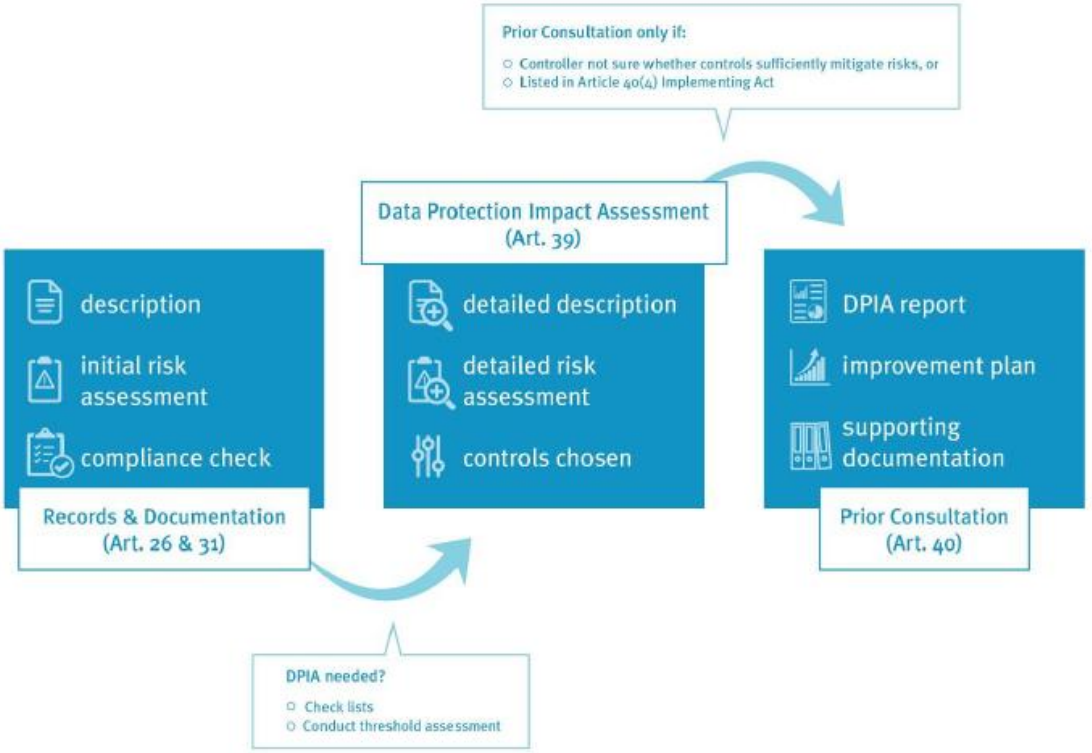
DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE (EDSB)

Rechenschaftspflicht in der Praxis: Leitfaden für Organe, Einrichtungen und Agenturen der Union über die Dokumentierung von Verarbeitungs-vorgängen Zusammenfassung

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
initial risk assessment	Erste Risikobewertung
compliance check	Compliance-Kontrolle
Records & Documentation (Art. 26 &31)	Verzeichnisse und Dokumentierung (Artikel 26 und 31)
detailed description	Ausführliche Beschreibung
detailed risk assessment	Detaillierte 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

1 Rechenschaftspflicht in der Praxis

Wenn wir in den Organen, Einrichtungen und sonstigen Stellen der Union (EU-Institutionen) Informationen über natürliche Personen („personenbezogene Daten“) verarbeiten, müssen wir bestimmte Vorschriften beachten, um die Privatsphäre derjenigen, deren Daten wir verarbeiten, zu schützen. Dies gilt unabhängig davon, ob es sich bei den Personen um unsere eigenen Mitarbeiter, Leistungsempfänger, Auftragnehmer oder andere Personen handelt. Die von den EU-Institutionen einzuhaltenden Regeln sind in der Verordnung (EU) 2018/1725[1] („Verordnung“) niedergelegt.

Kurz gesagt, besagen diese Regeln,

(1) dass es für die Verarbeitung von Daten natürlicher Personen einen guten Grund geben muss;
(2) dass die Personen darüber zu informieren sind;
(3) dass Sie sowohl dafür, *was* Sie tun, als auch dafür, *wozu* Sie es tun, rechenschaftspflichtig sind.

Die Hauptakteure sind diejenigen, die in den EU-Institutionen für die Verarbeitung personenbezogener Daten rechenschaftspflichtig sind (die „Verantwortlichen“). **Sie sind für das, was Sie tun, und für die Art und Weise, in der Sie es tun, rechenschaftspflichtig**. Dies bedeutet: Sie müssen alle Vorschriften einhalten und die Vorschriftseinhaltung auch **nachweisen** können.

Dies gelingt am besten, indem Sie **bei der Gestaltung und Dokumentierung von Verarbeitungsvorgängen einer klar gegliederten Vorgehensweise** folgen. Das wiederum setzt voraus, dass Sie dies schon bedenken, wenn Sie über die Gestaltung neuer Prozesse nachdenken („Grundsatz des eingebauten Datenschutzes“). Das vom Europäischen Datenschutzbeauftragten (EDSB) herausgegebene Toolkit *Rechenschaftspflicht in der Praxis: Leitfaden für Organe, Einrichtungen und Agenturen der Union über die Dokumentierung von Verarbeitungsvorgängen* bietet dazu eine Orientierung, die in dieser Broschüre zusammengefasst ist. Dieser Prozess für die Gestaltung und Dokumentierung von Verarbeitungsvorgängen ist kein Selbstzweck, sondern vielmehr **Mittel zum Zweck**: Er dient dazu, Transparenz, Vorschriftseinhaltung und Rechenschaftspflicht zu erzielen.

Die Verordnung baut auf früheren Regelungen in der 2001 erlassenen Verordnung (EG) Nr. 45/2001[2] (die „alte Verordnung“) auf und spiegelt die Datenschutz-Grundverordnung (EU) 2016/679 [3](DSGVO) wider, die für die meisten[4] Organisationen gilt, die in den Mitgliedstaaten personenbezogene Daten verarbeiten (die „Verantwortlichen“), egal, ob es sich jeweils um die öffentliche Verwaltung, Unternehmen, gemeinnützige Vereine oder sonstige Organisationen handelt. Im Vergleich zu den früheren Vorschriften sind **Ihre Dokumentierungspflichten nach der neuen Verordnung stärker an den jeweiligen Risiken der Verarbeitung personenbezogener Daten ausgerichtet**. Dies bedeutet beispielsweise, dass die Dokumentationsanforderungen für das Abonnieren eines Newsletters von EU-Institutionen niedriger sind als etwa für eine intelligente Videoüberwachung, die den öffentlich zugänglichen Raum überwacht. Die Vorschriften berücksichtigen auch den Status des Datenschutzes als ein durch Artikel 8 der Charta der Grundrechte der Europäischen Union geschütztes Grundrecht.

Im Bereich der Grundrechte müssen die EU-Institutionen mit gutem Beispiel vorangehen, auch beim Datenschutz. Der **Europäische Datenschutzbeauftragte ist die Aufsichtsbehörde, die die Verarbeitung personenbezogener Daten durch die EU-Institutionen überprüft und umfangreiche Leitlinien zu zahlreichen Aspekten der Einhaltung dieser Vorschriften**

[1] ABl. L 295/39 vom 21.11.2018.
[2] ABl. L 8/1 vom 12.1.2001.
[3] ABl. L 119/1 vom 04.05.2016.
[4]Die Verarbeitung zu Strafverfolgungszwecken durch die zuständigen Behörden in den Mitgliedstaaten unterliegt dagegen der nationalen Umsetzung der Richtlinie 2016/680; ABl. L 119/89 vom 4.5.2016.

herausgibt.

Dieses Toolkit, das die besondere Situation der der Aufsicht des Europäischen Datenschutzbeauftragten unterliegenden EU-Institutionen behandelt, steht auch mit den Grundsätzen der DSGVO und den von der Artikel-29-Datenschutzgruppe (WP29) und dem Europäischen Datenschutzausschuss (EDSA) herausgegebenen Leitlinien in Einklang.[5] Wir werden es erforderlichenfalls aktualisieren, um stets mit der Auslegung der DSGVO durch den Europäischen Datenschutzausschuss Schritt zu halten. Insofern könnte das Toolkit auch für Verantwortliche, Datenschutzbeauftragte (DSB) und sonstige Interessenträger außerhalb der EU-Institutionen von Interesse sein. Da die für die EU-Institutionen geltenden Vorschriften denen in der DSGVO gleichwertig sind, sollten sie auch gleich ausgelegt werden. Deshalb nehmen wir zuweilen auch auf die DSGVO Bezug.

Falls Sie mehr darüber wissen möchten, **wenden Sie sich an den Datenschutzbeauftragten Ihrer EU-Institution** und sehen Sie sich das Toolkit an; überall, wo Sie in dieser Broschüre eckige Klammern sehen, sind die entsprechenden Fundstellen für die näheren Informationen im Toolkit angegeben. Weitere Leitlinien zu anderen Themen – etwa darüber, wann und auf welche Weise Sie Personen darüber informieren müssen, dass Sie deren Daten verarbeiten, oder über Datenschutzaspekte bestimmter Geschäftsprozesse (Rekrutierung, Mitarbeiterbeurteilung, Verwaltungsuntersuchungen und Disziplinarverfahren usw.) – finden Sie auf der Website des Europäischen Datenschutzbeauftragten.[6]

2 Zielgruppe, Gegenstand und Verhältnis zu anderen Dokumenten

Die **Zielgruppe für dieses Toolkit sind die Verantwortlichen und die für diese handelnden Mitarbeiter, die Datenschutzbeauftragten (DSB), die Datenschutzkoordinatoren** (DSK)[7] sowie alle anderen, die in EU-Institutionen an der Entwicklung und Verwaltung von Verarbeitungsvorgängen, bei denen personenbezogene Daten verarbeitet werden, mitwirken. 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".[8]

In diesem Toolkit beziehen sich Personalpronomen der 2. Person auf den „Durchführungsverantwortlichen aufseiten des Verantwortlichen" oder auf den für einen bestehenden Verarbeitungsvorgang „in der Praxis Verantwortlichen" (im Geschäftsbereich Zuständigen) oder auf den Projektverantwortlichen für in Entwicklung befindliche Tätigkeiten.

Dieses Toolkit bietet eine Orientierung über die nach der Verordnung einzuhaltenden Anforderungen an die Datenschutzdokumentation und Risikobewertungen für als „riskant" eingestufte Verarbeitungsvorgänge. Es behandelt folgende Aspekte (und enthält für die meisten dieser Aspekte auch Vorlagen):

- wie man die eigenen Verarbeitungstätigkeiten dokumentiert;

[5] Z.B. 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", WP248, abrufbar unter: http://ec.europa.eu/newsroom/document.cfm?doc id=44137

[6] https://edps.europa.eu/data-protection/our-work/our-work-bY-tvpe/guidelines_en

[7] Einige der größeren EU-Institutionen haben in jeder Generaldirektion oder ähnlichen Organisationseinheit Datenschutzkoordinatoren (o. Ä.) als lokale Kontaktstellen.

[8] Artikel 3 Ziffer 8 der Verordnung.

- in welchen Fällen Datenschutz-Folgenabschätzungen (DSFA) erforderlich sind;
- wie man eine Datenschutz-Folgenabschätzung 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;
- die Vorschriften für den Übergang von der alten zur neuen Datenschutzverordnung für die EU-Institutionen.

Dieses Toolkit behandelt *nicht*:

- die Rolle der Datenschutzbeauftragten im Allgemeinen;
- im Detail, wie bei spezifischen Verarbeitungsvorgängen (z. B. bei der Übermittlung personenbezogener Daten in Länder außerhalb der EU) oder bei spezifischen Verfahren (z. B. bei der Mitarbeiterauswahl und -rekrutierung) zu verfahren ist.[9]

Dieses Toolkit gibt Ihnen Aufschluss darüber, was Sie bei Geschäftsprozessen in Ihrer Organisation im Hinblick auf das Datenschutzmanagement und die Risiken für die Privatsphäre bedenken müssen und wie diese Überlegungen zu dokumentieren sind. Spezifische Vorschläge für zu treffende Sicherheitsvorkehrungen finden Sie in den Leitlinien für den betreffenden Verarbeitungsvorgang (z. B. für Verfahren im Rahmen der Personalauswahl usw.).

3 Grundsatz der Rechenschaftspflicht

Rechenschaftspflicht bedeutet, dass der für die Verarbeitung Verantwortliche dafür zuständig ist, sicherzustellen, dass alle Vorschriften eingehalten werden und die Vorschriftseinhaltung auch nachgewiesen werden kann. 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** (bei dem im Geschäftsbereich Zuständigen). Der im Geschäftsbereich Zuständige / Durchführungsverantwortliche aufseiten des Verantwortlichen[10] für den jeweiligen Prozess ist der in erster Linie Zuständige, wobei er jedoch vom Datenschutzbeauftragten und Datenschutzkoordinatoren unterstützt wird (Teil I – Abschnitt 2, Teil II – Abschnitt 2).

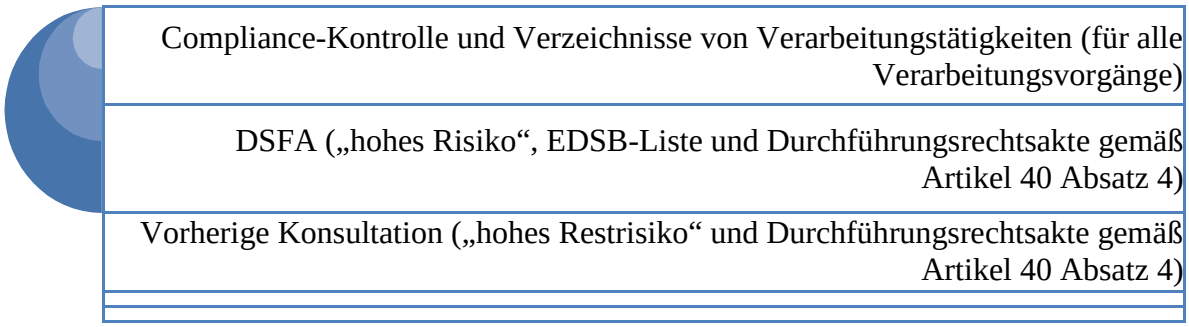
Für die meisten Verarbeitungsvorgänge in Ihrer Organisation wird es genügen, Verzeichnisse zu führen und eine Compliance-Kontrolle vorzunehmen. Eine Datenschutz-Folgenabschätzung wird nur für einige der Verarbeitungsvorgänge erforderlich sein. Nur für wenige dieser Verarbeitungsvorgänge wird zudem eine vorherige Konsultation nötig sein.

Zum Nachweis der Vorschriftseinhaltung ist es erforderlich, zu dokumentieren, **wie Sie die personenbezogenen Daten verarbeiten und warum deren Verarbeitung gerade auf diese Weise erfolgt**. Ihre **Dokumentierungspflichten sind von den Risiken abhängig**, die sich durch die

[9] Für diese besonderen Situationen und auch viele weitere (Verwaltungsuntersuchungen, Disziplinarverfahren, Urlaubsverwaltung und Gleitzeit, Patientendaten usw.) hat der Europäische Datenschutzbeauftragte eingehendere Leitlinien ausgearbeitet, die hier abrufbar sind: httpsy/edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en. Der Europäische Datenschutzbeauftragte wird diese Dokumente zur Anpassung an die neuen Vorschriften aktualisieren.

[10] Es kann vorkommen, dass die im Geschäftsbereich zuständige Person auf Input von anderen angewiesen ist; ein Beispiel dafür wäre etwa der Leiter einer Geschäftseinheit, für den die IT-Abteilung eine Anwendung entwickelt. Doch auch wenn die im Geschäftsbereich zuständige Person viele Informationen bei der IT-Abteilung einholen muss, liegt die Verantwortung für das System insgesamt bei der im Geschäftsbereich zuständigen Person.

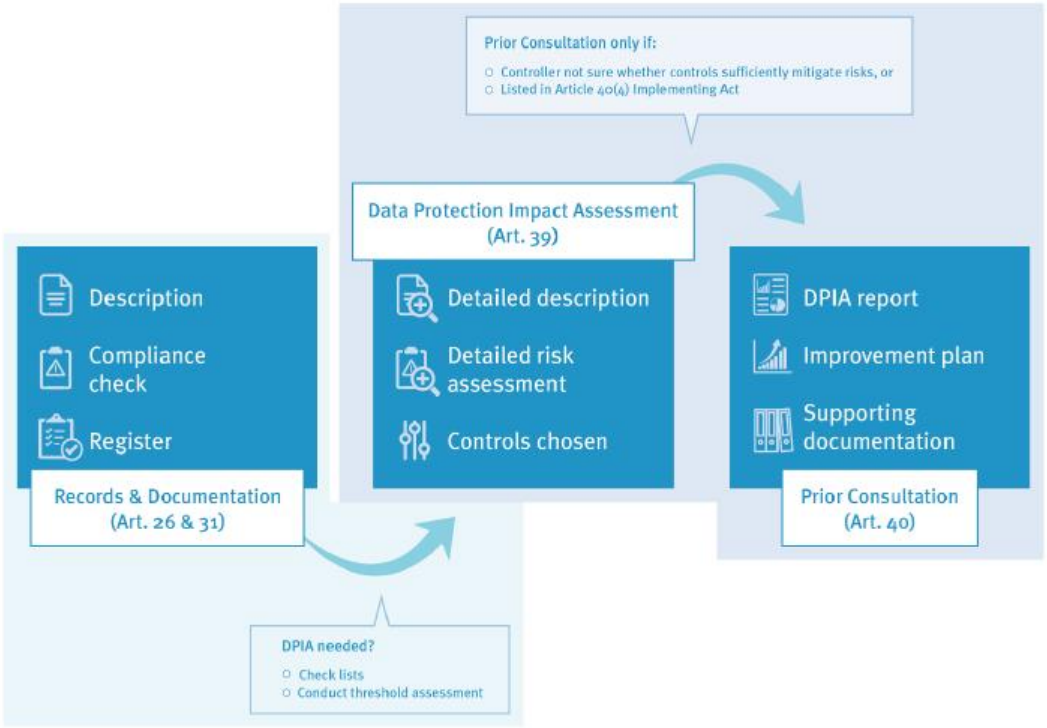
Art der Verarbeitung personenbezogener Daten ergeben. So sind die Dokumentationsanforderungen für das Abonnieren eines Newsletters viel geringer als diejenigen für eine Datenbank für das Profiling von Reisenden zu Risikoscreening-Zwecken. Relevant ist auch, wie Sie den Prozess gestaltet haben: Eine Mitarbeiterbeurteilung, die auf einem einfachen Beurteilungsgespräch mit dem zuständigen Bediensteten beruht, wird weniger Dokumentation erfordern als ein System, bei dem aus dem Fallverwaltungssystem automatisch Vergleichskennzahlen erzeugt werden, die in das Beurteilungsverfahren einfließen.



Je nachdem, um welchen Prozess es jeweils geht, brauchen Sie möglicherweise nicht sämtliche der folgenden Schritte einzuhalten:

- Für sämtliche Prozesse ist eine Grunddokumentation (das sogenannte „Verzeichnis“) zu erstellen; nutzen Sie diese Gelegenheit, eine Compliance-Kontrolle durchzuführen.
- Prüfen Sie, ob der Vorgang wahrscheinlich ein hohes Risiko für die Personen darstellt, deren Daten verarbeitet werden; wenn dies der Fall zu sein scheint, müssen Sie Ihren Datenschutzbeauftragten konsultieren.
- Wenn Sie eine Datenschutz-Folgenabschätzung durchführen müssen, müssen Sie diese Risiken eingehender untersuchen und spezifische Garantien/Kontrollen dagegen entwickeln.
- Wenn die Datenschutz-Folgenabschätzung ergibt, dass trotz allem noch ein hohes Restrisiko im Hinblick auf den Datenschutz besteht, ist der Europäische Datenschutzbeauftragte zu konsultieren.

Die ersten beiden Schritte werden in Teil I des Toolkits behandelt, die letzten beiden in Teil II.



4 Was ist unter Verzeichnissen zu verstehen? [Teil I – Abschnitt 3]

Für alle Ihre Verarbeitungsvorgänge ist eine gewisse Grunddokumentation erforderlich. Diese bezeichnet man als Verzeichnis. In der **Verordnung ist im Einzelnen aufgelistet**, welche Angaben in die Verzeichnisse aufzunehmen sind [Teil I – Abschnitt 3.1]. Wenn Sie ein Verzeichnis erstellen, sollten Sie gleichzeitig **prüfen, ob Ihre Verarbeitung rechtskonform ist**, d. h., ob sie den Vorschriften genügt [Teil I – Abschnitt 3.2]. Vgl. [Teil I – Anhang 1], wo Sie eine Vorlage finden, die Sie hierfür verwenden können. Bei der Verzeichniserstellung können Sie sich auf die in Ihrer EU-Institution bereits vorhandenen Meldungen stützen [Teil I – Abschnitt 5]. Nach Erstellung des Verzeichnisses müssen Sie darauf achten, diese stets auf dem aktuellen Stand zu halten [Teil I – Abschnitt 3.3].

Die Verzeichnisse werden dann in ein **zentrales Register** aufgenommen, das von Ihrer EU-Institution geführt und vom Datenschutzbeauftragten verwaltet wird [Teil I – Abschnitt 3.4]. Der Datenschutzbeauftragte ist als die am besten dafür geeignete Stelle derjenige, der für die Registerführung zuständig ist; für den Inhalt der von Ihnen erstellten Verzeichnisse bleiben jedoch Sie als der im Geschäftsbereich Zuständige verantwortlich. **Bestimmte Informationen im Register müssen öffentlich sein** [Teil I – Abschnitt 3.5].

Dies sind die Anforderungen an die Datenschutzdokumentation, die für die meisten Verarbeitungsvorgänge gelten.

5 Wann ist eine Datenschutz-Folgenabschätzung durchzuführen? [Teil I – Abschnitt 4]

Allerdings sind für einige **als „riskant“ eingestufte Verarbeitungsvorgänge die Anforderungen höher**. Dies gilt **zum Beispiel** für die Verarbeitung **großer Mengen** von **sensiblen personenbezogenen Daten**, etwa Gesundheitsdaten, Daten bezüglich Disziplinarangelegenheiten oder den Einsatz von **Profiling**, um hier nur einige Beispiele zu nennen. Für die Entscheidung, ob eine

Datenschutz-Folgenabschätzung durchzuführen ist, müssen Sie sich zwei Fragen stellen:

- Ist der Verarbeitungsvorgang auf der Liste aufgeführt, die der Europäische Datenschutzbeauftragte gemäß Artikel 39 Absatz 4 der Verordnung herausgibt?
- Ergibt die Schwellenwertanalyse, dass eine Datenschutz-Folgenabschätzung erforderlich ist?

Sollten Sie eine dieser Fragen mit „ja“ beantwortet haben, ist eine Datenschutz-Folgenabschätzung durchzuführen. Der Europäische Datenschutzbeauftragte gibt Ihnen eine **Vorlage** für diese Schwellenwertanalyse an die Hand; außerdem hat er gemäß Artikel 39 Absatz 4 der Verordnung eine Liste der maßgeblichen Kriterien sowie eine Liste einiger üblicherweise als „riskant“ eingestufter Verarbeitungsvorgänge aufgestellt [Teil II – Anhang 5].

6 Wie führt man eine Datenschutz-Folgenabschätzung durch? [Teil II – Abschnitt 3]

Nach der Verordnung ist eine **Datenschutz-Folgenabschätzung erforderlich, wenn ein Verarbeitungsvorgang** für diejenigen, deren Daten Sie verarbeiten, **wahrscheinlich ein „hohes Risiko“ zur Folge hat**.

Der Europäische Datenschutzbeauftragte **schreibt dafür keine bestimmte Methode vor**, sondern **stellt Vorlagen bereit**, die Sie für die Durchführung der Datenschutz-Folgenabschätzung verwenden können [Teil II – Anhang 3]. Wenn Sie diese Vorlagen nicht benutzen möchten, können Sie jede sonstige Methode verwenden, die den Anforderungen der Verordnung genügt [siehe dazu die nicht erschöpfende Liste in Teil II – Anhang 4.1].

In einer Datenschutz-Folgenabschätzung geht es darum, Ihre geplanten Verarbeitungsvorgänge eingehender zu analysieren, um zu sehen, wo die Datenschutzrisiken liegen und wie Sie diesen begegnen können. **Dabei geht es um mehr als nur Informationssicherheits-Risikomanagement**. Die erste Datenschutz-Folgenabschätzung endet mit einem DSFA-Bericht, in dem der betreffende Verarbeitungsvorgang, die festgestellten Risiken und die (implementierten / zu implementierenden) Risikokontrollen erklärt werden. **Eine Datenschutz-Folgenabschätzung ist ein laufender Prozess**, nicht eine einmalige Übung – die DSFA muss laufend aktualisiert werden, und zwar jedes Mal, wenn sich Ihre Verarbeitungsvorgänge erheblich ändern, sowie in regelmäßigen Abständen [Teil II – Abschnitt 3.8].

Es ist **bewährte Praxis, 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 [Teil II – Abschnitt 3.9].

7 Erforderlichkeit der vorherigen Konsultation [Teil II – Abschnitt 4]

In Ihrem DSFA-Bericht können Sie zu drei verschiedenen Ergebnissen gelangen:

(1) dass Sie sich sicher sind, dass die Maßnahmen, die in der DSFA ausgewählt wurden, genügen, die Risiken auf ein annehmbares Niveau zu reduzieren. In diesem Fall implementieren Sie die Maßnahmen und setzen das Projekt fort;
(2) dass Sie zum dem Schluss gelangen, dass die analysierten Kontrollen nicht geeignet sind, die Risiken auf ein annehmbares Niveau zu reduzieren. In diesem Fall müssen Sie das Projekt aufgeben oder neu gestalten, da es sich als unmöglich erwiesen hat, es auf gesetzeskonforme Weise zu implementieren;
(3) dass Sie sich unsicher sind, ob die von Ihnen analysierten Maßnahmen genügen, die Risiken auf ein annehmbares Niveau zu reduzieren.

In diesem dritten Fall ist als nächstes eine „vorherige Konsultation“ des Europäischen Datenschutzbeauftragten erforderlich (Artikel 40 der Verordnung). Außerdem kann die Europäische Kommission **im Wege eines Durchführungsrechtsakts eine Liste der Arten von Verarbeitungsvorgängen festlegen, die stets der vorherigen Konsultation bedürfen**.

Dazu müssen Sie dem Europäischen Datenschutzbeauftragten Ihre Datenschutz-Folgenabschätzung sowie einige andere Informationen übermitteln [Teil II – Abschnitt 4]. Der **Europäische Datenschutzbeauftragte antwortet innerhalb von acht Wochen**; in besonders komplizierten Fällen können wir diese Frist um vier Wochen verlängern. Sollten wir weitere Informationen von Ihnen anfordern, würde diese Frist dadurch jeweils gehemmt. Soweit angemessen, wird der Europäische Datenschutzbeauftragte in seiner Antwort **Empfehlungen zur Verbesserung der Rechtskonformität** geben.

8 Was ist zu tun? [Teil I – Abschnitt 5; Teil II – Abschnitt 5]

Ihre EU-Institution verfügt bereits in gewissem Umfang über eine Datenschutzdokumentation, **Sie brauchen also nicht bei Null anzufangen**. Für die Verzeichniserstellung **können Sie auf die Meldungen an Ihren Datenschutzbeauftragten zurückgreifen, die nach der alten Verordnung** (EG) Nr. 45/2001 erforderlich waren [Teil I – Abschnitt 5]. Wenn Ihre Meldungen auf dem aktuellen Stand sind, dürfte es nicht viel Mühe machen, daraus Verzeichnisse anzufertigen. Was die als „riskant“ eingestuften Verarbeitungsvorgänge angeht, für die Datenschutz-Folgenabschätzungen erforderlich sind, wird für viele bereits nach der alten Verordnung eine „Vorabkontrolle“ durchgeführt worden sein [Teil II – Abschnitt 5].

Darüber hinaus kommen mit der neuen Verordnung **weitere Änderungen** auf Sie zu. Zum Beispiel werden Sie Ihre **Auftragnehmer**[11] genauer im Auge behalten und wahrscheinlich auch Ihre Datenschutzhinweise aktualisieren müssen.[12]

9 Was kann Ihr Datenschutzbeauftragter für Sie tun?

In jeder EU-Institution gibt es mindestens einen Datenschutzbeauftragten (DSB), der als **Anlaufstelle für alle Datenschutzangelegenheiten** dient. Einige größere EU-Institutionen haben außerdem Datenschutzkoordinatoren / Datenschutz-Kontaktstellen (DSK) für die einzelnen Generaldirektionen. Diese können Ihnen bei der Verzeichniserstellung und der Durchführung von Datenschutz-Folgenabschätzungen behilflich sein. Wenn Sie Fragen zum Datenschutz haben, wenden Sie sich bitte an diese Stellen. Allerdings ist zu beachten, dass die Verpflichtung, alle Vorschriften einzuhalten, beim Verantwortlichen liegt.

Die Datenschutzbeauftragten sind also die **Hauptkontaktstelle zwischen den EU-Institutionen und dem Europäischen Datenschutzbeauftragten** – wenn Sie Fragen an den Europäischen Datenschutzbeauftragten haben, übermitteln Sie diese bitte stets über Ihren behördlichen

---

[11] Siehe dazu Consultation concerning certain clauses that a contractor wants to include in service contracts to align with the conditions set forth by Regulation (EU) 2016/679 [Konsultation über gewisse Klauseln, die ein Auftragnehmer zur Anpassung an die Anforderungen der Verordnung (EU) 2016/679 in Dienstleitungsverträge aufnehmen möchte], https://edps.europa.eu/data-protection/our-work/publications/consultations/consultation-concerning-updating-service_en. Musterklauseln, die in derartige Verträge aufgenommen werden können, sind an die Datenschutzbeauftragten verteilt worden.

[12] Europäischer Datenschutzbeauftragter, Guidance Paper, Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations [Leitlinien, Artikel 14-16 der neuen Verordnung (EU) 45/2001: Transparenzrechte und -pflichten], abrufbar unter: https://edps.europa.eu/data-protection/our-work/publications/other-documents/articles-14-16-new-regulation-452001_en.

Datenschutzbeauftragten. Oftmals dürfte dieser bereits in der Lage sein, Ihre Frage zu beantworten.

10 Was kann der Europäische Datenschutzbeauftragte für Sie tun?

Der **Europäische Datenschutzbeauftragte ist die Aufsichtsbehörde für die Verarbeitung personenbezogener Daten durch EU-Institutionen**.
Als solche überwachen und überprüfen wir die Einhaltung der Datenschutzvorschriften – sei es auf Beschwerden hin, in Inspektionen, in Erwiderung auf Konsultationsersuchen von EU-Institutionen oder aus eigener Initiative. Wir geben auf unserer Erfahrung beruhende Leitlinien dazu heraus, wie die Vorschriften eingehalten werden können, und bieten Schulungen, um Ihnen zu helfen, eine Führungsstellung im Datenschutz einzunehmen und bewährte Verfahren zu implementieren.

Abgesehen von seiner Aufsichtsfunktion berät der Europäische Datenschutzbeauftragte **auch den Unionsgesetzgeber** über neue Vorschriften über die Verarbeitung personenbezogener Daten, zum Beispiel über Vorschläge für Rechtsakte, durch die neue EU-Datenbanken eingerichtet werden. Wir stellen auch das **Sekretariat für den Europäischen Datenschutzausschuss**, das Forum für die Zusammenarbeit der europäischen Datenschutzbehörden in grenzübergreifenden Angelegenheiten.