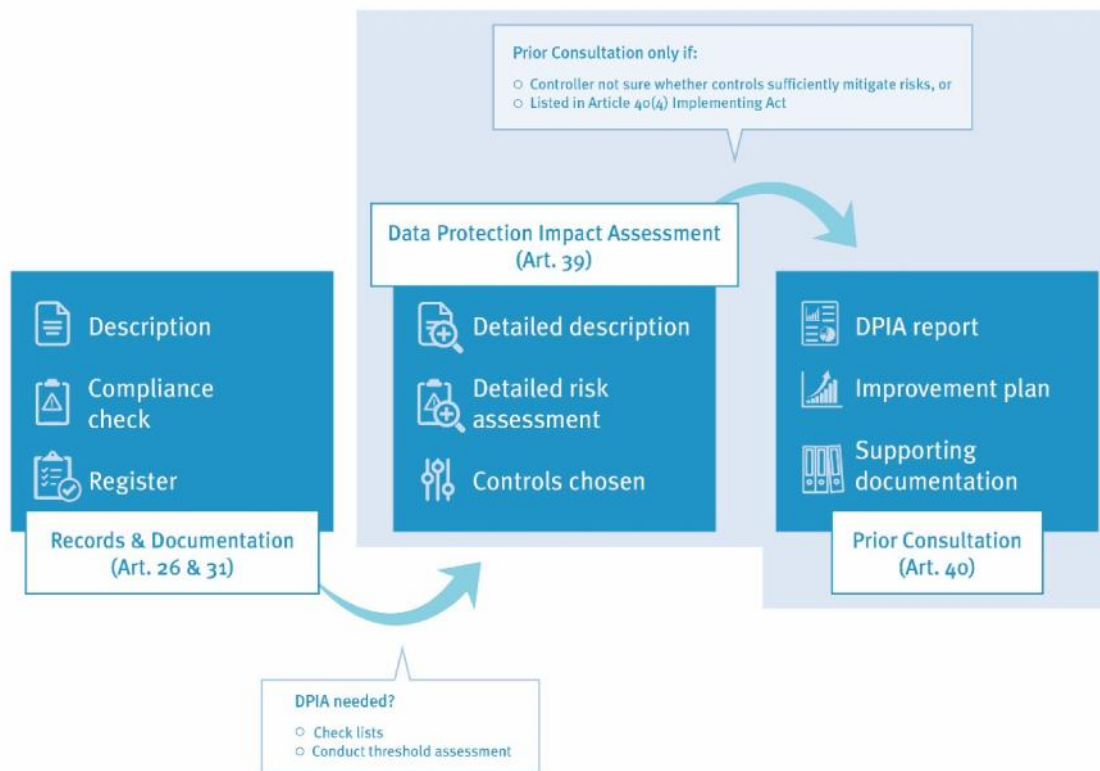


DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE (EDSB)

Rechenschaftspflicht in der Praxis Teil II: Datenschutz- Folgenabschätzung und vorherige Konsultation



v1.3 Juli 2019



Prior Consultation only if:	Vorherige Konsultation nur, wenn:
Controller not sure whether controls sufficiently mitigate risks, or Listed in Article 40 (4) Implementing Act	Verantwortlicher nicht sicher, ob Kontrollmaßnahmen ausreichen, oder 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

1. Einleitung und Gegenstand von Teil II	3
2. Verantwortlichkeiten – wer macht was?	4
3. Durchführung von Datenschutz-Folgenabschätzungen (DSFA)	5
3.1 GRUNDANFORDERUNGEN AN DIE DATENSCHUTZ-FOLGENABSCHÄTZUNG UND METHODENWAHL	6
3.2 BESCHREIBUNG DER VERARBEITUNG	8
3.3 BEWERTUNG DER NOTWENDIGKEIT UND VERHÄLTNISSMÄßIGKEIT	9
3.4 RISIKOBEWERTUNG	9
3.5 LEITFRAGEN ZU DEN DATENSCHUTZGRUNDSÄTZEN	13
3.6 RISIKOBEHANDLUNG	20
3.7 DOKUMENTIERUNG UND BERICHTERSTATTUNG	22
3.8 ÜBERPRÜFUNGSZYKLEN	22
3.9 VERÖFFENTLICHUNG VON DSFA-BERICHTEN	23
4. In welchen Fällen ist eine vorherige Konsultation durchzuführen?	23
5. Was ist zu tun?	26
6. Schlusswort	26
Anhänge	28
1. AUFGABENVERTEILUNG	28
2. LEITFRAGENKATALOG ZU DEN DATENSCHUTZGRUNDSÄTZEN	28
3. GLIEDERUNG DER VORLAGE FÜR DEN DSFA-BERICHT	31
4. REFERENZDOKUMENTE	33
5. GLOSSAR	34

Abbildungsverzeichnis

Abbildung 1: Überblick über die Dokumentierungspflichten	3
Abbildung 2: RACI-Matrix zum DSFA-Prozess	5
Abbildung 3: Allgemeiner DSFA-Prozess	7
Abbildung 4: Datenschutzgrundsätze in der Verordnung	12
Abbildung 5: Relevanz der Schutzziele für die Schritte im Datenflussdiagramm	13
Abbildung 6: Leitfragen zur Verarbeitung nach Treu und Glauben	15
Abbildung 7: Leitfragen zur Transparenz	15
Abbildung 8: Leitfragen zur Zweckbindung	16
Abbildung 9: Leitfragen zur Datenminimierung	17
Abbildung 10: Leitfragen zur Richtigkeit	17
Abbildung 11: Leitfragen zur Speicherbegrenzung	18
Abbildung 12: Leitfragen zur Sicherheit	19
Abbildung 13: Liste mit Beispielen für allgemeine Risikokontrollen, geordnet nach Schutzziele	22
Abbildung 14: Zusammenspiel: Verzeichnisse – DSFA – vorherige Konsultation	25

1. Einleitung und Gegenstand von Teil II

Wenn die Verarbeitung mit „hohen Risiken“ verbunden ist, sind Sie – als Durchführungsverantwortlicher aufseiten des für die Verarbeitung Verantwortlichen – für die Risikoanalyse und Risikokontrolle zuständig, die mittels Datenschutz-Folgenabschätzungen (DSFA) vorzunehmen ist. Teil II des Toolkits Rechenschaftspflicht in der Praxis zeigt Ihnen, wie dabei vorzugehen ist. In manchen Fällen ist auch die vorherige Konsultation des Europäischen Datenschutzbeauftragten (EDSB) erforderlich, die hierin ebenfalls behandelt wird. In Teil I des Toolkits Rechenschaftspflicht in der Praxis haben Sie bereits gesehen, wie man Verzeichnisse und die dazugehörigen Unterlagen erstellt und in welchen Fällen eine DSFA erforderlich ist.

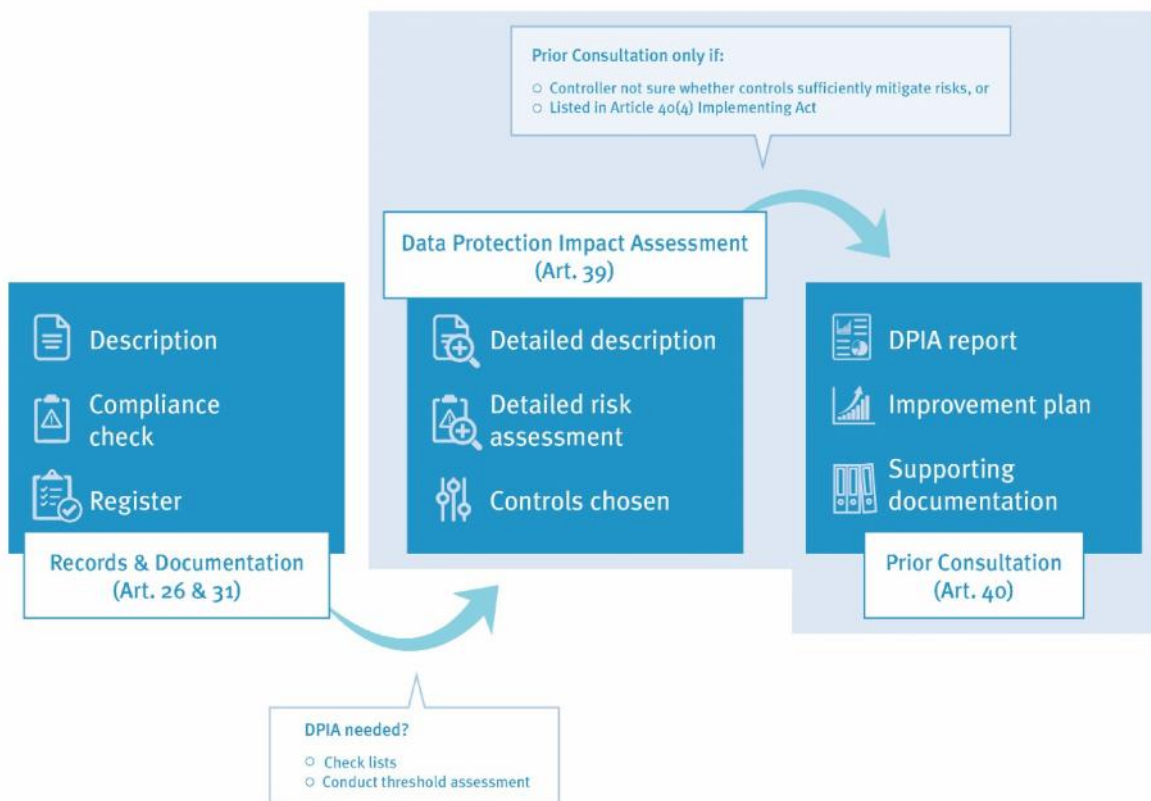


Abbildung 1: Überblick über die Dokumentierungspflichten

Gemäß Artikel 39 Absatz 1 der Verordnung¹ kann „[f]ür die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken ... eine einzige Abschätzung vorgenommen werden“. Derartige „gemeinsame“ **DSFA können in Betracht kommen, wenn mehrere EU-Institutionen Verarbeitungsvorgänge auf dieselbe Weise implementieren**, z. B. weil sie für bestimmte Verfahren denselben Vorschriften unterliegen oder weil sie bestimmte Produkte auf dieselbe Weise benutzen.

Wenn der DSFA-Bericht ergibt, dass noch **hohe Restrisiken** bestehen (oder wenn die Verarbeitung unter denen aufgelistet ist, für die eine vorherige Konsultation obligatorisch ist), schreibt Artikel 40 vor, dass eine Konsultation des EDSB erforderlich ist (siehe dazu nachstehend Abschnitt 4).

¹ ABl. L 295/39 vom 21.11.2018.

Dieses Dokument umfasst folgende Aspekte:

-) wie man DSFA durchführt;
-) in welchen Fällen die Datenschutz-Folgenabschätzung dem Europäischen Datenschutzbeauftragten (EDSB) im Zuge der vorherigen Konsultation zuzusenden ist;
-) wer in den obigen Prozessen wofür zuständig ist;
-) sowie die die DSFA und vorherige Konsultation betreffenden Vorschriften für den Übergang von der alten Verordnung (EU) 45/2001 zur neuen Datenschutzverordnung für die EU-Institutionen.

Informationen darüber, wie Sie Verzeichnisse erstellen und herausfinden, ob eine DSFA erforderlich ist, finden Sie dagegen in Teil I.

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 in erster Linie zuständig, wobei Ihnen der Datenschutzbeauftragte (DSB) assistiert (und auch der Datenschutzkoordinator (DPK), falls Ihre EU-Institution einen solchen hat)³.

Sollten Sie eine DSFA durchführen müssen, ist es gemäß Artikel 39 der Verordnung auch die Aufgabe des Verantwortlichen (in der Praxis: Rechenschaftspflicht der obersten Verwaltungsebene, Durchführungsverantwortung des im Geschäftsbereich Zuständigen), den Rat des DSB einzuholen. Der Grund dafür ist, dass **die Verantwortlichen als die Rechenschaftspflichtigen auch für den DSFA-Prozess zuständig sein müssen**. Allerdings sind die DSB häufig diejenigen, die in der Organisation über das größte Fachwissen über Datenschutz verfügen und deshalb im DSFA-Prozess Anleitung und Hilfe geben können.

Verantwortung und Rechenschaftspflicht für den DSFA-Prozess liegen bei den für die Verarbeitung Verantwortlichen, doch die DSB können dabei eine wichtige Rolle spielen, indem sie die Verantwortlichen durch den Prozess führen.

Die die DSFA betreffenden Verantwortlichkeiten der verschiedenen Rollen in Ihrer Organisation sind nachstehend aufgeführt:

² Artikel 3 Ziffer 8 der 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.

	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
Oberste Verwaltungsebene		X		
Im Geschäftsbereich zuständige Person	X			
DSB			X	
IT-Abteilung			X	
ggf. Auftragsverarbeiter			X	
Vertreter der betroffenen Person			(X)	

Abbildung 2: RACI-Matrix zum DSFA-Prozess

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 die IT-Abteilung die technische Infrastruktur bereitstellen; sie wird sich auch am besten mit den die Informationssicherheit betreffenden Aspekten auskennen.

In geeigneten Fällen sind auch Vertreter der betroffenen Personen zu konsultieren. Betrifft die Verarbeitung Bedienstete der EU-Institution, ist dies zumeist die Personalvertretung. Wenn Personen außerhalb ihrer EU-Institution betroffen sind, muss der Verantwortliche unter Umständen Lösungen finden, auch deren Meinungen einzuholen, wenn dies geboten ist. **Eine öffentliche Konsultation aller betroffenen Parteien ist jedoch nicht unbedingt erforderlich.** Wenn Ihre EU-Institution beispielsweise Nutzern der öffentlichen Verwaltungen der Mitgliedstaaten ein System anbietet, in dem personenbezogene Daten der Nutzer verarbeitet werden, müssen Sie unter Umständen Vertreter des Nutzerkreises konsultieren – z. B. über den Lenkungsausschuss für das System oder ähnliche Gremien. In der Konsultation ist den Vertretern der betroffenen Personen eine angemessene Frist zur Stellungnahme zu geben.

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 allem zur Seite stehen – wobei allerdings Verantwortung und Rechenschaftspflicht letztendlich beim für die Verarbeitung 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. Durchführung von Datenschutz-Folgenabschätzungen (DSFA)

3.1 Grundanforderungen an die Datenschutz-Folgenabschätzung und Methodenwahl

Der DSFA-Prozess soll gewährleisten, dass die Verantwortlichen (die hier durch Sie als den Durchführungsverantwortlichen aufseiten des Verantwortlichen / im Geschäftsbereich Zuständigen vertreten sind) angemessene Maßnahmen gegen die mit „riskanten“ Verarbeitungsvorgängen verbundenen Risiken im Hinblick auf den Schutz der Privatsphäre und Datenschutz ergreifen. **Durch eine strukturierte Herangehensweise an die Risiken für die betroffenen Personen und deren Eindämmung helfen Datenschutz-Folgenabschätzungen den Organisationen, die Anforderung des „Datenschutzes durch Technik“ zu erfüllen**, wo sie am dringendsten benötigt wird, d. h. bei „riskanten“ Verarbeitungsvorgängen.

Für die Durchführung der Datenschutz-Folgenabschätzung sind Sie als der im Geschäftsbereich Zuständige für den zur Bewertung stehenden Verarbeitungsvorgang verantwortlich; der Datenschutzbeauftragte Ihrer EU-Institution kann Ihnen jedoch im gesamten Verfahren Hilfe leisten. Wenn Sie in einer Verfahrensphase Rat brauchen, ist der Datenschutzbeauftragte Ihrer EU-Institution Ihr erster Ansprechpartner. Sie sollten den Datenschutzbeauftragten Ihrer EU-Institution auch in jeder Phase des DSFA-Prozesses konsultieren.

Artikel 39 Absatz 6 der Verordnung bestimmt, dass die Datenschutz-Folgenabschätzung mindestens Folgendes enthalten muss:

„a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

(b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf die Zwecke,

(c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

(d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Es gibt für die EU-Institutionen keine vom **Europäischen Datenschutzbeauftragte vorgeschriebene Standardmethode für die Durchführung von Datenschutz-Folgenabschätzungen**. Allerdings **muss die verwendete Methode den Anforderungen aus der Verordnung genügen** und auch denen, die sich aus den von der Artikel-29-Datenschutzgruppe herausgegebenen und vom EDSA gebilligten Leitlinien für DSFA⁴ ergeben, die die entsprechenden Bestimmungen der DSGVO auslegen. Den EU-Institution können unter den diese Anforderungen erfüllenden Methoden frei wählen. Viele Mitglieder des EDSA haben bereits DSFA-Methoden oder werden solche künftig bereitstellen. Möglicherweise werden auch Normungsorganisationen und Branchenverbände Vorlagen ausarbeiten.

⁴ Wp248rev.01, 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“, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Als Hilfe gibt der **Europäische Datenschutzbeauftragte ein Beispiel** für die allgemeinen Grundsätze der DSFA-Prozesse, das auch eine Vorlage für die Berichtsgliederung enthält (siehe Anhang 3). Einige andere Methoden sind im ersten Teil von Anhang 4 aufgeführt.

Der Europäische Datenschutzbeauftragte schreibt den EU-Institutionen keine bestimmte DSFA-Methode vor. Sie können jede den Vorschriften genügende Methode, das vom EDSB in diesem Dokument gegebene Beispiel oder jede sonstige Methode verwenden, die den von der Artikel-29-Datenschutzgruppe / dem EDSA herausgegebenen Leitlinien genügt.

Eine Datenschutz-Folgenabschätzung ist ein **zyklischer Prozess** und keine einmalige Maßnahme. Wenn Sie im Zuge der Entwicklung eines neuen Verarbeitungsvorgangs eine Datenschutz-Folgenabschätzung durchführen, ist sie nicht mit der Annahme und Einführung des Verarbeitungsvorgangs beendet. Mit jeder Änderung des Verarbeitungsvorgangs ändert sich die Risikoumgebung. Deshalb müssen Sie bei Änderungen, aber auch in bestimmten zeitlichen Abständen überprüfen, ob Ihre Datenschutz-Folgenabschätzung immer noch den Gegebenheiten entspricht. Falls nicht, müssen Sie sie aktualisieren.

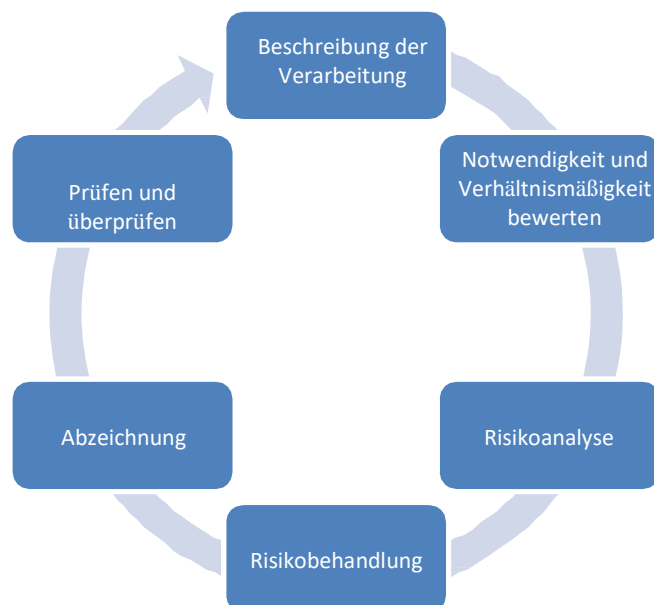


Abbildung 3: Allgemeiner DSFA-Prozess

Einfach gesagt, steht am Anfang die Beschreibung Ihrer Verarbeitung – „**Was tun wir und wie tun wir es?**“ Hier brauchen Sie eine ausführlichere Fassung der im Verzeichnis für den Verarbeitungsvorgang enthaltenen Angaben, einschließlich Datenflussdiagramm. Außerdem ist zu erklären, warum Ihre Organisation diesen Verarbeitungsvorgang durchführen muss und auf welche Weise Sie sich auf das für das Ziel der Verarbeitung Notwendige beschränken (Notwendigkeit und Verhältnismäßigkeit) – „**Wozu tun wir dies?**“ Danach bewerten Sie die Risiken, die sich durch die Verarbeitung ergeben. Dies sind zum einen die Risiken für die betroffenen Personen – „**Welche Auswirkungen wird dies, wenn alles planmäßig funktioniert, auf die betroffenen Personen haben? Welche Auswirkungen wird dies haben, wenn es nicht planmäßig funktioniert?**“, zum anderen die Compliance-Risiken für Ihre EU-Institution – „**Dürfen wir das? Gibt es bestimmte Verpflichtungen, die wir erfüllen müssen?**“ Sodann wählen Sie angemessene Maßnahmen gegen die festgestellten Risiken –

„Was tun wir dagegen?“ Diesen Prozess müssen Sie jeweils vollständig dokumentieren und darüber Bericht erstatten – **„... und alles aufschreiben“**. Wenn Sie dann ans Ende des ersten (bzw. späteren) Zyklus dieses Prozesses gelangen, holen Sie die Genehmigung des zuständigen Vorgesetzten ein. Zu guter Letzt müssen Sie ein Auge darauf behalten, ob die gewählten Maßnahmen funktionieren, und auf Änderungen Ihrer Umgebung und/oder des Prozesses achten – **„Funktioniert das? Entspricht die Darstellung immer noch dem, was wir jetzt tatsächlich tun?“** Erforderlichenfalls ist die Dokumentation zu aktualisieren. Anhang 3 enthält eine Vorlage für die Gliederung des DSFA-Berichts.

3.2 Beschreibung der Verarbeitung

Die Grundlage eines soliden DSFA-Prozesses ist es, den Kontext festzustellen und den Verarbeitungsvorgang zu beschreiben. Kurz gesagt: Sie müssen beschreiben, was Sie zu tun beabsichtigen und wie Sie es zu tun planen.

Aus dieser Dokumentierung sollte für den Leser – sei es für von der Verarbeitung Betroffene, Ihre eigene oberste Verwaltungsebene, die den DSFA-Bericht abzeichnen muss, den Europäischen Datenschutzbeauftragten oder sonstige Interessenträger – nachvollziehbar sein, um was es bei der Verarbeitung geht und zu welchem Zweck sie erfolgt. Natürlich können Sie auf andere Unterlagen Ihrer EU-Institution verweisen; Sie sollten aber darauf achten, dass die Beschreibung auch aus sich heraus verständlich ist, da sie ein Kapitel des DSFA-Berichts darstellt, welcher ein eigenständiges Dokument ist.

Der beschreibende Teil einer Datenschutz-Folgenabschätzung beginnt mit den Informationen im Verzeichnis, ist jedoch ausführlicher und enthält auch ein detailliertes Datenflussdiagramm.

Als Ausgangsmaterial für die systematische Beschreibung dieses Verarbeitungsvorgangs nehmen Sie die bereits in Ihrem Verzeichnis enthaltenen Informationen, die um Folgendes zu ergänzen sind:

-)] Datenflussdiagramm für den Verarbeitungsvorgang (Flussdiagramm): Welche Daten erfassen wir wo / von wem, was tun wir damit, wo speichern wir sie, an wen geben wir sie weiter?
-)] Detaillierte Beschreibung aller Zwecke des Verarbeitungsvorgangs: Darstellung der einzelnen Schritte des Vorgangs, erforderlichenfalls mit Unterscheidung der verschiedenen Zwecke.
-)] Beschreibung des Zusammenspiels mit anderen Verarbeitungsvorgängen: Werden für diesen Verarbeitungsvorgang personenbezogene Daten aus anderen Systemen verarbeitet? Werden personenbezogene Daten aus diesem Verarbeitungsvorgang in anderen Verarbeitungsvorgängen wiederverwendet?
-)] Beschreibung der dazugehörigen Infrastruktur: Dateisysteme, IT usw.

Für diese Dokumentation können Sie auch bestehende Dokumentationen für den Verarbeitungsvorgang oder dessen Entwicklung verwenden. Wenn Sie so vorgehen, sollten Sie die vorhandene Dokumentation nochmals unter dem Gesichtspunkt „Wie wird das die Menschen, deren Daten wir verarbeiten, betreffen?“ durchlesen und, soweit erforderlich, überarbeiten.

Viele der Informationen, die man für die DSFA braucht, wird es in Ihrer EU-Institution bereits geben, nämlich als Teil der anderen Zwecken als dem Datenschutz dienenden Projekt- oder

Prozessdokumentationen. Soweit praktisch möglich, können Sie derartige Dokumentationen wiederverwenden. Dabei ist allerdings zu beachten, dass diese anderen Dokumentationen meist aus dem Blickwinkel Ihrer EU-Institution verfasst wurden – „Was bedeutet dieser Verarbeitungsvorgang für unsere EU-Institution?“ Was muss unsere EU-Institution tun? Inwiefern berührt dies unsere EU-Institution? Bei der Datenschutz-Folgenabschätzung geht es darum, wie der Verarbeitungsvorgang die Menschen betrifft, deren Daten Ihre EU-Institution verarbeitet. Wenn Sie für die Datenschutz-Folgenabschätzung vorhandene Dokumentationen wiederverwenden, sollte Sie diese andere Perspektive bedenken und erforderlichenfalls Anpassungen oder Ergänzungen vornehmen.

3.3 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Gemäß Artikel 39 Absatz 6 Buchstabe b der Verordnung müssen Sie auch eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge vornehmen. In diesem Abschnitt müssen Sie erklären, welchem Zweck die geplante Verarbeitung dienen soll. Dabei ist darauf zu achten, dass erklärt wird, dass die Verarbeitung wirklich erforderlich ist, um die in der Rechtsgrundlage genannten Ziele zu erreichen; dass die Verarbeitung dieses Erfordernis wirksam erfüllt; und dass die Verarbeitung die am wenigsten in Grundrechte eingreifende Vorgehensweise ist, um das gesetzte Ziel zu erreichen (Notwendigkeit). Außerdem müssen Sie sicherstellen, dass sich die aus der Verarbeitung ergebenden Grundrechtseingriffe nicht die Vorteile aus der Verarbeitung überwiegen (Verhältnismäßigkeit).

Dazu müssen Sie erklären:

- a) warum die vorgeschlagenen Verarbeitungsvorgänge für Ihre Organisation notwendig sind, um die ihr übertragene Aufgabe wahrzunehmen. Erklären Sie, auf welche Weise und warum die vorgeschlagenen Verarbeitungsvorgänge für Ihre Organisation ein wirksames Mittel zur Wahrnehmung ihrer Aufgabe sind und ob andere Möglichkeiten zur Wahrnehmung dieser Aufgabe von Ihnen in Erwägung gezogen wurden, wobei auch zu begründen ist, weshalb die gewählte Vorgehensweise die am wenigsten in Grundrechte eingreifende ist;
- b) inwiefern die Verarbeitung im Hinblick auf die Wahrnehmung der Aufgabe verhältnismäßig ist; Stellen Sie den Nutzen der Verarbeitung den sich durch die Verarbeitung ergebenden Risiken für die Grundrechte gegenüber. Es kann vorkommen, dass eine Verarbeitung die Voraussetzung der Notwendigkeit erfüllt, aber dennoch als unverhältnismäßig anzusehen ist.

3.4 Risikobewertung

Nach Feststellung des Kontexts müssen Sie als nächstes die Risiken⁵, die sich durch die geplante Verarbeitung ergeben, im Detail prüfen. Dabei sind zwei Seiten zu berücksichtigen: zum einen die Risiken für die Rechte und Freiheiten der betroffenen Personen, zum anderen die Risiken für Ihre Organisation. Diese sind nicht unbedingt dieselben.

Bei einer Datenschutz-Folgenabschätzung geht es in erster Linie um die Abschätzung der Risiken für die Rechte und Freiheiten der betroffenen Personen. Gleichzeitig sind auch die

⁵ Die Fragen, die in Teil 1 der Verzeichnisvorlage für Fragen zur Risikoprüfung aufgeführt sind, beziehen sich auf die erste Abschätzung, bei der es darum geht, ob möglicherweise eine Datenschutz-Folgenabschätzung erforderlich ist. Bei der hier vorgenommenen Risikobewertung geht es darum, die Risiken von Verarbeitungsvorgängen, für die Sie die Erforderlichkeit einer Datenschutz-Folgenabschätzung bereits festgestellt haben, im Einzelnen zu analysieren, um die nötigen Maßnahmen zur Risikokontrolle zu gestalten.

Compliance-Risiken für Ihre Organisation zu analysieren. Diese stehen in einem Zusammenhang, sind aber nicht unbedingt identisch.

Ein „Risiko“ in diesem Sinne ist ein mögliches Ereignis, das Schäden oder Verluste verursachen oder die Fähigkeit, die Ziele zu erreichen, beeinträchtigen könnte. Risiken haben *Auswirkungen* („Wie gravierend könnte dies sein?“) sowie eine *Wahrscheinlichkeit* („Wie wahrscheinlich ist es, dass dies passiert?“). Potenzielle Datenschutzrisiken sind etwa die unbefugte Offenlegung personenbezogener Daten oder dass unzutreffende Daten zu nicht gerechtfertigten Entscheidungen über einzelne Personen führen. Diese Vorgehensweise kennt man aus dem Informationssicherheits-Risikomanagement (ISRM) und der Geschäftskontinuitätsplanung, nur dass die hier bewerteten Risiken andere sind: Bei der Geschäftskontinuitätsplanung ginge es zum Beispiel eher um Risiken wie Stromausfälle, Überschwemmungen und Streiks im öffentlichen Nahverkehr.

Der Begriff der „Rechte und Freiheiten“ der betroffenen Personen bezieht sich in erster Linie auf die Rechte auf Privatsphäre und Datenschutz (Artikel 7 und 8 der Charta), umfasst aber auch damit zusammenhängende Rechte, in die unter Umständen ebenfalls eingegriffen wird (z. B. die abschreckende Wirkung von Überwachungsmaßnahmen im Hinblick auf die Rede- oder Versammlungsfreiheit). Hier geht es um die Folgenabschätzung gemäß Artikel 39 Absatz 6 Buchstabe c der Verordnung.

Die Risiken für Ihre Organisation sind letztendlich Compliance-Risiken – die Nichterfüllung der Pflichten, denen Ihre EU-Institution z. B. in Bezug auf die Unterrichtung derjenigen, deren Daten Sie verarbeiten, oder das Erfordernis, die Daten sicher zu speichern, unterliegt. Hält Ihre EU-Institution diese Pflichten nicht ein, drohen ihr aufsichtsrechtliche Maßnahmen und negative Berichterstattung in den Medien.

In einigen Fällen kann es auch andere Risiken geben: Die rechtswidrige Offenlegung von Patientendaten könnte dem Ruf Ihrer EU-Institution schaden, sie jedoch nicht in ihrer Existenz gefährden. Für Personen, deren Patientendaten bekannt werden, sind allerdings gravierendere Folgen möglich.

Diese beiden Arten von Risiken stehen natürlich in einem Zusammenhang. Die Ihrer EU-Institution auferlegten spezifischen rechtlichen Verpflichtungen sind letzten Endes vom Unionsgesetzgeber gewählte Sicherheitskontrollen: Da immer die Gefahr besteht, dass Risiken in unvorhergesehenen Zusammenhängen wiederverwendet werden, gibt es den Grundsatz der Zweckbindung; weil eine Datenverarbeitung, die vorgenommen wird, ohne die betroffenen Personen darüber zu informieren, stets einen Eingriff in die Privatsphäre darstellt, sind die Verantwortlichen verpflichtet, die betroffenen Personen, deren Daten sie verarbeiten, darüber zu unterrichten. Überdies sind Risiken für die betroffenen Personen letztendlich auch Risiken für Ihre Organisation: Wenn z. B. ein neues Tool nicht benutzt wird, weil es im Hinblick auf die Privatsphäre für bedenklich gehalten wird, kann das dazu führen, dass Ihre Organisation die mit dem Tool verfolgten Ziele nicht erreicht; ein weiteres offensichtliches Beispiel sind Datenschutzverletzungen und die sich daraus ergebenden Rufschäden.

Offenkundig gibt es hier auch einen das ISRM betreffenden Aspekt (nicht zuletzt, weil die sichere Datenspeicherung zu den Datenschutzgrundsätzen zählt), aber das ISRM ist bei Weitem nicht alles, worum es hier geht. Beim ISRM liegt der Fokus eher auf Risiken, die sich ergeben, wenn sich ein System nicht ordnungsgemäß verhält (z. B. unbefugte Offenlegung personenbezogener Daten). Dagegen geht es bei den Risiken für die betroffenen Personen und

den Compliance-Risiken zum Teil um Risiken, die sich ergeben, wenn sich das System, für das Sie die Datenschutz-Folgenabschätzung erstellt haben, ordnungsgemäß verhält.

Auch völlig planmäßig verlaufende Verarbeitungsvorgänge können Auswirkungen auf betroffene Personen haben (z. B. bei der Personalüberwachung). Eine genaue Risikoabschätzung ist auch für diese Risiken erforderlich, nicht nur für Risiken, die sich ergeben, „wenn’s schiefgeht“. Nehmen Sie dabei die Datenschutzgrundsätze zum Maßstab.

Ein Beispiel: Mit intelligenten Messgeräten ist es möglich, den Stromverbrauch in Echtzeit zu messen, woraus sich auf das Verhalten von Privatpersonen schließen lässt (Wer ist zuhause? Was tun diese Personen?). Dies ist sowohl etwas, was von den betroffenen Personen als Eingriff empfunden wird, als auch eine erwartete Folge dieser Technologie. Nehmen wir als hypothetisches Beispiel eine EU-Institution, die ein in Grundrechte eingreifendes Fallverwaltungssystem hätte, das alle Handlungen erfasst und in Echtzeit den Vorgesetzten meldet, die dies zur Evaluierung und zur Erstellung von Mitarbeiterprofilen nutzen (Wie lange hat der Mitarbeiter an jedem einzelnen Dokument gearbeitet? Wie schnell war die Erledigung im Vergleich zu den Kollegen? Wie viele Fälle wurden im Vergleich zu anderen Kollegen abgearbeitet? Wem könnten / sollten andere Aufgaben zugewiesen werden?). Was die Mitarbeiter bei diesem hypothetischen System als Eingriff empfinden, ist genau das, was mit dem System bezweckt wird.

In all diesen Beispielen würde ein klassischer ISRM-Ansatz diese Aspekte wahrscheinlich nicht berücksichtigen. Natürlich gibt es einen engen Zusammenhang mit dem ISRM – kein guter Datenschutz ohne gute Informationssicherheit. Die Risiken, um die es hier geht, sind jedoch nicht diejenigen, um die es bei den klassischen ISRM-Zielen der Vertraulichkeit, Integrität und Verfügbarkeit geht.

Die Datenschutzgrundsätze sind in Artikel 4 der Verordnung aufgeführt⁶. In anderen Artikeln werden sie eingehender erklärt:

⁶ Nähere Erläuterungen dazu, siehe Anhang 2 von Teil I.

DS-Grundsatz	Artikel	Erwägungsgründe
Verarbeitung nach Treu und Glauben	Artikel 4 Absatz 1 Buchstabe a, 17 bis 25	20, 26, 34, 35, 37-41
Transparenz	Artikel 4 Absatz 1 Buchstabe a, 14 bis 16, 25	20, 35, 36
Zweckbindung	Artikel 4 Absatz 1 Buchstabe b, 6, 13	25
Datenminimierung	Artikel 4 Absatz 1 Buchstabe c, 12, 13, 36	20
Richtigkeit	Artikel 4 Absatz 1 Buchstabe d, 18	38
Speicherbegrenzung	Artikel 4 Absatz 1 Buchstabe e, 13	20, 33
Sicherheit	Artikel 4 Absatz 1 Buchstabe f, 33	53

Abbildung 4: Datenschutzgrundsätze in der Verordnung

Gehen Sie Ihr Datenflussdiagramm durch und fragen Sie sich bei jedem Schritt, welche Auswirkungen dieser im Hinblick auf die Datenschutzgrundsätze auf die betroffenen Personen haben könnte.

Nehmen Sie die nachstehenden Leitfragen als Ausgangspunkt und fragen Sie sich, was das Erreichen dieser Ziele beeinträchtigen könnte und welche Auswirkungen dies für die betroffenen Personen haben könnte. Beurteilen Sie dabei die Schwere und die Wahrscheinlichkeit. Es gibt keine besonderen Vorgaben dazu, welche Skala für die Beurteilung zugrunde zu legen ist. Vielleicht möchten Sie die Skalen verwenden, mit denen ihre internen Interessenträger vertraut sind, weil Sie sich z. B. in Ihrem ISRM-Prozess oder anderen Bereichen des Risikomanagements verwenden. Die meisten EU-Institutionen verwenden eine 5-stufige Skala, von „sehr gering“ bis „sehr hoch“. Um die Einheitlichkeit der Risikobeurteilung zu gewährleisten, ist für jede Stufe festzulegen, was sie bedeutet, z. B. im Hinblick auf Rufschäden oder finanzielle Auswirkungen bzw., was die Wahrscheinlichkeit angeht, im Hinblick auf die Häufigkeit. So wird zum Beispiel die Offenlegung von Patientendaten gegenüber Personen, die nicht auf deren Kenntnis angewiesen sind, wahrscheinlich eine stärkere Beeinträchtigung bedeuten, als die Offenlegung der Kontaktangaben von Mitarbeitern der EU-Institution; die Offenlegung gegenüber unbefugten Mitarbeitern innerhalb Ihrer EU-Institution wird eine geringere Beeinträchtigung darstellen als die versehentliche Veröffentlichung.

Und so geht's: Gehen Sie Ihr Datenflussdiagramm durch und fragen Sie sich bei jedem Schritt, welche Auswirkungen dieser auf die Schutzziele haben könnte. Einige Schutzziele werden für bestimmte Arten von Verfahrensschritten von höherer Relevanz sein als für andere. In der nachstehenden Tabelle ist dargestellt, welche Schutzziele für einige allgemeine Verarbeitungsschritte relevant sind, wobei jeweils die Schutzziele mit der höchsten Relevanz angegeben sind. Dies sind die Aspekte, die die Prüfung mindestens umfassen muss.

	Verarbeitung nach Treu	Transparenz	Zweck- bindung	Daten- minimierung	Richtig- keit	Speicher- begrenzung	Sicherheit
Datenerhebung	X	X	X	X	X		X
Datenzusammenführung	X	X	X	X	X		X
Organisation / Gliederung			X	X	X		
Auslesen / Abfragen /	X	X	X		X	X	X
Bearbeitung / Veränderung		X		X	X		X
Offenlegung /	X	X	X	X	X		X
Beschränkung			X	X	X	X	X
Speicherung	X	X	X			X	X
Löschen / Vernichtung			X			X	X

Abbildung 5: Relevanz der Schutzziele für die Schritte im Datenflussdiagramm

Für die Risikobewertung gehen Sie Ihr Datenflussdiagramm durch und stellen Sie sich bei jedem Schritt die Frage, welche Auswirkungen dieser Schritt unter dem Gesichtspunkt der Schutzziele / Datenschutzgrundsätze haben könnte. Beginnen Sie mit den nachstehenden Leitfragen.

3.5 Leitfragen zu den Datenschutzgrundsätzen

Die nachstehenden Leitfragen dienen als Ausgangspunkt sowohl für die Prüfung der einzelnen Schritte als auch für die Gesamtbewertung. Nicht alle Fragen werden für alle Schritte relevant sein, manchmal sind vielleicht auch detailliertere Angaben nötig.

„**Verarbeitung nach Treu und Glauben**“ umfasst mehrere Aspekte: Käme diese Verarbeitung für die betroffenen Personen **unerwartet**? Hat sie **abschreckende Wirkung** in Bezug auf die Ausübung der sonstigen Rechte der betroffenen Personen; ist es wahrscheinlich, dass die Verarbeitung sie von der Rechtsausübung abhält? Wie können die betroffenen Personen **sich wehren** und Gehör verschaffen?

Ist die Verarbeitung für die betroffenen Personen **unerwartet**, weil z. B. Daten für einen anderen als den Zweck, für den sie ursprünglich erhoben wurden, wiederverwendet werden, oder zwei zuvor getrennte Datenbanken aufgrund neuer Gesetze zusammengeführt oder miteinander verbunden wurden? Wäre diese Verarbeitung selbst für betroffene Personen, die sich den Datenschutzhinweis nicht durchgelesen haben, zu erwarten?

In den Fällen, in denen Sie die Verarbeitung auf die Einwilligung stützen, ist darauf zu achten, dass diese rechtsgültig, freiwillig und in informierter Weise erteilt wurde, weil es ansonsten sein kann, dass Ihre Verarbeitung rechtswidrig ist oder gegen Treu und Glauben verstößt (z. B. wenn die Einwilligung für eine andere als die von Ihnen durchgeführte Verarbeitung erteilt wurde).

Drittens müssen Sie sich fragen, ob die von Ihnen geplanten Verarbeitungsvorgänge möglicherweise **abschreckende Wirkung** haben und die betroffenen Personen von der Ausübung ihrer sonstigen Rechte abhalten könnten. „Abschreckende Wirkung“ bedeutet, dass es weniger wahrscheinlich ist, dass die betroffenen Personen ihre Grundrechte ausüben. Ein Beispiel wäre etwa die Videoüberwachung eines allgemein zugänglichen Bereichs außerhalb des Eingangs Ihrer EU-Institution und deren mögliche Auswirkungen auf die Versammlungs- und Redefreiheit an diesem Ort.

Der dritte Aspekt der Verarbeitung nach Treu und Glauben ist die Gewährleistung der den betroffenen Personen zustehenden Rechte, sich gegen die Verarbeitung zu wehren; der kollektive Begriff umfasst die den betroffenen Personen aufgrund der Verordnung zustehenden Rechte auf Auskunft, Berichtigung, Löschen, Einschränkung der Verarbeitung, Beschwerde und Datenübertragbarkeit. Es muss den betroffenen Personen möglich sein, von Ihnen eine Kopie der personenbezogenen Daten zu bekommen, die Gegenstand der Verarbeitung sind; deren Berichtigung zu verlangen, wenn die Daten unrichtig sind, sie löschen zu lassen, falls die Daten rechtswidrig in Ihrem Besitz sind; unter bestimmten Voraussetzungen eine Einschränkung der Verarbeitung zu erwirken (indem die Daten z. B. nur noch für bestimmte Mitarbeiter sichtbar sind); der Verarbeitung aus Gründen, die sich aus ihrer besonderen Situation ergeben, zu widersprechen; sowie in bestimmten Fällen die Datenübertragbarkeit zu erwirken.

Wenn es jemandem nicht möglich ist, unrichtige Informationen zeitnah zu berichtigen, könnte dies negative Folgen für ihn haben. Sie müssen sicherstellen, dass die betroffenen Personen diese sich aus der Verordnung ergebenden Rechte ausüben können, ohne dass dies den Betrieb Ihrer EU-Institution beeinträchtigt.

Das bedeutet zum Beispiel, dass Systeme so zu gestalten sind, dass Sie bestimmte Einträge in der Datenbank einschränken / sperren können, ohne dass dies den Betrieb der Datenbank beeinträchtigt, oder dass es den Betroffenen möglich ist, leicht auf ihre im System gehaltenen personenbezogenen Daten zuzugreifen und diese zu exportieren. Sie sollten es den Betroffenen möglichst einfach machen, ihre Rechte auszuüben. Die Angaben zu den Kontaktstellen sollten leicht zu finden sein und die zu erfüllenden Voraussetzungen sollten gleich zu Beginn klargestellt werden (z. B. wie man nachweisen kann, dass man selbst tatsächlich die betroffene Person ist, die Auskunft über ihre Daten verlangt). Nähere Informationen zu all diesen Rechten sind in den Leitlinien zu den Rechten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten⁷ zu finden.

Leitfragen zur Verarbeitung nach Treu und Glauben

1. Wäre diese Verarbeitung selbst für diejenigen, die sich den Datenschutzhinweis nicht durchgelesen haben, zu erwarten?
2. Wenn die Verarbeitung auf Einwilligung beruht: Wurde diese freiwillig erteilt? Wie dokumentieren Sie, dass die Einwilligung erteilt wurde? Wie kann derjenige seine Einwilligung widerrufen?
3. Könnte dies abschreckende Wirkung haben?
4. Könnte dies zu Diskriminierung führen?
5. Ist es für die Betroffenen einfach, ihre Rechte auf Auskunft, Berichtigung, Löschen usw. auszuüben?

⁷ https://edps.europa.eu/data-protection/our-work/publications/guidelines/rights-individuals_en.

„**Transparenz**“ ist zusammen mit der Verarbeitung nach Treu und Glauben in Artikel 4 Absatz 1 Buchstabe a genannt. Dabei geht es darum, dass diejenigen, deren Daten Sie verarbeiten, wissen, dass Sie die Daten verarbeiten, und verstehen können, was Sie mit deren Daten machen und wozu dies geschieht (Artikel 14 bis 16 der Verordnung). Besonders wichtig ist dies, wenn Sie die Daten nicht direkt bei den betroffenen Personen erheben, sondern aus anderen Quellen beziehen. Wenn es eine Rechtsgrundlage dafür gibt, Betroffene nicht (oder – z. B. in den früheren Phasen einer OLAF-Untersuchung – noch nicht) zu unterrichten, müssen Sie darüber nachdenken, wann und auf welche Weise Sie sie darüber unterrichten werden.

Wer nicht weiß, dass Sie seine personenbezogenen Daten verarbeiten, kann die sonstigen Rechte, die ihm aufgrund der Verordnung zustehen, nicht ausüben; wenn Sie die Verarbeitung auf eine Einwilligung stützen, die Betroffenen aber nicht ordnungsgemäß unterrichten, bedeutet dies zudem, dass die Einwilligung ungültig ist. Nähere Informationen finden Sie in den Leitlinien des EDSB zu Artikel 14 bis 16 der Verordnung⁸.

Leitfragen zur Transparenz

1. Wie stellen Sie sicher, dass Sie mit Ihren Informationen tatsächlich die betroffenen Personen erreichen?
2. Sind die Informationen vollständig und leicht verständlich?
3. Sind sie auf die Zielgruppe zugeschnitten? Für Kinder sind z. B. unter Umständen speziell zugeschnittene Informationen erforderlich.
4. Falls Sie die Betroffenen erst später unterrichten wollen: Weshalb ist dies begründet?

Abbildung 7: Leitfragen zur Transparenz

„**Zweckbindung**“ in Artikel 4 Absatz 1 Buchstabe b ist der Grundsatz, dass personenbezogene Daten, die für einen bestimmten Zweck erhoben werden, nicht für andere, damit nicht vereinbare Zwecke wiederverwendet werden dürfen. Die EU-Institutionen können diesen Grundsatz sowohl durch entsprechende Regeln als auch durch die Gestaltung der eigentlichen Systeme und Prozesse gewährleisten. Ein wichtiges Gestaltungsmerkmal, das hier oft nützlich sein kann, ist die „Unverknüpfbarkeit“. Dies bedeutet, dass sich personenbezogene Daten nicht (jedenfalls nicht ohne Weiteres) mit anderen Informationen über dieselbe Person verknüpfen lassen. Dies hilft, die Zweckbindung durchzusetzen, indem es zum Beispiel verhindert, dass über jemanden umfassende Profile zu Zwecken erstellt werden, mit denen derjenige niemals gerechnet hätte.

Archivierung, wissenschaftliche Forschung, historische oder statistische Zwecke mögen als miteinander vereinbar anzusehen sein, erfordern jedoch gewisse Schutzmaßnahmen. Wenn Sie personenbezogene Daten zu solchen Zwecken speichern bzw. zur Verfügung stellen wollen, ist zu bedenken, welche Auswirkungen dies auf die Betroffenen haben könnte und wie sich dieses Risiko minimieren ließe. Dies wäre zum Beispiel durch Datenaggregation (Zusammenfassung von Geburtsdaten in Altersgruppen) oder durch verzögerte Offenlegung (Archivöffnung) möglich.

Die Zweckbindung verhindert die schleichende Ausweitung auf andere Zwecke. Ein Beispiel dafür wäre die hypothetische Situation, dass Bedienstete in einer vertraulichen Karriereberatung sagen, dass sie gerne die Arbeit wechseln würden, und diese Information dann

⁸ https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf.

dazu wiederverwendet wird, ihnen Weiterbildung abzulehnen, weil sie möglicherweise bald aus der Organisation ausscheiden werden. Dies wäre ein klarer Verstoß gegen den Grundsatz der Zweckbindung.

Leitfragen zur Zweckbindung

1. Haben Sie alle Zwecke Ihres Verarbeitungsvorgangs festgestellt?
2. Sind alle Zwecke mit dem ursprünglichen Zweck vereinbar?
3. Besteht das Risiko, dass die Daten zu anderen Zwecken wiederverwendet werden könnten (schleichende Ausweitung auf andere Zwecke)?
4. Wie können Sie sicherstellen, dass Daten ausschließlich zu den für sie festgelegten Zwecken verwendet werden?
5. Falls Sie Daten für wissenschaftliche Forschung, zu statistischen oder historischen Zwecken bereitstellen bzw. wiederverwenden wollen: Welche Maßnahmen haben Sie ergriffen, um die betroffenen Personen zu schützen?

Abbildung 8: Leitfragen zur Zweckbindung

„**Datenminimierung**“ bedeutet, dass Ihre EU-Institution nur solche personenbezogenen Daten verarbeitet, auf die sie tatsächlich angewiesen ist, um den Zweck der Verarbeitung zu erfüllen, und diese auch nur solange, wie für diesen Zweck erforderlich speichert. Dies trägt auch entscheidend dazu bei, dass personenbezogenen Daten nicht in übermäßigem Umfang rechtswidrig verarbeitet werden.

Dies erfordert zum Beispiel, sicherzustellen, dass Sie auf den Formularen nur die erforderlichen Informationen abfragen und dass Sie niemals personenbezogene Daten „für alle Fälle“ speichern, falls Sie sie später nochmal gebrauchen könnten. Spezifische Risiken sind hier z. B. Standardeinstellungen in handelsüblicher Standardsoftware, die dazu führen, dass personenbezogene Daten verarbeitet werden, die für Ihre Zwecke gar nicht nötig sind. Es erfordert auch, dass Sie darüber nachdenken, ob die Daten, die Sie erheben wollen, Ihnen tatsächlich die Informationen liefern, die Sie erlangen möchten: Können Sie mit den Daten messen, was Sie zu messen beabsichtigen?

Falls Sie planen, personenbezogene Daten für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, die nichts mit dem Geschäftszweck zu tun haben, zur Verfügung zu stellen, ist darüber nachzudenken, welche Auswirkungen dies auf die betroffenen Personen haben könnte und wie sich diese Auswirkungen minimieren ließen. Wenn Sie diese Zwecke auf andere Weise erreichen können, ohne dass personenbezogene Daten betroffen wären (z. B. indem man die statistischen Daten speichert, jedoch nicht die Mikrodaten), dann wählen Sie eine solche Vorgehensweise. Sollte es erforderlich sein, (einige) personenbezogene Daten für diese Zwecke zu speichern, sollten sie überlegen, wie Sie dies minimieren können (z. B. Altersgruppen statt Geburtsdaten oder sonstige Datenaggregation).

Leitfragen zur Datenminimierung

1. Können Sie mit den Daten, die Sie erheben, messen, was Sie zu messen beabsichtigen?
2. Gibt es Teile der Daten, die Sie entfernen (oder ausblenden / verbergen) könnten, ohne dass der Zweck der Verarbeitung beeinträchtigt würde?
3. Wird auf den Formularen klar zwischen Pflicht- und optionalen Angaben unterschieden?
4. Falls Sie Informationen zu statistischen Zwecken speichern möchten: Wie managen Sie das Risiko der Re-Identifizierung?

„**Richtigkeit**“ bedeutet, dass Ihre EU-Institution verpflichtet ist, sicherzustellen, dass die Informationen, die sie verarbeitet, richtig sind (Artikel 4 Absatz 1 Buchstabe d der Verordnung) – auf falscher Informationsgrundlage beruhende Entscheidungen können negative Auswirkungen auf Menschen haben, für die Ihre EU-Institution unter Umständen haftet. Wenn Ihre EU-Institution feststellt, dass Informationen unrichtig oder unvollständig sind, muss sie diese unverzüglich berichtigen⁹ oder löschen. Hier hilft es, wenn man den betroffenen Personen leichten Zugang gewährt. Es gibt Verarbeitungsvorgänge, bei denen über die Wahrheitsgemäßheit von Behauptungen unter den betroffenen Parteien gestritten wird (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.¹⁰

Leitfragen zur Richtigkeit

1. Ist die Datenqualität dem Zweck angemessen?
2. Welche Folgen könnte es für die betroffenen Personen haben, wenn bei diesem Verarbeitungsvorgang auf Grundlage unrichtiger Informationen gehandelt würde?
3. Wie stellen Sie die Richtigkeit der Daten, die Sie selbst erheben, sicher?
4. Wie stellen Sie sicher, dass Daten, die Sie von Dritten erlangen, richtig sind?
5. Ist es mit Ihren Tools möglich, Daten erforderlichenfalls zu aktualisieren / zu berichtigen?
6. Sind mit Ihren Tools Stimmigkeitsprüfungen möglich?¹¹

Abbildung 10: Leitfragen zur Richtigkeit

„**Speicherbegrenzung**“ in Artikel 4 Absatz 1 Buchstabe e der Verordnung bedeutet, dass personenbezogene Daten „so lange wie nötig, so kurz wie möglich“ gespeichert werden. In manchen Fällen ist diese Aufbewahrungsfrist in den Unionsvorschriften niedergelegt; ansonsten muss Ihre EU-Institution diese Fristen festlegen. Ihre Aufbewahrungsfristen sind im Hinblick auf die geschäftlichen Erfordernisse bezüglich des spezifischen Verarbeitungsvorgangs festzulegen – dies ist keine technische Frage, sondern eine, die nach den behördlichen Erfordernissen zu entscheiden ist. In erster Linie geht es hier um die verwaltungstechnische Speicherungsfrist; im Falle der Archivierung sollten Sie aber auch darüber nachdenken, was nach der Speicherung passiert.

Falls Sie personenbezogene Daten (vollständig oder in Teilen) für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, die nichts mit dem behördlichen Zweck zu tun haben, speichern möchten, ist darüber nachzudenken, welche Auswirkungen dies auf die betroffenen Personen haben könnte (siehe dazu auch oben

⁹ Änderungen, die zur Berichtigung personenbezogener Daten vorgenommen werden, sollten im Interesse der Datenintegrität nachverfolgbar sein.

¹⁰ 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 Verordnung.

¹¹ Z. B. eine automatische Prüfung, ob die angegebenen Geburtsdaten das richtige Format haben und in einer plausiblen Spanne liegen.

„Zweckbindung“). Dabei ist zu beachten, dass die 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. Aggregation 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.

Nähere Informationen über Aufbewahrungsfristen finden Sie in vielen der vom EDSB herausgegebenen Leitlinien zu spezifischen Verarbeitungsvorgängen¹².

Leitfragen zur Speicherbegrenzung

1. Sehen die Unionsvorschriften Speicherfristen für Ihren Verarbeitungsvorgang vor?
2. Wie lange müssen Sie die Daten speichern? Zu welchem/n Zwecke(n)?
3. Können Sie die Speicherfristen für verschiedene Teile der Daten unterscheiden?
4. Falls Sie die Daten noch nicht löschen können, können Sie dann den Zugang dazu beschränken?
5. Ist mit Ihren Tools eine automatisierte dauerhafte Löschung bei Ablauf der Speicherfrist möglich?

Abbildung 11: Leitfragen zur Speicherbegrenzung

„**Sicherheit**“ in Artikel 4 Absatz 1 Buchstabe f bezieht sich auf die bereits aus dem ISRM vertrauten Begriffe „Vertraulichkeit“ und „Integrität“. „Vertraulichkeit“ bedeutet, dass Informationen nur den befugten Personen, die auf deren Kenntnis angewiesen sind, zur Verfügung gestellt werden. „Integrität“ bedeutet, dass Informationen nicht ohne ordnungsgemäße Autorisierung abgeändert werden können.¹³ Die dritte der drei ISRM-Begriffe, die Verfügbarkeit, ist nicht in Artikel 4 Absatz 1 Buchstabe f aufgeführt; Artikel 33 Absatz 1 Buchstabe c betont jedoch das Erfordernis der Wiederherstellung der Verfügbarkeit der Daten, sodass auch diese wesentliche Dimension der Informationssicherheit berücksichtigt ist.

Wird die Vertraulichkeit personenbezogener Daten verletzt, kann dies den betroffenen Personen Schäden verschiedener Art verursachen: psychische Belastung (z. B. beim Bekanntwerden von Daten aus der Patientenakte) und auch finanziellen Schaden (z. B. wenn bekanntgewordene personenbezogene Daten zum Identitätsdiebstahl verwendet werden). Um das zu vermeiden, sollten Sie Ihre Systeme so gestalten, dass der Zugang zu personenbezogenen Daten strikt auf diejenigen beschränkt ist, die auf deren Kenntnis angewiesen sind, und dass personenbezogene Daten in allen Phasen – sowohl im Speicher als auch bei der Übermittlung – (ggf. durch Verschlüsselung) davor geschützt sind, von Unbefugten gelesen zu werden. Protokolle über den Zugang zu personenbezogenen Daten sind eine Möglichkeit, sicherzustellen, dass Sie etwaige Datenschutzverletzungen erkennen und ggf. Nachweise darüber haben, wer auf die Daten zugegriffen hat.

Wird die Integrität personenbezogener Daten verletzt, kann das für die Betroffenen die Folge haben, dass sie betreffende Entscheidungen auf Grundlage verfälschter Informationen getroffen

¹² https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en.

¹³ Wenn Informationen abgeändert werden können, müssen solche Änderungen nachvollziehbar sein.

werden. Um dies zu vermeiden, müssen Sie zum Beispiel Ihre Systeme so gestalten, dass personenbezogene Daten nur von befugten Nutzern geändert werden können und dass derartige Änderungen nachverfolgbar sind.

Wird die Verfügbarkeit verletzt, können die Daten unter Umständen überhaupt nicht genutzt werden. Für die Betroffenen kann das Nachteile haben (z. B. wenn wegen Unzugänglichkeit der Daten oder Systemausfalls keine Gehaltszahlungen erfolgen können) und auch die Ausübung der ihnen zustehenden Rechte (auf Auskunft, Berichtigung usw.) erschweren oder unmöglich machen.

Eingehendere Informationen dazu enthalten die vom EDSB herausgegebenen Leitlinien für Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten¹⁴. Ihre Organisation sollte auch einen Ansatz für das allgemeine Management der Informationssicherheit haben, der auch für den Datenschutz nützlich sein wird.

Leitfragen zur Sicherheit

1. Haben Sie ein Verfahren für die Erkennung, Analyse und Bewertung von Informationssicherheitsrisiken mit potenziellen negativen Auswirkungen auf personenbezogene Daten und die deren Verarbeitung unterstützenden IT-Systeme?
2. Bedenken Sie auch die Auswirkungen auf die Grundrechte, Freiheiten und Interessen der betroffenen Personen und nicht nur die Risiken für Ihre Organisation?
3. Berücksichtigen Sie bei der Beurteilung der Risiken Art, Umfang, Umstände und Zweck der Verarbeitung?
4. Managen Sie die Risiken in Bezug auf die Schwachstellen Ihres Systems und die Gefährdung Ihrer Daten und Systeme?
5. Haben Sie für die Durchführung der Risikobewertung Ressourcen und Mitarbeiter mit zugewiesenen Rollen?
6. Nehmen Sie im Hinblick auf den Kontext der Verarbeitung und der Risiken systematische Überprüfungen und Aktualisierungen der Sicherheitsvorkehrungen vor?

Abbildung 12: Leitfragen zur Sicherheit

Nachdem Sie das Datenflussdiagramm durchgegangen sind, müssen Sie sich im Hinblick auf die festgestellten Risiken fragen, ob die Verarbeitung möglicherweise horizontale Risiken aufweist, die sich nicht ohne Weiteres einem bestimmten Verarbeitungsschritt zuordnen lassen. Achten Sie darauf, auch diese Arten von Risiken zu erfassen – manchmal ist das Ganze mehr als die Summe seiner Teile.

Diese Fragen sind nur der Ausgangspunkt; sie dürften Ihnen jedoch helfen, die problematischen Aspekte geplanter Verarbeitungsvorgänge genau in den Blick zu bekommen.

Wenn Sie diese Phase abgeschlossen haben, dokumentieren Sie Ihre Ergebnisse in der DSFA-Dokumentation. Je höher das Risiko, desto mehr müssen Sie im nächsten Schritt darüber nachdenken, welche Maßnahmen Sie dagegen vorsehen.

¹⁴ https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en (Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten) und https://edps.europa.eu/data-protection/our-work/publications/guidelines/it-governance-and-it-management_en (Leitlinien zum Schutz personenbezogener Daten für die Bereiche IT-Governance und IT-Management der EU-Institutionen)

3.6 Risikobehandlung

Wenn Sie die Risiken festgestellt haben, müssen Sie geeignete Maßnahmen zur Risikominderung (Risikokontrolle) auswählen. In diesem Abschnitt wird beschrieben, welche Ansätze für die Risikominimierung in Betracht kommen; außerdem werden einige allgemeine Risikokontrollen vorgestellt.

Bitte beachten Sie, dass die Umstellung auf einen „risikobasierten Ansatz“ in der DSGVO und in der Verordnung ein wichtiges Merkmal der neuen Vorschriften ist. Zur Sicherstellung der Vorschriftseinhaltung gibt es aber nach wie vor gewisse Mindestanforderungen, die Ihre Organisation erfüllen muss, um sich nicht aufsichtsbehördlichen Maßnahmen auszusetzen. Anders gesagt: Es gibt Risiken, die Ihre Organisationen nicht einfach hinnehmen dürfen, sondern mindern oder vermeiden müssen. Sie müssen sich dies wie obligatorische Kontrollen vorstellen, die der Gesetzgeber in die Vorschriften aufgenommen hat, weil sie immer sinnvoll sind. Dies betrifft insbesondere das Schutzziel der Verarbeitung nach Treu und Glauben. Ihre EU-Institution kann nicht einfach sagen: „Wir geben keine Auskunft, das ist zu viel Aufwand.“ Sie kann aber, in geeigneten Fällen, sagen: „Da wir bei diesem neuen System nur wenige Auskunftsanträge erwarten, werden wir nicht in ein automatisiertes Selbstbedienungssystem investieren, über das die Betroffenen selbst Zugang erlangen, sondern lediglich eine Kontaktstelle angeben, die die eingehenden Anträge händisch bearbeitet.“

Bei der Auswahl der Maßnahmen zur Risikokontrolle / -minderung ist die Einhaltung der Verordnung die Mindestanforderung, die auf jeden Fall erfüllt sein muss.

Die Risikokontrollen können auf die Wahrscheinlichkeit (Beispiel: Schulung der Mitarbeiter in der Personalabteilung führt dazu, dass die Offenlegung gegenüber Unbefugten weniger wahrscheinlich ist; dies ändert aber ggf. nichts an den Auswirkungen, falls es doch passiert), die Auswirkungen (Beispiel: Wenn alle Datenspeicher verschlüsselt sind, sind die Auswirkungen, wenn ein USB-Stick mit personenbezogenen Daten im Zug vergessen wird, geringer; dies ändert aber nichts an der Wahrscheinlichkeit, dass dies passiert) oder beides abzielen. Manchmal mag es möglich sein, Risiken ganz auszuschalten (Beispiel: Neugestaltung des Verarbeitungsvorgangs, damit keine personenbezogenen Daten gebraucht werden – Daten, die man nicht hat, können nicht rechtswidrig offengelegt werden).

Sie können ganz neue Risikokontrollen gestalten oder sich von bewährten Katalogen inspirieren lassen, zum Beispiel von den themenspezifischen Leitlinien des EDSB¹⁵ und anderer DSB; den Leitlinien nationaler, europäischer und internationaler Normierungsorganisationen wie BSI, CEN/CENELEC/ETSI und ISO; den Leitlinien von Organisationen und Projekten im Bereich der Informationssicherheit wie ENISA und OWASP; von Erkenntnissen aus wissenschaftlichen Arbeiten, von der EU kofinanzierten Forschungsprojekten sowie Initiativen, die im Bereich der technischen Lösungen für Sicherheit und Schutz der Privatsphäre arbeiten (wie z. B. das Internet Privacy Engineering Network¹⁶) und auch von den eigenen Vorschriften Ihrer Organisation auf dem Gebiet der Informationssicherheit. Achten Sie darauf, dass die von Ihnen gewählten Risikokontrollen den Anforderungen der Verordnung genügen.

¹⁵ Dies ist stets im Hinblick auf den konkreten Kontext zu überprüfen – die Leitlinien des EDSB geben allgemeine Empfehlungen, deren Anwendung auf Ihre Organisation unter Umständen von den Besonderheiten des Verarbeitungsvorgangs abhängig ist.

¹⁶ Nähere Informationen sowie Informationsbibliothek, siehe: https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

Hier sind beispielhaft einige allgemeine Kontrollmaßnahmen danach, wie sie zur Risikokontrolle beitragen, in Gruppen zusammengefasst:

-) Prävention: verhindern, dass Risiken eintreten, z. B. indem Sie:
 - Mitarbeiter aufklären, um unbefugter Datenweitergabe vorzubeugen;
 - Aufbewahrungsfristen und erhobene Datenmengen auf das Minimum begrenzen, so dass es weniger Daten gibt, die rechtswidrig bekannt werden könnten, und die Versuchung, den Zweck nachträglich zu ändern, geringer ist;
 - Nutzermanagement vorsehen, um die Zugangsrechte derjenigen, die nicht mehr auf die Kenntnis angewiesen sind (weil sie zum Beispiel auf eine andere Stelle versetzt wurden), schnell zu deaktivieren;
 - personenbezogene Daten trennen, damit Vertraulichkeitsverletzungen in einem Bereich keine Auswirkungen auf andere Bereiche haben;
-) Aufdeckung: Verarbeitungsvorgänge überwachen, um sicherzustellen, dass Sie Verletzungen schnell erkennen, z. B. indem Sie:
 - Vorgänge protokollieren und selbst überwachen, um Datenschutzverletzungen oder rechtswidrige Nutzung zu erkennen;
 - aufzeichnen, wann und wie die betroffenen Personen über die Verarbeitung unterrichtet wurden;
-) Repression: sicherstellen, dass Sie über die Mittel verfügen, festgestellte Datenschutzverletzungen schnell zu unterbinden, z. B. durch:
 - Verfahren zur Berichtigung unrichtiger Daten;
 - Vorkehrungen für den Widerruf von Zertifikaten, um die missbräuchliche Verwendung von Berechtigungsnachweisen zu unterbinden;
-) Korrektur: sicherstellen, dass Sie die Mittel haben, eingetretene Schäden zu beheben oder zu begrenzen, z. B. durch:
 - Anfertigung von Sicherungskopien, damit Sie den Status quo ante wiederherstellen können, falls Ihre Systeme beschädigt wurden;
 - Benachrichtigung der Empfänger unbefugter Übermittlungen mit der Anweisung, die Daten zu löschen.

Nachstehend finden Sie einige Beispiele für Risikokontrollen, die nach dem Schutzziel in Gruppen zusammengefasst sind. Da die Risiken (und damit auch die vorzusehenden Risikokontrollen) vom konkreten Verarbeitungsvorgang abhängig sind, für den Sie die DSFA durchführen, können diese Beispiele nur ein Ausgangspunkt für Ihre Überlegungen sein.

Schutzziel	Allgemeine Risikokontrollen
Verarbeitung nach Treu und Glauben) bei der Wiederverwendung von Datenmengen die zulässige / erwartete Nutzung prüfen
Transparenz) betroffene Personen automatisch unterrichten
Zweckbindung) Exportfunktionalitäten begrenzen) Allgemeine Identifikatoren vermeiden
Datenminimierung) Altersgruppen statt Geburtsdaten erheben
Richtigkeit) Stimmigkeitsprüfungen) Datenqualität überprüfen

Speicher-begrenzung) unterschiedliche Aufbewahrungsfristen für verschiedene Teile der Daten; Zugangsbeschränkung auf relevante Profile
Sicherheit) Siehe ISRM-Rahmen Ihrer EU-Institution

Abbildung 13: Liste mit Beispielen für allgemeine Risikokontrollen, geordnet nach Schutzziele

Wählen Sie die Risikokontrollen, die erforderlich sind, um die Einhaltung der Vorschriften und angemessene Risikominderung sicherzustellen.

Wenn Sie denken, dass diese verbessert werden müssen, um die Risiken auf ein annehmbares Maß zu mindern, stellen Sie einen Verbesserungsplan mit den für erforderlich erachteten Maßnahmen und den Fristen für deren Umsetzung auf.

3.7 Dokumentierung und Berichterstattung

Der DSFA-Prozess hilft Ihnen, die Auswirkungen der Verarbeitungsvorgänge im Hinblick auf Privatsphäre und Datenschutz zu bedenken. Zum Nachweis dafür, dass Sie diesen Prozess durchlaufen haben, müssen Sie ihn dokumentieren.

Das wichtigste Produkt des DSFA-Prozesses ist der DSFA-Bericht, in dem die Ergebnisse aus diesem Abschnitt zusammengefasst werden. Anhang 3 enthält eine Vorlage für den DSFA-Bericht.

Der DSFA-Bericht ist das Hauptprodukt des DSFA-Prozesses.

3.8 Überprüfungszyklen

Eine Datenschutz-Folgenabschätzung ist ein Prozess, sie ist also niemals endgültig erledigt. Insofern ist sie anderen Managementprozessen, etwa dem ISRM, vergleichbar.

Die Länge des Überprüfungszyklus ist nach den Risiken für Ihre Verarbeitungsvorgänge zu bemessen. Die höher die Risiken, desto kürzer sollte der Überprüfungszyklus sein. Die Länge des Zyklus bestimmt der Verantwortliche für die Datenverarbeitung. Der Europäische Datenschutzbeauftragte empfiehlt grundsätzlich einen Überprüfungszyklus von zwei Jahren, mit außerordentlichen Überprüfungen, falls Verarbeitungsvorgänge erheblich verändert werden. Es kann auch andere Umstände geben, die eine außerordentliche Überprüfung erfordern, zum Beispiel im Falle erheblicher Datenschutzverletzungen, an denen deutlich wird, dass die Sicherheitsvorkehrungen Ihrer EU-Institution möglicherweise nicht ausreichen. Geringfügigere Veränderungen wie Verbesserungen der Sicherheitsvorkehrungen im Zuge der kontinuierlichen Verbesserung Ihrer Dienste erfordern nicht unbedingt eine Aktualisierung der Datenschutz-Folgenabschätzung: Prüfen Sie, ob Ihre Datenschutz-Folgenabschätzung immer noch auf die tatsächliche Risikobehandlung zutrifft, und aktualisieren Sie sie erforderlichenfalls.¹⁷

¹⁷ Beispiel: Eine der von Ihnen getroffenen organisatorischen Maßnahmen zur Verhinderung von Vertraulichkeitsverletzungen sieht vor, dass die Nutzer eines bestimmten Systems Vertraulichkeitserklärungen unterzeichnen müssen. Der Wortlaut der Erklärung wird aktualisiert, so dass er noch strenger ist. Dies würde wahrscheinlich keine Aktualisierung des DSFA-Berichts erfordern.

Es ist vielleicht sinnvoll, diese Überprüfungszyklen mit anderen regelmäßigen Überprüfungen relevanter Prozesse und deren Dokumentierung zu synchronisieren (z. B. mit dem ISRM oder internen Kontrollmaßnahmen).

Die DSFA-Berichte sind regelmäßig zu überprüfen (Vorschlag: alle zwei Jahre), erforderlichenfalls sind außerordentliche Überprüfungen vorzunehmen.

3.9 Veröffentlichung von DSFA-Berichten

Die Verordnung enthält keine besondere Vorschrift über die Veröffentlichung von DSFA-Berichten. Nach Ansicht des Europäischen Datenschutzbeauftragten hat sich die Veröffentlichung von DSFA-Berichten jedoch bewährt. Sie sollten bestrebt sein, zumindest eine Zusammenfassung des Berichts zu veröffentlichen. Teile der Berichte, die nicht öffentlich verbreitet werden sollten (z. B. Angaben zu Sicherheitsmaßnahmen), können gegebenenfalls entfernt werden.¹⁸

Es kann daher sinnvoll sein, Ihren DSFA-Prozess so zu dokumentieren, dass die Teile der Dokumentation, die öffentlich sind (oder veröffentlicht werden können), leicht von denjenigen zu unterscheiden sind, die intern bleiben sollten. Die Vorlage für einen DSFA-Bericht in Anhang 3 ist so gegliedert, dass Sie leicht entscheiden können, welche Teile Sie veröffentlichen und welche intern bleiben sollen.

Die Veröffentlichung trägt dazu bei, den Interessenträgern und der allgemeinen Öffentlichkeit zu versichern, dass Ihre EU-Institution die Datenschutzvorschriften einhält; dies schafft Vertrauen und zeigt, dass die EU-Institutionen bei der Wahrung der Grundrechte mit gutem Beispiel vorangehen. Zur Veröffentlichung von DSFA-Berichten eignen sich Ihr öffentlich zugängliches Register und der Teil der Website Ihrer EU-Institution, in dem die Regelung erklärt wird, für die die Verarbeitungsvorgänge eingesetzt werden.

„Tu Gutes und rede darüber“ – Es ist sinnvoll, die DSFA-Berichte zumindest in Form einer Zusammenfassung zu veröffentlichen. Die Veröffentlichung zeigt, dass darauf geachtet wurde, die Verarbeitungsvorgänge rechtskonform zu gestalten. Das schafft Vertrauen bei Ihren Interessenträgern und bei der allgemeinen Öffentlichkeit.

4. In welchen Fällen ist eine vorherige Konsultation durchzuführen?

Die vorherige Konsultation des Europäischen Datenschutzbeauftragten ist nicht bei allen Verarbeitungsvorgängen, für die eine DSFA erforderlich ist, nötig, sondern nur in „grauen“ Fällen. Dies sind die Fälle, in denen Sie sich nicht sicher sind, ob die vorgenommene Risikominderung ausreicht, die Risiken jedoch nicht so groß sind, dass ganz klar ist, dass das Projekt aufgegeben werden muss. In einer solchen Situation sollten Sie sich an Ihren Datenschutzbeauftragten wenden.

Artikel 40 Absatz 1 der Verordnung bestimmt, dass der Verantwortliche vor der Verarbeitung den Europäischen Datenschutzbeauftragten konsultiert, wenn aus einer Datenschutz-Folgenabschätzung „hervorgeht, dass die Verarbeitung ohne Garantien,

¹⁸ Bitte beachten Sie, dass die vollständige DSFA-Dokumentation als Dokument Ihrer EU-Institution dem Recht auf Zugang der Öffentlichkeit gemäß der Verordnung (EG) 1049/2001 unterliegt.


Sicherheitsvorkehrungen und Verfahren zur Risikominderung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte, und das Risiko nach Auffassung des Verantwortlichen nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel gemindert werden kann“. In einem solchen Fall muss der Verantwortliche – nach Beratung durch den Datenschutzbeauftragten – eine vorherige Konsultation des Europäischen Datenschutzbeauftragten vornehmen.¹⁹ Wie dem Begriff zu entnehmen ist, muss diese Konsultation erfolgen, bevor mit den Verarbeitungsvorgängen begonnen wird.

Nach den von der Artikel-29-Datenschutzgruppe herausgegebenen DSFA-Leitlinien ist nicht bei allen Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung erforderlich ist, auch die vorherige Konsultation erforderlich.

1. Es gibt Fälle, in denen die in der Datenschutz-Folgenabschätzung erkannten Risiken durch (zusätzliche) Kontrollmaßnahmen auf ein annehmbares Risikoniveau gemindert werden können. In solchen Fällen ist keine vorherige Konsultation nötig.
2. Es kann auch vorkommen, dass Sie nach der Datenschutz-Folgenabschätzung feststellen, dass es Risiken gibt, die nicht auf ein annehmbares Maß gemindert werden können. In einem solchen Fall müssen Sie das Projekt aufgeben, wenn es sich als unmöglich erweist, es auf gesetzeskonforme Weise zu implementieren.
3. Es wird Fälle geben, in denen Sie erkennen, dass Verbesserungen nötig sind, um die Risiken auf ein annehmbares Niveau zu mindern, und dass aktuell noch „hohe Restrisiken“ bestehen. Für solche „grauen“ Fälle ist die vorherige Konsultation gedacht.

Davon unabhängig kann die Europäische Kommission gemäß Artikel 40 Absatz 4 der Verordnung im Wege eines Durchführungsrechtsakts eine Liste der Fälle festlegen, 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. Bislang hat die Europäische Kommission dies noch nicht getan. Sollte die Europäische Kommission dies jedoch tun, werden wir die betreffenden (Arten von) Verarbeitungsvorgänge(n) unserer Liste gemäß Artikel 39 Absatz 4 hinzufügen.

Nachstehend finden Sie einen Überblick über das Zusammenspiel der Vorschriften über „Verzeichnisse von Verarbeitungstätigkeiten“ (Artikel 31), Datenschutz-Folgenabschätzungen (Artikel 39) und vorherige Konsultation (Artikel 40). Für alle Verarbeitungsvorgänge sind Verzeichnisse erforderlich; für einige wird eine DSFA erforderlich sein; und für einige von diesen ist auch die vorherige Konsultation erforderlich.



Compliance-Kontrolle und Verzeichnisse von Verarbeitungstätigkeiten (für alle Verarbeitungsvorgänge)
DSFA (für „hohes Risiko“, EDSB-Liste und Durchführungsrechtsakte gemäß Artikel 40 Absatz 4)
Vorherige Konsultation (für „hohes Restrisiko“ und Durchführungsrechtsakte gemäß Artikel 40 Absatz 4)

¹⁹ Artikel 39 der Verordnung (EU) 2016/794 sieht eine besondere Verpflichtung zur „vorherigen Konsultation“ des Europäischen Datenschutzbeauftragten im Falle von Europol vor. Dies ist eine andere Verpflichtung, für die andere Voraussetzungen gelten.

Wenn Sie eine vorherige Konsultation durchführen, wird der Europäische Datenschutzbeauftragte die eingereichte Dokumentation prüfen und erforderlichenfalls zu Verbesserungen raten. Was den zeitlichen Ablauf angeht, sollten Sie die vorherige Konsultation zu einem Zeitpunkt vornehmen, zu dem Sie noch in der Lage sind, die in der Erwiderung gegebenen Empfehlungen zu berücksichtigen. Wenn Sie den Bau des Systems für Ihren geplanten Verarbeitungsvorgang an einen Auftragnehmer vergeben wollen, wäre es sinnvoll, den Zeitpunkt zu wählen, zu dem Sie die Ausschreibungsunterlagen / technische Spezifikation fast fertiggestellt, das Vergabeverfahren jedoch noch nicht begonnen haben,

Die Unterlagen für das Ersuchen um vorherige Konsultation ist im Wesentlichen der DSFA-Bericht.²⁰ Bitte übersenden Sie folgende Unterlagen:

-) das Verzeichnis und den vollständigen DSFA-Bericht;
-) den Plan für die Risikobearbeitung, mit Erklärungen zu den geplanten Verbesserungen der Risikokontrollen;
-) die dazugehörigen Unterlagen aus Ihrem ISRM-Prozess;
-) alle sonstigen Unterlagen, die Ihres Erachtens notwendig sind, um die mit der geplanten Verarbeitung und der Auswahl der Risikokontrollen verbundenen Risiken zu verstehen.

Auf Ihr Konsultationsersuchen hin wird der Europäische Datenschutzbeauftragte Empfehlungen dazu geben, wie die Vorschriftseinhaltung sichergestellt werden kann.

Nach Artikel 40 der Verordnung muss der Europäische Datenschutzbeauftragte die Empfehlungen innerhalb von acht Wochen ab Eingang des Ersuchens um Konsultation erteilen, wobei diese Frist bis zum Eingang angeforderter Informationen ausgesetzt werden kann. Die Frist kann unter Berücksichtigung der Komplexität des Falles innerhalb eines Monats nach Eingang des Ersuchens um sechs Wochen verlängert werden. Der Europäische Datenschutzbeauftragte wird die Verantwortlichen (sowie ggf. die Auftragsverarbeiter) unter Angabe der Gründe von der Verlängerung unterrichten.²¹

Beantwortet der Europäische Datenschutzbeauftragte das Ersuchen nicht fristgerecht, lässt dies mögliche spätere Eingriffe durch ihn unberührt (siehe Erwägungsgrund 58 der Verordnung).

Artikel 27 der alten Verordnung sah vor, dass man bestimmte „riskante“ Verarbeitungsvorgänge dem Europäischen Datenschutzbeauftragten zur Vorabkontrolle melden musste. Es gibt allerdings einige wichtige Unterschiede zwischen der Vorabkontrolle nach der alten Verordnung und der vorherigen Konsultation nach der jetzigen Verordnung:

-) unterschiedliche Voraussetzungen: Restrisiko im Gegensatz zu besonderen Risiken;
-) Nichtbeantwortung ist nicht als Genehmigung zu werten.

Wegen der Verschiedenheit der Voraussetzungen wird die Zahl der künftigen vorherigen Konsultationen geringer sein als die der bisherigen Vorabkontrollen.

²⁰ Die in Artikel 40 Absatz 3 Buchstaben a bis c genannten Informationen sind schon im DSFA-Bericht enthalten (die Informationen unter Buchstabe d sind dem Europäischen Datenschutzbeauftragten ohnehin bekannt).

²¹ Für vorherige Konsultation im Rahmen von Kapitel IX der Verordnung gelten andere Fristen: sechs Wochen mit der Möglichkeit der Verlängerung um vier Wochen, wobei die Verlängerung innerhalb des erstens Monats mitzuteilen ist (Artikel 90).

5. Was ist zu tun?

Als Durchführungsverantwortlicher aufseiten des Verantwortlichen brauchen Sie mit Ihrer Dokumentation nicht bei Null anzufangen. Die EU-Institutionen führen bereits Verarbeitungsvorgänge durch, bei denen die Voraussetzungen für die Durchführung einer Datenschutz-Folgenabschätzung erfüllt sind. Viele davon werden bereits gemäß Artikel 27 der alten Verordnung zur Vorabkontrolle gemeldet worden sein. Auch wenn die Voraussetzungen nach der alten Verordnung (Vorabkontrolle) und der neuen Verordnung nicht dieselben sind, gibt es doch gewisse Überschneidungen. Für die meisten Verarbeitungsvorgänge, für die nach der Verordnung eine Datenschutz-Folgenabschätzung erforderlich ist, war auch schon nach der alten Verordnung eine Vorabkontrolle nötig. Es gibt auch Verarbeitungsvorgänge, die nach der alten Verordnung zur Vorabkontrolle zu melden waren, für die jedoch keine Datenschutz-Folgenabschätzung nötig ist.

Zur Vorbereitung auf die neue Verordnung sollten Sie prüfen, welche Fälle Ihre EU-Institution bisher zur Vorabkontrolle melden musste. Für einige dieser Fälle ist unter Umständen eine Datenschutz-Folgenabschätzung erforderlich.

Wie im Falle bestehender Verarbeitungsvorgänge, die unter Umständen einer Datenschutz-Folgenabschätzung bedürfen, zu verfahren ist, erfahren Sie im Folgenden:

(i) Abgeschlossene Fälle der Vorabkontrolle

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung erforderlich ist und für die bereits eine Vorabkontrolle nach der alten Verordnung mit positivem Ergebnis vorliegt (und etwaige Folgemaßnahmen ggf. erledigt wurden), gilt eine Schonfrist von zwei Jahren, so dass Sie die Datenschutz-Folgenabschätzung nicht sofort brauchen.

Sollten sich die Verfahren und/oder Risiken jedoch ändern, wird eine Datenschutz-Folgenabschätzung erforderlich sein, um zu prüfen, ob die Verordnung nach wie vor eingehalten wird.

(ii) Noch nicht erledigte Folgemaßnahmen zu Stellungnahmen im Rahmen der Vorabkontrolle

Sollten die Folgemaßnahmen zu Verarbeitungsvorgängen, die der Vorabkontrolle gemäß Artikel 27 der alten Verordnung und einer Datenschutz-Folgenabschätzung nach der Verordnung bedürfen, bei Inkrafttreten der Verordnung noch nicht erledigt worden sein, sollten Sie mittels einer Schwellenwertanalyse (siehe Teil I – Abschnitt 4) prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

6. Schlusswort

Teil II des *Toolkits Rechenschaftspflicht in der Praxis* erklärt Ihnen, wann Sie eine Datenschutz-Folgenabschätzung durchführen müssen und wann zusätzlich eine vorherige Konsultation des Europäischen Datenschutzbeauftragten erforderlich ist.

Als die im Geschäftsbereich zuständige Person tragen Sie 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.

Datenschutz-Folgenabschätzungen sind ein wichtiges Instrument, mit dem Sie bei Ihren Verarbeitungsvorgängen, für die ein erhöhtes Risiko festgestellt wurde, die Risiken im Hinblick

auf den Schutz der Privatsphäre und Datenschutz managen können. Indem Sie den Prozess durchlaufen, gewinnen Sie Nachweise dafür, dass Sie diese Risiken bedacht und für das Risikomanagement Mittel ausgewählt haben, die angesichts der Risiken gerechtfertigt sind. Wenn der Europäische Datenschutzbeauftragte prüft, ob Ihre EU-Institution ihren Datenschutzpflichten genügt, wird er sich mit Sicherheit Ihre Datenschutz-Folgenabschätzungen ansehen. Werden die Datenschutz-Folgenabschätzungen nicht ordnungsgemäß durchgeführt, kann dies mit Geldbußen gegen Ihre EU-Institution geahndet werden.²²

In besonders komplizierten Fällen ersuchen Sie den Europäischen Datenschutzbeauftragten um vorherige Konsultation; in seiner Antwort wird der Europäische Datenschutzbeauftragte Empfehlungen dazu geben, wie die Einhaltung der Datenschutzvorschriften sichergestellt werden kann. Die Verordnung setzt jedoch vor allem auf die „Rechenschaftspflicht“, weshalb wir nicht erwarten, dass es in vielen Fällen eine vorherige Konsultation geben wird. Wir rechnen jedenfalls damit, dass vorherige Konsultationen seltener vorkommen werden als die Vorabkontrollen nach der alten Verordnung.

²² Artikel 66 der Verordnung. Ein Leitlinienentwurf ist den Datenschutzbeauftragten informationshalber zugeschickt worden.

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;

-) entwirft die Datenschutz-Folgenabschätzungen;
-) analysiert, ob die vorherige Konsultation fortzuführen ist.

Datenschutzbeauftragter:

-) leitet die Verantwortlichen durch den DSFA-Prozess;
-) gibt Feedback zum Entwurf der Dokumentation / Datenschutz-Folgenabschätzung
-) erwidert auf Konsultationsersuchen von Verantwortlichen / im Geschäftsbereich Zuständigen;
-) dient als Verbindungsstelle zwischen der EU-Institution und dem Europäischen Datenschutzbeauftragten, auch bei Ersuchen um vorherige Konsultation.

Sonstige Funktionen (z. B. IT oder Rechtsabteilung)

-) unterstützt den Verantwortlichen / im Geschäftsbereich Zuständigen und den Datenschutzbeauftragten, soweit erforderlich.

2. Leitfragenkatalog zu den Datenschutzgrundsätzen

Leitfragen zur Verarbeitung nach Treu und Glauben

1. Wäre diese Verarbeitung auch für diejenigen, die sich den Datenschutzhinweis nicht durchgelesen haben, zu erwarten?
2. Wenn die Verarbeitung auf Einwilligung beruht: Wurde diese wirklich freiwillig erteilt? Wie dokumentieren Sie, dass die Einwilligung erteilt wurde? Wie kann die Einwilligung widerrufen werden?
3. Könnte dies abschreckende Wirkung haben?
4. Könnte dies zu Diskriminierung führen?
5. Ist es für die Betroffenen einfach, ihre Rechte auf Auskunft, Berichtigung, Löschen usw. auszuüben?

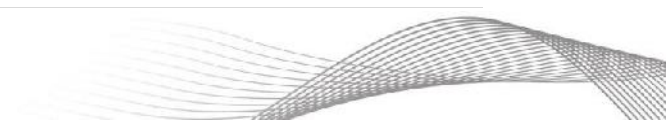
Leitfragen zur Transparenz

1. Wie stellen Sie sicher, dass Sie mit Ihren Informationen tatsächlich die betroffenen Personen erreichen?
2. Sind die Informationen vollständig und leicht verständlich?
3. Sind sie auf die Zielgruppe zugeschnitten? Für Kinder sind z. B. unter Umständen speziell zugeschnittene Informationen erforderlich.
4. Falls Sie die Betroffenen erst später unterrichten wollen: Weshalb ist dies begründet?

Leitfragen zur Zweckbindung

1. Haben Sie alle Zwecke Ihres Verarbeitungsvorgangs festgestellt?
2. Sind alle Zwecke mit dem ursprünglichen Zweck vereinbar?

3. Besteht das Risiko, dass die Daten zu anderen Zwecken wiederverwendet werden könnten (schleichende Ausweitung auf andere Zwecke)?
4. Wie können Sie sicherstellen, dass Daten ausschließlich zu den für sie festgelegten Zwecken verwendet werden?
5. Falls Sie Daten für wissenschaftliche Forschung, zu statistischen oder historischen Zwecken bereitstellen bzw. wiederverwenden wollen: Welche Maßnahmen haben Sie ergriffen, um die betroffenen Personen zu schützen?



Leitfragen zur Datenminimierung

1. Ist die Datenqualität dem Zweck angemessen?
2. Können Sie mit den Daten, die Sie erheben, messen, was Sie zu messen beabsichtigen?
3. Gibt es Teile der Daten, die Sie entfernen (oder ausblenden / verbergen) könnten, ohne dass der Zweck der Verarbeitung beeinträchtigt würde?
4. Wird auf den Formularen klar zwischen Pflicht- und optionalen Angaben unterschieden?
5. Falls Sie Informationen zu statistischen Zwecken speichern möchten: Wie managen Sie das Risiko der Re-Identifizierung?

Leitfragen zur Richtigkeit

1. Welche Folgen könnte es für die betroffenen Personen haben, wenn bei diesem Verarbeitungsvorgang auf Grundlage unrichtiger Informationen gehandelt würde?
2. Wie stellen Sie die Richtigkeit der Daten, die Sie selbst erheben, sicher?
3. Wie stellen Sie sicher, dass Daten, die Sie von Dritten erlangen, richtig sind?
4. Ist es mit Ihren Tools möglich, Daten erforderlichenfalls zu aktualisieren / zu berichtigen?
5. Sind mit Ihren Tools Stimmigkeitsprüfungen möglich?

Leitfragen zur Speicherbegrenzung

1. Sehen die Unionsvorschriften Speicherfristen für Ihren Verarbeitungsvorgang vor?
2. Wie lange müssen Sie die Daten speichern? Zu welchem/n Zwecke(n)?
3. Können Sie die Speicherfristen für verschiedene Teile der Daten unterscheiden?
4. Falls Sie die Daten noch nicht löschen können: Können Sie den Zugang dazu beschränken?
5. Ist mit Ihren Tools eine automatisierte dauerhafte Löschung bei Ablauf der Speicherfrist möglich?

Leitfragen zur Sicherheit

1. Haben Sie ein Verfahren für die Erkennung, Analyse und Bewertung von Informationssicherheitsrisiken mit etwaigen negativen Auswirkungen auf personenbezogene Daten und die deren Verarbeitung unterstützenden IT-Systeme?
2. Wurden auch die Auswirkungen auf die Grundrechte, Freiheiten und Interessen der betroffenen Personen und nicht nur die Risiken für Ihre Organisation bedacht?
3. Wurden bei der Beurteilung der Risiken Art, Umfang, Umstände und Zweck der Verarbeitung berücksichtigt?
4. Gibt es ein auf die Schwachstellen Ihres Systems und die Gefährdung Ihrer Daten und Systeme zugeschnittenes Risikomanagement?
5. Haben Sie speziell für die Durchführung der Risikobewertung vorgesehene Ressourcen und Mitarbeiter?
6. Führen Sie systematische Überprüfungen und Aktualisierungen der Sicherheitsvorkehrungen durch, die den Verarbeitungskontext und die Risiken berücksichtigen?

3. Gliederung der Vorlage für den DSFA-Bericht

Die nachstehende Gliederung kann als Vorlage für DSFA-Berichte dienen.

1. Projektbezeichnung

2. Validierung / Abzeichnung

Genehmigungskette und Abzeichnung

3. Überprüfung

Angaben zu Überprüfungszyklus, aktuellem Status und Versionierungsinformationen zu früheren Fassungen

4. Zusammenfassung

Kurzer Überblick über die Hauptergebnisse der Datenschutz-Folgenabschätzung; festgestellte Hauptrisiken, ausgewählte Risikokontrollen ...

5. Grund für diese Datenschutz-Folgenabschätzung

Kurz erklären: (a) in Positivliste aufgeführt oder (b) Ergebnis der Schwellenwertanalyse

6. Beteiligte Hauptakteure

Überblick darüber, wer wann an welchen Teilen mitgearbeitet hat

7. Beschreibung der Verarbeitung

Mit den Angaben im Verzeichnis für den Verarbeitungsvorgang als Ausgangspunkt Folgendes erstellen:

-) Datenflussdiagramm für den Verarbeitungsvorgang (Flussdiagramm): Welche Daten erfassen wir wo / von wem, was tun wir damit, wo speichern wir sie, an wen geben wir sie weiter?*
-) Detaillierte Beschreibung aller Zwecke des Verarbeitungsvorgangs: Darstellung der einzelnen Schritte des Vorgangs, erforderlichenfalls mit Unterscheidung der verschiedenen Zwecke.*
-) Beschreibung des Zusammenspiels mit anderen Verarbeitungsvorgängen: Werden für diesen Verarbeitungsvorgang personenbezogene Daten aus anderen Systemen verarbeitet? Werden personenbezogene Daten aus diesem Verarbeitungsvorgang in anderen Verarbeitungsvorgängen wiederverwendet?*
-) Beschreibung der dazugehörigen Infrastruktur: Dateisysteme, IT usw.*

8. Notwendigkeit und Verhältnismäßigkeit

Mit den Angaben im Verzeichnis für den Verarbeitungsvorgang als Ausgangspunkt Folgendes erklären:

-) warum die vorgeschlagenen Verarbeitungsvorgänge für Ihre EU-Institution notwendig sind, um die ihr übertragene Aufgabe wahrzunehmen;*
-) dass sich die Verarbeitung im Rahmen des für die Wahrnehmung der Aufgabe Verhältnismäßigen hält.*

9. Risikoanalyse und Festlegung der im Hinblick auf die festgestellten Risiken ergriffenen Risikokontrollen

Hier können Sie die Liste in Anhang 2 zum Ausgangspunkt nehmen

Nr .	Position im Datenflussdiagramm	Risikobeschreibung	Einschlägige Datenschutzgrundsätze (einer oder mehrere)	Schweregrad (gesamt)	Wahrscheinlichkeit	Risikokontrollen	Schweregrad (Restrisiko)	Wahrscheinlichkeit
1	Elektronische Personalakten	Unbefugte Sekundärnutzung	Zweckbindung, Sicherheit	3	3	Datenschutzschulung für Mitarbeiter Beschränkung durch Zugangskontrollliste derjenigen, die auf die Kenntnis angewiesen sind Zugangsprotokollierung und Protokollanalyse;	3	1
2	Elektronische Personalakten	Datenbeschädigung	Datenqualität, Sicherheit	4	1	Änderungsprotokollierung, Speicherung von Sicherungskopien	1	1
...								
n								

10. Anmerkungen zum Datenschutz (ggf.)

Wen haben Sie konsultiert? Welche Anmerkungen und Bedenken wurden in der Konsultation geäußert? Wie wurden diese berücksichtigt (z. B. durch Ergänzung zusätzlicher Risiken im obigen Abschnitt 7)?

11. Anmerkungen des Datenschutzbeauftragten

Welche Anmerkungen und Bedenken wurden vom Datenschutzbeauftragten geäußert? Wie wurden diese berücksichtigt (z. B. durch Ergänzung zusätzlicher Risiken im obigen Abschnitt 5)?

4. Referenzdokumente

4.1. Sonstige DSFA-Methoden von Mitgliedern des Europäischen Datenschutzausschusses (EDSA)

Wenn Sie die in diesem Dokument vorgeschlagenen Methoden nicht benutzen möchten, steht es Ihnen frei, die nachstehend genannten Methoden zu verwenden, sofern sie erforderlichenfalls angepasst werden, um den Anforderungen nach der DSGVO / der Verordnung zu genügen.

-) Belgischer Ausschuss für den Schutz des Privatlebens: DPIA-Leitlinien ([FR/NL](#))
-) Dänemark [Datatilsynet – Konsekvensanalyse](#) (März 2018)
-) Deutschland (Datenschutzkonferenz): Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern): [DE](#) / [EN](#)
-) Spanische Datenschutzbehörde – [Guía práctica de Evaluaciones de impacto \(2018\)](#)
-) Französische CNIL
 - o [DPIA Software Tool](#) (aktualisiert 2018)
 - o [CNIL Privacy Impact Assessment Manuals 1 \(Methodology\), 2 \(Tools: templates & knowledge bases\) & 3 \(Good Practices\)](#); Juli 2015
-) Slowenische Datenschutzbehörde: [Smernice ocene u inkov na varstvo osebnih podatkov \(2018\)](#)
-) UK Information Commissioner [Data Protection Impact Assessments](#) (Mai 2018)

4.2. Sonstige (D)SFA-Methoden Dritter

Diese Methoden wurden von Dritten (z. B. von Datenschutzbehörden in Drittländern) beschlossen. Sie genügen unter Umständen nicht den Anforderungen nach der DSGVO oder der Verordnung und sind hier nur als Hintergrundinformation aufgeführt:

-) Australian Information Commissioner – [Guide to undertaking privacy impact assessment \(Mai 2014\)](#)
-) Canadian Privacy Commissioner – [Guide for submitting privacy impact assessment \(März 2011\)](#)
-) New Zealand's Privacy Commissioner (2015) - [Privacy Impact Assessment Toolkit](#)
-) USA DHS – [PIA guidance & template \(Juni 2010\)](#)
-) USA SEC – [PIA guide \(Januar 2007\)](#)
-) USA NIST – [An Introduction to Privacy Engineering and Risk Management in Federal Systems](#) (Januar 2017)
-) Ireland HIQA – [Guidance on Privacy Impact Assessment in Health and Social Care \(Dezember 2010\)](#) [ISO/IEC 29134:2017](#)
-) [ISACA GDPR Data Protection Impact Assessments](#) (2017)
-) [NL NOREA – De beroepsorganisatie van IT-auditors](#) (November 2015)
-) Forum Privatheit: [White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz, dritte, überarbeitete Auflage](#), zum Teil auf dem Standard-Datenschutzmodell basierend
-)

4.3. Forschungsberichte und wissenschaftliche Literatur

- J Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M. (2016): [A Process for Data Protection Impact Assessment under the European General Data Protection Regulation](#), in: K. Rannenber, D. Ikonomou (Hrsg.): Privacy Technologies and Policy. Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London.
- J Bieker, F., Hansen, M., Friedewald, M. (2016): Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2016, Ausgabe 4, S. 188.
- J Hansen, M. (2016): Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge?, [DuD 9/2016, S. 587](#).
- J Ireland HIQA (2010): [International Review of Privacy Impact Assessments](#).
- J PIAF Project Consortium (de Hert, Paul et al.) Deliverables: [Review and analysis of existing PIA](#) (2011), [survey of DPAs on PIAs](#) (2012), [Final report with recommendations for a EU PIA framework](#) (2012), [Website](#).
- J Wright, D., Finn, R., Rodrigues, R. (2013): A Comparative Analysis of Privacy Impact Assessment in Six Countries, [Journal of Contemporary European Research \(JCER\)](#), 9 (1), [S. 160](#).

5. 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.
Angemessenheitsbeschluss	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 Datenschutzbeauftragter (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).
Datenschutzkoordinator	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.
Durchführungsverantwortlicher aufseiten des für die	Als für die Datenverarbeitung Verantwortlicher ist Ihre EU-Institution für die Verarbeitungsvorgänge rechenschaftspflichtig; wobei jedoch in der Regel die Ausführungsverantwortung auf einer

Verarbeitung Verantwortlichen	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 ersetzt die WP29.
Europäischer Datenschutzbeauftragter (EDSB)	Die Datenschutzbehörde für die EU-Institutionen (siehe Verordnung).
Informationssicherheitsrisikomanagement (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-Terminologie 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,

	<p>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.</p>
Profiling	<p>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).</p>
Rechenschaftspflicht	<p>Ein Grundsatz, der sicherstellen soll, dass die für die Verarbeitung Verantwortlichen im allgemeinen in der Lage sind, die Einhaltung datenschutzrechtlicher 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.</p>
Recht auf Auskunft	<p>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).</p>
Recht auf Berichtigung	<p>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).</p>
Recht auf Löschen / Recht auf Vergessen- werden	<p>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).</p>
Recht auf Unterrichtung	<p>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.</p>
Rechtmäßigkeit der Verarbeitung	<p>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</p>

	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).