerdem müssen Sie darüber nachdenken, welche Schutzmaßnahmen Sie ergreifen können – z. B. Aggregierung der für Forschungszwecke gespeicherten/offengelegten personenbezogenen Daten, Aufnahme eines Verbots der Re-Identifikation in die für die Gewährung des Zugangs zu Forschungszwecken geltenden Bedingungen usw.

**„Datenminimierung“** in Unterabsatz c bedeutet, dass Sie für jede Datenkategorie in der Lage sein müssen, zu erklären, warum sie zum Erreichen des Verarbeitungszwecks erforderlich ist. Sie müssen sich fragen: „Brauchen wir das wirklich für diesen Zweck? Ginge das nicht auch ohne diese Daten?“[23]

**„Richtigkeit“** in Unterabsatz d bedeutet, dass Sie alle angemessenen Anstrengungen unternehmen müssen, sicherzustellen, dass die Daten, die Sie verarbeiten, richtig sind; schließlich können auf falscher Informationsgrundlage beruhende Entscheidungen negative Auswirkungen auf Menschen haben, für die Ihre EU-Institution unter Umständen haftet. Besonders wichtig ist dies, wenn Sie die Daten nicht direkt bei den Menschen erfassen, deren Daten es sind, sondern aus anderen Quellen beziehen. Bei manchen Verarbeitungsvorgängen kann es sein, dass die Wahrheitsgemäßheit von Behauptungen unter den betroffenen Parteien streitig ist (z. B. wenn Whistleblower Vorwürfe erheben). In solchen Fällen bezieht sich der Begriff „Richtigkeit“ darauf, dass eine bestimmte Erklärung (die personenbezogene Daten enthält) angegeben und zutreffend aufgezeichnet wurde; der Gegenseite sollte Gelegenheit gegeben werden, die aufgezeichneten Informationen zu ergänzen und selbst dazu Stellung zu nehmen.[24]

Der Grundsatz der **„Speicherbegrenzung“** in Unterabsatz e bedeutet, dass es für alle verarbeiteten personenbezogenen Daten einen (mit dem obigen Zweck zusammenhängenden) Grund dafür geben muss, dass diese für den vorgesehenen Zeitraum gespeichert werden. In manchen Fällen ist diese Aufbewahrungsfrist in den einschlägigen Unionsvorschriften

[22] https://edps.europa.eu/data-protection/our-work/publications/guidelines/rights-individuals_en.

[23] Beachten Sie dabei den Unterschied zur Erforderlichkeit der Verarbeitung insgesamt (vgl. obige Erläuterungen zu Artikel 5 Buchstabe a – hier fragen wir uns: „Wir haben festgestellt, dass wir dies tun sollten, *aber was brauchen wir dafür*?“).

[24] Um ein weiteres Beispiel zu geben: Eine Mitarbeiterin ist mit dem negativen Feedback, das ihre Vorgesetzte ihr in der Beurteilung gegeben hat, nicht einverstanden. Das Feedback der Vorgesetzten ist insofern „richtig“, als es sich um das Feedback handelt, das von der Vorgesetzten gegeben wurde. Dennoch muss es den Mitarbeitern möglich sein, dazu eine eigene Stellungnahme abzugeben und in einem Beschwerdeverfahren gegen negative Kommentare vorzugehen. Wenn die Beurteilung dann auf die Beschwerde hin geändert wird, handelt es sich allerdings nicht um eine „Berichtigung“ im Sinne von Artikel 14 der neuen Verordnung.

niedergelegt; ansonsten muss ihre EU-Institution diese Fristen festlegen. Dabei gilt der Grundsatz „so lange wie erforderlich, so kurz wie möglich“, wobei jeweils auf die sich aus den behördlichen Aufgaben ergebenden Erfordernisse abzustellen ist – die Aufbewahrungsfrist darf nicht unter technischen Gesichtspunkten bemessen werden! Wenn Daten zu Beweiszwecken oder aus ähnlichen Gründen gespeichert werden müssen, ist der Zugang dazu auf diejenigen Nutzerprofile zu beschränken, die auf deren Kenntnis angewiesen sind.

Unterabsatz f bestimmt, dass Sie personenbezogene Daten in solcher Weise verarbeiten müssen, dass **„angemessene Sicherheit“** gewährleistet ist. Was „angemessen“ ist, ist von den mit der Verarbeitung verbundenen Risiken abhängig (siehe auch Artikel 26). Dabei sind technische und organisatorische Maßnahmen umzusetzen. Oft werden Sie an dieser Stelle auf Ihre allgemeine Dokumentation zum Informationssicherheits-Risikomanagement (ISRM) verweisen können. Eingehendere Informationen dazu enthalten die Leitlinien des EDPS zu Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten[25].

Zu vielen dieser Aspekte hat der EDSB Leitlinien herausgegeben[26]. Erforderlichenfalls wird der EDSB diese im Hinblick auf die angenommene neue Verordnung aktualisieren. Wenn Sie nähere Informationen dazu wünschen, wenden Sie sich bitte an Ihren Datenschutzbeauftragten.

# 4 Konkordanztabelle: Meldungen gemäß Artikel 25 der alten Verordnung und Verzeichnisse im Sinne der Verordnung

Nach Artikel 25 der alten Verordnung mussten die Meldungen an den behördlichen Datenschutzbeauftragten Folgendes enthalten:

(a) Name und Anschrift des für die Verarbeitung Verantwortlichen und Angabe der organisatorischen Einheiten eines Organs oder einer Einrichtung, die mit der Verarbeitung personenbezogener Daten für einen bestimmten Zweck beauftragt sind;
(b) Zweckbestimmung(en) der Verarbeitung;
(c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;
(d) Rechtsgrundlage der Verarbeitung, für die die Daten bestimmt sind;
(e) Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;
(f) eine allgemeine Angabe der Fristen für die Sperrung und Löschung der verschiedenen Datenkategorien;
(g) geplante Datenübermittlungen in Drittländer oder internationale Organisationen;
(h) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 22 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Für diese Meldungen haben die EU-Institutionen ihre eigenen Vorlagen benutzt, die zuweilen zusätzliche Punkte enthielten, zum Beispiel bei Einbeziehung eines Auftragsverarbeiters einen Hinweis darauf. Wie vorstehend in Abschnitt 3.1 erklärt, sind in Artikel 31 der Verordnung die Punkte aufgeführt, die in den Verzeichnissen im Sinne der Verordnung anzugeben sind. Vergleicht man diese Artikel, werden die Gemeinsamkeiten und Unterschiede deutlich. Sie werden sehen, dass ein Großteil der für die Verzeichnisse erforderlichen Informationen bereits

[25] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en.
[26] Siehe https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en.

in Ihren Meldungen gemäß Artikel 25 zu finden sind. Sie können diese Informationen als Grundlage für die von Ihnen zu erstellenden Verzeichnisse verwenden.

| Artikel 25 der alten Verordnung | Artikel 31 der Verordnung |
|---|---|
| (a) | (a), hier zusätzlich: Kontaktangaben zum Datenschutzbeauftragten und, ggf. zum Auftragsverarbeiter und/oder gemeinsam für die Verarbeitung Verantwortlichen; |
| (b) | (b) |
| (c) | (c) |
| (d) | gestrichen, jedoch bei der Angabe der Zwecke unter (b) zu erwähnen: In den meisten Fällen wird die von EU-Institutionen vorgenommene Verarbeitung für die Wahrnehmung einer ihnen übertragenen Aufgabe oder zur Erfüllung einer unionsrechtlichen Verpflichtung erforderlich sein; |
| (e) | (d), jedoch klarere Anforderungen, dass auch Empfänger in Drittländern / internationalen Organisationen genannt werden müssen (mit Bezeichnung der jeweiligen Empfänger); |
| (g) | (e) zusätzliche Informationen zu den Garantien bei Übermittlung in Drittländer / internationale Organisationen (z. B. Standardvertragsklauseln, Angemessenheitsbeschluss, internationale Übereinkunft) |
| (f) | (f) Sperrung nicht mehr ausdrücklich erwähnt; hier sind Ihre Aufbewahrungsfristen (einschließlich Fristbeginn) anzugeben[27]; |
| (h) | (g) dies ist nur eine allgemeine Beschreibung der ergriffenen Maßnahmen; |

[27] Dies ist „wenn möglich“ anzugeben; nach dem Grundsatz der Speicherbegrenzung in Artikel 4 Absatz 1 Buchstabe e muss Ihre EU-Institution jedoch stets die Aufbewahrungsfrist angeben können („X Jahre ab Ereignis Z“). Wenn personenbezogene Daten rechtmäßig veröffentlicht werden und auf ewig öffentlich bleiben, ist dies ebenfalls anzugeben.

# 5 Listen gemäß Artikel 39 Absätze 4 und 5 sowie Vorlage für die Schwellenwertanalyse

Die hier wiedergegebene Entscheidung ist auf der Website des EDSB veröffentlicht.

---


EUROPEAN DATA PROTECTION SUPERVISOR

## ENTSCHEIDUNG DES EUROPÄISCHEN DATENSCHUTZBEAUFTRAGTEN VOM 16. JULI 2019 ÜBER GEMÄß ARTIKEL 39 ABSÄTZE 4 UND 5 DER VERORDNUNG (EU) 2018/1725 ERSTELLTE DSFA-LISTEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE,

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG[28], insbesondere auf Artikel 39 Absätze 4 und 5,

Nach Konsultation des Europäischen Datenschutzausschusses,

in Erwägung nachstehender Gründe:

(1) Die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union verarbeiten große Mengen personenbezogener Daten über natürliche Personen sowohl inner- als auch außerhalb der Institutionen. Diese Verarbeitung kann, auch wenn sie rechtmäßig erfolgt, Risiken für die Rechte und Freiheiten natürlicher Personen verursachen. Datenschutzvorschriften dienen dazu, sicherzustellen, dass personenbezogene Daten auf eine verantwortungsvolle Weise verarbeitet werden, die diese Risiken minimiert. Die Dokumentierungspflichten sind dem Risikoumfang angemessen – je höher das Risiko, das ein Verarbeitungsvorgang birgt, desto genauer ist er zu prüfen.

(2) Datenschutz-Folgenabschätzungen (DSFA) sind ein mit der Verordnung (EU) 2018/1725 (im Folgenden: Verordnung) neu eingeführter Begriff. Es handelt sich dabei um ein strukturiertes Verfahren für das Risikomanagement im Hinblick auf Datenschutzrisiken gewisser „hoher Risiken“ für die betroffene Person bergender Verarbeitungsvorgänge, das nicht für alle Arten von Verarbeitungsvorgängen erforderlich ist.

(3) In Artikel 39 Absatz 1 der Verordnung heißt es: „Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der

[28] ABl. L 295 vom 21.11.2018, S. 39-98.

Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch."

(4) Nach Artikel 39 Absatz 4 der Verordnung „erstellt [der EDSB] eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese".

(5) Nach Artikel 39 Absatz 5 der Verordnung kann der EDSB „des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist".

(6) Nach Artikel 39 Absatz 6 der Verordnung fordert der Europäische Datenschutzbeauftragte vor der Festlegung der in den Absätzen 4 und 5 des vorliegenden Artikels 39 genannten Listen den Europäischen Datenschutzausschuss auf, diese Listen gemäß Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 zu prüfen, wenn „sie sich auf Verarbeitungsvorgänge eines Verantwortlichen beziehen, der gemeinsam mit einem oder mehreren Verantwortlichen, die nicht Organe oder Einrichtungen der Union sind, tätig ist".

(7) Da Situationen, in denen Organe und Einrichtungen der Union gemeinsam oder allein Verantwortliche sind, nicht anders behandelt werden sollten als Situationen, in denen sie zusammen mit einem oder mehreren Verantwortlichen, die keine Organe und Einrichtungen der Union sind, gemeinsam Verantwortliche sind, hat der EDSB entschieden, eine einzige Liste gemäß Artikel 39 Absatz 4 zu erstellen. Allerdings deckt die Liste gemäß Artikel 39 Absatz 5 nur Situationen ab, in denen Organe oder Einrichtungen der Union die gemeinsam oder allein Verantwortlichen sind, ohne dass andere Verantwortliche als Organe und Einrichtungen der Union mitverantwortlich wären, da sich die dort aufgeführten Verarbeitungsvorgänge auf das interne Management der Organe oder Einrichtungen der Union beziehen.

(8) Laut dem fünften Erwägungsgrund der Verordnung sollten, „[s]oweit die Bestimmungen der vorliegenden Verordnung auf denselben Grundsätzen beruhen wie die der Verordnung (EU) 2016/679, … diese Bestimmungen der beiden Verordnungen … einheitlich ausgelegt werden, insbesondere da der Rahmen der vorliegenden Verordnung als dem Rahmen der Verordnung (EU) 2016/679 gleichwertig verstanden werden sollte".

(9) Schon bevor die Verordnung (EU) 2016/679 anwendbar wurde, hatte die Datenschutzgruppe nach Artikel 29 Leitlinien zu Artikel 35 der genannten Verordnung[29] herausgegeben, die denselben Grundsätzen folgen wie Artikel 39 der Verordnung. In diesen Leitlinien sind die Kriterien für die Feststellung eines „hohen Risikos" aufgeführt. In seiner ersten Plenarsitzung hat der Europäische Datenschutzausschuss (EDSA) die WP-29-Leitlinien zur DSGVO gebilligt[30].

(10) Die Leitlinien bestätigten, dass derartige Listen nicht erschöpfend sein könnten, sondern die Kriterien für die Beurteilung, ob hohe Risiken für die betroffenen Personen wahrscheinlich sind, auflisten würden. Soweit konkrete Verarbeitungsvorgänge erwähnt wurden, waren dies nur der Veranschaulichung

[29] Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", wp248rev.01, angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017.
[30] EDPB Endorsement 1/2018 (Billigung durch den Europäischen Datenschutzausschuss).

dienende Beispiele. Ist ein konkreter Verarbeitungsvorgang nicht in Anhang 2 aufgeführt, bedeutet das nicht, dass keine DSFA nötig ist. Ist umgekehrt ein bestimmter Verarbeitungsvorgang nicht in Anhang 3 aufgeführt, bedeutet das nicht, dass eine DSFA nötig ist.

(11) Im Februar 2018 hat der EDSB vorläufige Leitlinien zu den Dokumentierungspflichten[31] nach der – damals noch nicht angenommenen – Verordnung herausgegeben. Diese enthielten erste Angaben dazu, für welche Arten von Verarbeitungsvorgängen eine DSFA erforderlich sein würde, nach den von der Artikel-29-Datenschutzgruppe veröffentlichten und später vom EDSA gebilligten Leitlinien. Die vorliegende Liste baut auf den in dem Dokument enthaltenen Leitlinien für Verantwortliche auf.

(12) Der Entwurf der Liste wurde dem EDSA am 18. März 2019 vorgelegt; eine aktualisierte Fassung wurde am 21. Juni 2019 vorgelegt. Der EDSA hat darauf am 10. Juli 2019 erwidert[32]. Die endgültige Liste in ihrer angenommenen Fassung berücksichtigt sämtliche Empfehlungen des EDSA.

(13) Die Europäische Kommission kann mittels Durchführungsrechtsakten gemäß Artikel 40 Absatz 4 der Verordnung eine Liste der Fälle festlegen, in denen die Verantwortlichen den Europäischen Datenschutzbeauftragten konsultieren und seine vorherige Genehmigung einholen müssen. Damit der EDSB eine solide Entscheidungsgrundlage für eine solche Konsultation und Genehmigung hat, sollte der Verantwortliche auch in solchen Fällen eine DSFA durchführen.

HAT FOLGENDEN BESCHLUSS ERLASSEN:

*Artikel 1*

**Gegenstand und Anwendungsbereich**

1. In dieser Entscheidung wird eingehender erklärt, wann Verantwortliche gemäß der Verordnung (EU) 2018/1725 verpflichtet sind, eine Datenschutz-Folgenabschätzung (im Folgenden: DSFA) gemäß Artikel 39 der Verordnung durchzuführen.
2. Diese Entscheidung lässt die Vorschriften über Datenschutz-Folgenabschätzungen und vorherige Konsultation in den Artikeln 39 und 40 der Verordnung unberührt.

*Artikel 2*

**Anwendungsbereich und Begriffsbestimmungen**

1. Diese Entscheidung findet auf alle Verantwortlichen, die der Verordnung (EU) 2018/1725 unterliegen, Anwendung.

[31] Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies, erste, am 6. Februar 2018 veröffentlichte Fassung.
[32] Empfehlung 01/2019 zu der vom Europäischen Datenschutzbeauftragten entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz- Folgenabschätzung durchzuführen ist (Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725).

2. Für die Zwecke dieser Entscheidung gelten die Begriffsbestimmungen in Artikel 3 der Verordnung (EU) 2018/1725.

*Artikel 3*

**Verarbeitungsvorgänge, für die eine DSFA erforderlich ist [Artikel 39 Absatz 4 der Verordnung]**

1. Für die Beurteilung, ob für seine geplanten Verarbeitungsvorgänge die Durchführung einer DSFA gemäß Artikel 39 der Verordnung (EU) 2018/1725 vorgeschrieben ist, führt der Verantwortliche unter Verwendung der Vorlage in Anhang 1 zu dieser Entscheidung eine Schwellenwertanalyse durch.
2. Wenn mindestens zwei der in der Vorlage in Anhang 1 genannten Kriterien gegeben sind, ist der Verantwortliche im Allgemeinen verpflichtet, eine DSFA durchzuführen.
3. Sollte sich der Verantwortliche dafür entscheiden, keine DSFA durchzuführen, obwohl mehr als eines der Kriterien in der Vorlage in Anhang 1 gegeben sind, muss der Verantwortliche dies dokumentieren und seine Entscheidung begründen.
4. Sollte der geplante Verarbeitungsvorgang nur eines der Kriterien in der Vorlage in Anhang 1 erfüllen, kann sich der Verantwortliche dennoch dafür entscheiden, eine DSFA durchzuführen.
5. In Anhang 2 zu dieser Entscheidung sind einige übliche Verarbeitungsvorgänge aufgeführt, für die wahrscheinlich eine DSFA erforderlich ist. In solche Fällen braucht der Verantwortliche keine Schwellenwertanalyse durchzuführen, sondern kann sogleich eine DSFA durchführen.

*Artikel 4*

**Verarbeitungsvorgänge, für die die vorherige Konsultation erforderlich ist [Artikel 40 Absatz 4 der Verordnung]**

Wenn die Europäische Kommission Durchführungsrechtsakte gemäß Artikel 40 Absatz 4 der Verordnung (EU) 2018/1725 erlässt, die die Verantwortlichen verpflichten, den Europäischen Datenschutzbeauftragten zu konsultieren und seine vorherige Genehmigung einzuholen, müssen die Verantwortlichen auch DSFA für die in den Durchführungsrechtsakten aufgelisteten Verarbeitungsvorgänge durchführen.

*Artikel 5*

**Verarbeitungsvorgänge, für die keine DSFA erforderlich ist [Artikel 39 Absatz 5 der Verordnung]**

In Anhang 3 zu dieser Entscheidung sind einige übliche Verarbeitungsvorgänge aufgeführt, für die wahrscheinlich keine DSFA erforderlich ist.

*Artikel 6*

**Nicht erschöpfender Charakter der Listen**

Die dieser Entscheidung im Anhang beigefügten Listen von Verarbeitungsvorgängen sind nicht erschöpfend.

*Artikel 7*

**Inkrafttreten**

Diese Entscheidung tritt am Tag nach ihrer Veröffentlichung in Kraft.

Für den Europäischen Datenschutzbeauftragten

[gezeichnet]

Wojciech Rafał WIEWIÓROWSKI

*Anhang 1*

*Liste der Kriterien für die Beurteilung, ob Verarbeitungsvorgänge wahrscheinlich hohe Risiken zur Folge haben*

Allgemein gilt, dass der Verantwortliche eine DSFA durchführen sollte, wenn mindestens zwei der Kriterien in der Liste gegeben sind. Sollte der Verantwortliche der Ansicht sein, dass die Risiken im betreffenden Fall nicht „hoch" sind, obwohl für mehr als ein Kriterium „ja" angekreuzt wurde, muss der Verantwortliche erklären und begründen, warum die Verarbeitung seiner Meinung nach dennoch kein „hohes Risiko" darstellt. Für jedes Kriterium werden jeweils einige Beispiele und ein Gegenbeispiel angeführt, wann das betreffende Kriterium wahrscheinlich gegeben ist (bzw. wann nicht).

| **I Überschrift** | |
|---|---|
| Bezeichnung des Verarbeitungsvorgangs | [Name] |
| Kontaktstelle beim Verantwortlichen | [Funktion und Kontaktangaben] |
| Verzeichnis der Verarbeitungsvorgänge | [Aktenzeichen des Verzeichnisses] |
| Konsultation des Datenschutzbeauftragten | [Datum der Antwort] |
| Genehmigung | [Name und Datum] |
| II Kriterien dafür, wann eine Verarbeitung „wahrscheinlich hohe Risiken zur Folge hat" | |
| Kriterium | Anwendbar? Ja [ggf. angeben, inwiefern] / Nein [falls Grenzfall: Warum nicht?] |
| 1. Systematische und umfassende Bewertung persönlicher Aspekte oder Scoring, einschließlich Profiling und Prognosen. *Beispiele: eine Bank, die nach einschlägigem Recht systematische Überprüfungen (Screening) vornimmt, um etwaige betrügerische Geschäftsvorfälle aufzudecken; Profiling von Mitarbeitern auf Grundlage ihrer Geschäftsvorfälle in einem Fallverwaltungssystem mit automatischer Neuzuweisung von Aufgaben.* *Gegenbeispiele: Standardgespräche im Zuge der Mitarbeiterbeurteilung, freiwillige 360°-Beurteilungen, um Mitarbeitern bei der Entwicklung von Schulungsplänen zu helfen.* | [J (inwiefern?) / N] |
| 2. Automatisierte Entscheidungsfindung mit rechtlicher oder vergleichbarer erheblicher Wirkung: Verarbeitung, die darauf abzielt, Entscheidungen über die betroffenen Personen zu treffen. Beispiel: automatisierte Mitarbeiterbeurteilung („Wenn die Zahl der von Ihnen bearbeiteten Fälle zu den untersten 10 % im Team zählt, erhalten Sie die Note „ungenügend" in Ihrer Leistungsbeurteilung, ohne jede Diskussion"). | [J (inwiefern?) / N] |

| | | |
|---|---|---|
| | *Gegenbeispiel: eine Nachrichten-Website, auf der die Reihenfolge der angezeigten Artikel sich nach früheren Besuchen des Nutzers richtet.* | |
| 3. | Systematische Überwachung: Die Verarbeitung erfolgt, um betroffene Personen zu beobachten, zu überwachen oder zu kontrollieren, insbesondere in allgemein zugänglichen Bereichen. Dabei kann es sich um Videoüberwachung handeln, aber auch um sonstige Formen der Überwachung, z. B. die Internetnutzung durch die Mitarbeiter.<br>*Beispiele: verdeckte Videoüberwachung, smarte Videoüberwachung in allgemein zugänglichen Bereichen, Data-Loss-Prevention-Tools, die in die SSL-Verschlüsselung eingreifen, Bewegungsverfolgung über Geodaten.*<br>*Gegenbeispiel: offene Videoüberwachung einer Garageneinfahrt, die keinen öffentlichen Raum erfasst.* | [J (inwiefern?) / N] |
| 4. | Sensible Daten oder Daten höchstpersönlicher Art: Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person, strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten oder Daten höchstpersönlicher Art.<br>*Beispiele: Vor der Einstellung vorgenommene Gesundheitsprüfungen und polizeiliche Führungszeugnisse, Verwaltungsuntersuchungen und Disziplinarverfahren, jeder Einsatz von biometrischer Identifikation (1:n).*<br>*Gegenbeispiel: Fotos an sich sind keine sensiblen Daten (nur in Verbindung mit Gesichtserkennung / Biometrik oder bei Verwendung zur Ableitung anderer sensibler Daten).* | [J (inwiefern?) / N] |
| 5. | Umfangreiche Datenverarbeitung, sei es im Hinblick auf die Anzahl der betroffenen Personen und/oder die Menge der über jede von ihnen verarbeiteten Daten und/oder die Dauerhaftigkeit und/oder die geografische Abdeckung.<br>*Beispiel: Europäische Datenbanken zur Krankheitsüberwachung.*<br>*Gegenbeispiel: In einer mittelgroßen EU-Institution stattfindendes Verfahren gemäß Artikel 78 des Statuts der Beamten wegen Invalidität.* | [J (inwiefern?) / N] |
| 6. | Abgleich oder Kombination von Datenmengen mit solchen aus anderen Datenverarbeitungsvorgängen, die für andere Zwecke und/oder von anderen für die Verarbeitung Verantwortlichen durchgeführt wurden, soweit Abgleich oder Kombination auf eine Weise erfolgen, die für die betroffene Person angemessenerweise nicht zu erwarten war.<br>*Beispiele: Abgleich von Daten aus der Zugangskontrolle mit den selbst angegebenen Arbeitsstunden nach Betrugsverdacht wegen Einlassungen, die in einer (nach den einschlägigen Vorschriften durchgeführten) Verwaltungsuntersuchung gemacht wurden.*<br>*Gegenbeispiel: Weitere Nutzung der für einen Förderungsantrag verarbeiteten Daten im Zuge der Überprüfung des Gewährungsverfahrens.* | [J (inwiefern?) / N] |
| 7. | Daten schutzbedürftiger betroffener Personen: Situationen, in denen ein Ungleichgewicht im Verhältnis zwischen der betroffenen Person und dem Verantwortlichen festgestellt werden kann.<br>*Beispiele: Kinder, Asylsuchende.*<br>*Gegenbeispiele: Delegierte in einer Ratsarbeitsgruppe (für Anwesenheitslisten), Mitglieder von Expertengruppen (für* | [J (inwiefern?) / N] |

| | |
|---|---|
| *die Erstattung der Reisekosten).* | |
| 8. Innovative Nutzung oder Anwendung technischer oder organisatorischer Lösungen, die unter Umständen neuartige Formen der Datenerfassung und Datennutzung vorsehen. In der Tat kann es sein, dass die persönlichen und gesellschaftlichen Folgen des Einsatzes neuer Technologie nicht bekannt sind. Beispiele: maschinelles Lernen, vernetzte Autos, Social-Media-Screening von Stellenbewerbern.<br>*Gegenbeispiel: Biometrische Zugangskontrolle (1:1) mittels Fingerabdruck.* | [J (inwiefern?) / N] |
| 9. Hinderung betroffener Personen an der Rechtsausübung, Inanspruchnahme von Dienstleistungen bzw. Vertragsdurchführung.<br>*Beispiele: Ausschlussdatenbanken, Bonitätsprüfung.*<br>*Gegenbeispiel: Feststellung zustehender Ansprüche bei Diensteintritt (z. B. Ansprüche auf Zulagen wegen Expatriierung oder unterhaltsberechtigter Kinder).* | [J (inwiefern?) / N] |
| **III Ergebnis** | |
| Anzahl der oben angekreuzten „Ja“ | [n] |
| Bewertung: Grundsätzlich sollten Sie, wenn mindestens zwei der Kriterien angekreuzt sind, eine DSFA durchführen. Sollten Sie der Ansicht sein, dass die Risiken im betreffenden Fall nicht „hoch“ sind, obwohl für mehr als ein Kriterium „ja“ angekreuzt wurde, müssen Sie erklären und begründen, warum die Verarbeitung Ihrer Meinung nach dennoch kein „hohes Risiko“ darstellt. | [Erklärung] |

*Anhang 2*

*Nicht erschöpfende Liste einiger üblicher Verarbeitungsvorgänge und mögliche Anzeichen für damit verbundene Risiken*

**Positivliste der Verarbeitungsvorgänge, für die prima facie eine DSFA erforderlich ist** (die in Klammern angegebenen Zahlen beziehen sich auf die Kriterien in der Vorlage für die Schwellenwertanalyse in Anhang 1, die bei derartigen Verarbeitungsvorgängen wahrscheinlich gegeben sein werden):

- Ausschlussdatenbanken (2, 4, 9);
- umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Krankheitsüberwachung, Pharmakovigilanz, zentrale Datenbanken für Zusammenarbeit im Bereich der Strafverfolgung) (1, 4, 5, 8);
- Internet-Verkehrsanalyse, die in die SSL-Verschlüsselung eingreift (Data-Loss-Prevention-Tools) (1, 3, 8);
- Online-Instrumente zur Personalauswahl mit automatischer Vorauswahl / automatischem Ausschluss von Bewerbern, ohne menschliches Eingreifen (1, 2, 8).

*Anhang 3*

*Nicht erschöpfende Liste einiger üblicher Verarbeitungsvorgänge, für die keine DSFA erforderlich ist*

**Liste mit Beispielen für Verarbeitungsvorgänge, für die prima facie keine DSFA erforderlich ist, wenn sie von Organen, Einrichtungen und sonstigen Stellen der Union durchgeführt werden, die als allein oder gemeinsam Verantwortliche handeln:**

- Verwaltung der Personalakten gemäß Artikel 26 des Statuts der Beamten *als solche*[33];
- Standardverfahren zur Mitarbeiterbeurteilung auf Grundlage des Statuts der Beamten (jährliche Beurteilung);
- Standard-360°-Beurteilungen, um den Mitarbeitern bei der Entwicklung von Schulungsplänen zu helfen;
- Standardverfahren für die Personalauswahl;
- Feststellung zustehender Ansprüche bei Diensteintritt;
- Verwaltung von Urlaubsansprüchen, Gleitzeit und Telearbeit;
- Standardsysteme für die Zugangskontrolle (nicht biometrisch)[34];
- Standard-Videoüberwachung in begrenztem Umfang (keine Gesichtserkennung, Erfassung auf Eingang/Ausgang beschränkt, nur auf eigenem Gelände, nicht im öffentlichen Raum).

[33] Für einige Verfahren, durch die die Personalakte um Informationen ergänzt wird, können DSFA erforderlich sein, nicht jedoch für die Personalakte an sich.
[34] Z. B. am Eingang aufzulegende Badges.

# 6 Referenzdokumente

## Von Mitgliedern des Europäische Datenschutzausschusses herausgegebene Leitlinien über Verzeichnisse

Einige Mitglieder des Europäische Datenschutzausschusses haben Leitlinien und Erläuterungen dazu herausgegeben, wie die Verzeichnisse der Verarbeitungsvorgänge nach der DSGVO funktional äquivalenten Vorschriften zu führen sind:

- Belgischer Ausschuss für den Schutz des Privatlebens: Erläuterung (FR/NL) & Vorlage registrieren (FR/NL)
- Dänemark: Datatilsynet: Vejledning om fortegnelse (Januar 2018)
- Deutschland (Datenschutzkonferenz): Hinweise zum Verzeichnis von Verarbeitungstätigkeiten & Vorlage für Verantwortliche / Auftragsverarbeiter
- Griechenland: Hellenic Data Protection Authority: Erläuterung zu Registern & Vorlagen für Verantwortliche / Auftragsverarbeiter.
- Vereinigtes Königreich: Information Commissioner's Office: Erläuterung und Vorlage

# 7 Glossar

In diesem Glossar werden einige der im Toolkit verwendeten Datenschutzbegriffe erklärt.

| | |
|---|---|
| (die) Verordnung | Verordnung (EU) 2018/1725 |
| Alte Verordnung | Verordnung (EG) Nr. 45/2001 |
| Angemessene Garantien | Maßnahmen, die bei der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisation ein angemessenes Schutzniveau bieten, z. B. Standardvertragsklauseln. |
| Angemessenheits-beschluss | Die Europäische Kommission kann beschließen, dass ein Drittland ein angemessenes Datenschutzniveau bietet. Datenübermittlungen in Drittländer mit angemessenem Schutzniveau bedürfen keiner zusätzlichen Schutzmaßnahmen, sondern sind so wie Übermittlungen an Empfänger innerhalb der EU zu behandeln. Nähere Informationen dazu, siehe Kapitel V der Verordnung. |
| Auftragsverarbeiter | eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Beispiel: ein Unternehmen, das für Ihre EU-Institution auf Grundlage eines Outsourcing-Vertrags ein Assessment-Center durchführt. |
| Behördlicher Datenschutz-beauftragter (DSB) | Der Datenschutzbeauftragte informiert und berät den Verantwortlichen / die EU-Institution, die Mitarbeiter der EU-Institution und die betroffenen Personen über Datenschutzangelegenheiten und stellt die interne Anwendung der Datenschutzvorschriften in seiner EU-Institution sicher; dabei handelt er unabhängig. Datenschutzbeauftragte sind auch die Hauptkontaktstellen zwischen den EU-Institutionen und dem Europäischen Datenschutzbeauftragten (EDSB). Jede EU-Institution hat einen Datenschutzbeauftragten. |

| | |
|---|---|
| Besondere Datenkategorien | Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person; Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person (Artikel 10 der Verordnung); Daten über strafrechtliche Verurteilungen und Straftaten (Artikel 11 der Verordnung). |
| Betroffene Person | Jede natürliche Person, deren personenbezogene Daten man verarbeitet, unabhängig davon, ob sie in der eigenen EU-Institution beschäftigt ist oder nicht. |
| Datenqualität | Siehe Artikel 4 der Verordnung. |
| Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen | Der Grundsatz, dass die Verantwortlichen den Datenschutz sowohl bei der Entwicklung als auch beim Einsatz berücksichtigen und Standardschutzeinstellungen vorsehen müssen (Artikel 27 der Verordnung). |
| Datenschutzbehörde (DSB) | Für die Aufsicht über die Verarbeitung personenbezogener Daten zuständige Behörde. Der EDSB ist die Datenschutzbehörde für die EU-Institutionen. |
| Datenschutz-Folgenabschätzung (DSFA) | Ein strukturiertes Verfahren für das Risikomanagement im Hinblick auf den Datenschutz bei bestimmten risikoträchtigen Verarbeitungsvorgängen (Artikel 39). |
| Datenschutz-Grundverordnung (DSGVO) | Verordnung (EU) 2016/0679. In der DSGVO sind die Datenschutzvorschriften niedergelegt, die in den Mitgliedstaaten der EU für Verantwortliche im Privatsektor sowie in den meisten Teilen des öffentlichen Sektors gelten (außer im Bereich der Strafverfolgung). |
| Datenschutzhinweis | Jeder Hinweis, der die betroffenen Personen darüber informiert, auf welche Weise der Verantwortliche ihre personenbezogenen Daten verarbeitet (Artikel 14 bis 16 der Verordnung). |
| Datenschutz-koordinator | Einige größere EU-Institutionen haben in jeder Generaldirektion oder ähnlichen Organisationseinheit Datenschutzkoordinatoren als lokale Kontaktstellen. Datenschutzkoordinatoren (DSK) unterstützen den Datenschutzbeauftragten (DSB). |
| Drittland | Länder, die nicht der EU oder dem EWR angehören; die Übermittlung personenbezogener Daten in Drittländer erfordert unter Umständen zusätzliche Schutzmaßnahmen. |
| Durchführungs-verantwortlicher aufseiten des für die Verarbeitung Verantwortlichen | Als für die Datenverarbeitung Verantwortlicher ist Ihre EU-Institution für die Verarbeitungsvorgänge rechenschaftspflichtig; wobei jedoch in der Regel die Ausführungsverantwortung auf einer niedrigeren Ebene wahrgenommen wird, z. B. von Personen in dem für eine bestimmte Verarbeitungstätigkeit zuständigen |

| | |
|---|---|
| | Geschäftsbereich. |
| Einschränkung der Verarbeitung | Die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken (Artikel 4 Ziffer 3 DSGVO). |
| Einwilligung | Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. |
| Europäischer Datenschutzausschuss (EDSA) | Das Forum, in dem die nationalen Datenschutzbehörden, der Europäische Datenschutzbeauftragte (EDSB) und die Kommission zusammenarbeiten, um die unionsweit einheitliche Anwendung der Datenschutzvorschriften sicherzustellen. Er ersetzte die WP29. |
| Europäischer Datenschutz-beauftragter (EDSB) | Die Datenschutzbehörde für die EU-Institutionen (siehe Verordnung). |
| Informations-sicherheits-Risikomanagement (ISRM) | Der Risikomanagementprozess, durch den sichergestellt wird, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Vermögenswerte einer Organisation auf die Ziele der Organisation abgestimmt sind. |
| Integrität | Genauigkeit und Vollständigkeit |
| Kontrolle | In ISRM-Terminologe eine Maßnahme zur Risikomodifizierung. |
| Meldung von Verletzungen des Schutzes personenbezogener Daten | Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten (von Datenschutzverletzungen) an die Datenschutzbehörde. |
| Meldung zur Vorabkontrolle | Meldung an den EDSB gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001. |
| Organe und Einrichtungen der Union (EU-Institutionen) | Oberbegriff für alle der Verordnung unterliegenden Organe, Einrichtungen und sonstigen Stellen der Union. |
| Personenbezogene Daten | Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Artikel 4 Ziffer 1 DSGVO). Betroffene |

| | |
|---|---|
| | Personen können direkt (z. B. durch Namen) oder indirekt (z. B. „eine maltesische Generaldirektorin in Ihrer EU-Institution“) identifizierbar sein. |
| Profiling | Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Artikel 4 Ziffer 4 DSGVO). |
| Rechenschaftspflicht | Ein Grundsatz, der sicherstellen soll, dass die Verantwortlichen allgemein die Kontrolle innehaben und in der Lage sind, die Einhaltung der datenschutzrechtlichen Grundsätze in der Praxis zu garantieren und nachzuweisen. Die Rechenschaftspflicht erfordert, dass die Verantwortlichen interne Mechanismen und Kontrollsysteme einrichten, die die Vorschriftseinhaltung sicherstellen und z. B. durch Prüfberichte Beweis dafür liefern, um die Einhaltung gegenüber externen Stellen, einschließlich Aufsichtsbehörden, nachzuweisen. |
| Recht auf Auskunft | Betroffene Personen haben das Recht, vom Verantwortlichen Auskunft über die personenbezogenen Daten zu verlangen, die er über sie hält; Ausnahmen von diesem Grundsatz sind möglich (Artikel 17 der Verordnung). |
| Recht auf Berichtigung | Betroffene Personen haben das Recht auf Berichtigung der personenbezogenen Daten, die ein Verantwortlicher über sie hält, wenn die Daten unrichtig sind (Artikel 18 der Verordnung). |
| Recht auf Löschung / Recht auf Vergessenwerden | Betroffene Personen haben unter bestimmten Voraussetzungen das Recht, die Löschung der personenbezogenen Daten zu verlangen, die ein Verantwortlicher über sie hält, wenn zum Beispiel die Daten rechtswidrig gehalten werden (Artikel 19 der Verordnung). |
| Recht auf Unterrichtung | Sie sind verpflichtet, betroffene Person darüber zu unterrichten, dass Sie deren personenbezogene Daten verarbeiten. Die Unterrichtung der betroffenen Personen kann durch Datenschutzhinweis oder Datenschutzerklärung erfolgen. |
| Rechtmäßigkeit der Verarbeitung | Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn und soweit mindestens eine der in Artikel 5 der Verordnung aufgeführten Bedingungen erfüllt ist, z. B. wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Organ oder der Einrichtung der Union durch Unionsrecht übertragen wurde. |
| Restrisiko | Nach der Risikobehandlung verbleibendes Risiko. |

| | |
|---|---|
| Risiko | Ein mögliches Ereignis, das Schäden oder Verluste verursacht oder das Erreichen der Ziele gefährden könnte. Risiken haben eine Auswirkung und eine Eintrittswahrscheinlichkeit. Kann auch als Auswirkung von Unsicherheit auf Ziele definiert werden. |
| Risikobehandlung | Anwendung einer Risikokontrollmaßnahme auf ein Risiko. |
| Risikomanagement | Das Verfahren zur Feststellung, Bewertung und Kontrolle / Behandlung von Risiken. |
| Schwellenwertanalyse | Vom Verantwortlichen mithilfe des Datenschutzbeauftragten durchgeführte Beurteilung, ob eine Datenschutz-Folgenabschätzung erforderlich ist. |
| Verantwortlicher | das Organ oder die Einrichtung der Union oder die Generaldirektion oder sonstige Organisationseinheit, das beziehungsweise die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten bestimmt; sind die Zwecke und Mittel dieser Verarbeitung durch einen besonderen Rechtsakt der Union bestimmt, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien für seine Benennung nach dem Unionsrecht vorgesehen werden (Artikel 3 Absatz 2 Buchstabe b der Verordnung). |
| Verarbeitung | Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Artikel 4 Ziffer 2 DSGVO). |
| Verfügbarkeit | Befugte Stellen können auf Anfrage Zugang zu den Informationen haben und sie nutzen. |
| Verletzung des Schutzes personenbezogener Daten / Datenschutzverletzungen | Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. |
| Vertraulichkeit | Informationen werden für unbefugte Personen, Stellen oder Verfahren weder bereitgestellt noch offengelegt. |
| Verzeichnis | Dokumentierung Ihrer Verarbeitungsvorgänge (Artikel 31 der Verordnung). |