Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2023
www.fedlex.admin.ch
Massgebend ist die signierte elektronische Fassung

Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung

(DSFA-Richtlinien)

vom 28. Juni 2023

Der Schweizerische Bundesrat
erlässt folgende Richtlinien:

1 Allgemeine Bestimmungen

1.1 Gegenstand

Diese Richtlinien regeln die Durchführung der Risikovorprüfung und der Datenschutz-Folgenabschätzung (DSFA) nach den Artikeln 22 und 23 des Datenschutzgesetzes vom 25. September 2020[1] (DSG) durch die Bundesverwaltung und deren Einbettung in das Rechtsetzungsverfahren des Bundes sowie die Koordination mit der Projektmanagementmethode HERMES[2].

1.2 Geltungsbereich

Diese Richtlinien gelten für die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[3].

1.3 Vorgehen

[1] Bei jeder geplanten Bearbeitung von Personendaten prüft die zuständige Verwaltungseinheit in einem ersten Schritt, ob die Bearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person mit sich bringen kann (Risikovorprüfung, Ziff. 2). Sie konsultiert die Datenschutzberaterin oder den Datenschutzberater.

1 SR **235.1**
2 www.hermes.admin.ch
3 SR **172.010.1**

[2] Ergibt sich aus der Risikovorprüfung, dass ein hohes Risiko für die Grundrechte der betroffenen Person besteht, so führt sie in einem zweiten Schritt eine DSFA durch (Ziff. 3). Sie konsultiert die Datenschutzberaterin oder den Datenschutzberater.

[3] Wird ein Rechtsetzungsverfahren durchgeführt, so ist Ziffer 4 anwendbar.

[4] Wird ein Projekt nach HERMES durchgeführt, so ist Ziffer 5 anwendbar.

2 Risikovorprüfung

[1] Die zuständige Verwaltungseinheit führt bei allen geplanten Bearbeitungen von Personendaten die Risikovorprüfung mit dem vom Bundesamt für Justiz (BJ) zur Verfügung gestellten Instrument durch (Instrument für die Risikovorprüfung)[4]. Wird ein Projekt nach HERMES durchgeführt, so kann die Risikovorprüfung auch im Rahmen der Schutzbedarfsanalyse erfolgen (Ziff. 5.1 Abs. 2).

[2] Wenn sich die Risiken ändern oder neue Risiken auftreten, überprüft die zuständige Verwaltungseinheit die Angaben und passt sie nötigenfalls an. Hat sie bereits eine DSFA erstellt, so passt sie diese an (Ziff. 3 Abs. 2); die im Rahmen der Risikovorprüfung gemachten Angaben müssen nicht angepasst werden.

3 DSFA

[1] Die DSFA besteht aus den folgenden Schritten:

a. Beschreibung der geplanten Datenbearbeitung;

b. Bewertung der Risiken für die Grundrechte der betroffenen Person;

c. Identifizierung der Massnahmen zum Schutz der Grundrechte;

d. Bewertung der Auswirkungen der vorgesehenen Massnahmen, um zu beurteilen, ob ein hohes Restrisiko besteht.

[2] Wenn sich die Risiken ändern oder neue Risiken auftreten, überprüft die zuständige Verwaltungseinheit die erstellte DSFA und passt sie nötigenfalls an.

[3] Das Vorgehen bei der Durchführung der DSFA und deren Inhalt richten sich nach dem DSFA-Leitfaden des BJ[5].

4 Koordination mit dem Rechtsetzungsverfahren

4.1 Risikovorprüfung

[1] Ist für die geplante Bearbeitung von Personendaten ein Erlass oder die Änderung eines Erlasses erforderlich, so sind die Risikovorprüfung und allenfalls die DSFA vor der Ämterkonsultation durchzuführen.

4 www.bj.admin.ch > Staat & Bürger > Datenschutz > Informationen für Bundesorgane
5 www.bj.admin.ch > Staat & Bürger > Datenschutz > Informationen für Bundesorgane

2 Das ausgefüllte Instrument für die Risikovorprüfung ist den Unterlagen zur Ämterkonsultation beizulegen, es sei denn, eine DSFA ist notwendig. Wird ein Projekt nach HERMES durchgeführt, so kann auch ein Auszug aus der Schutzbedarfsanalyse beigelegt werden.

3 Müssen die Angaben nach der Ämterkonsultation angepasst werden, so ist das aktualisierte Instrument für die Risikovorprüfung oder der aktualisierte Auszug aus der Schutzbedarfsanalyse den Unterlagen zur nachfolgenden Ämterkonsultation oder zum Mitberichtsverfahren beizulegen, es sei denn, eine DSFA ist notwendig.

4 Das federführende Departement und die Bundeskanzlei informieren insbesondere im Antrag an den Bundesrat, im erläuternden Bericht und in der Botschaft über die Ergebnisse der Risikovorprüfung und äussern sich dazu, ob und allenfalls aus welchen Gründen ein hohes Risiko für die Grundrechte der betroffenen Person besteht.

5 Die Ausführungen im erläuternden Bericht und in der Botschaft sind gemäss den Vorgaben des Botschaftsleitfadens[6] darzustellen.

4.2 DSFA

1 Die Ergebnisse der DSFA sowie im Fall eines hohen Restrisikos nach Artikel 23 DSG[7] die Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sind den Unterlagen zur Ämterkonsultation beizulegen. Die Ergebnisse umfassen insbesondere die festgestellten Risiken, die vorgesehenen Massnahmen sowie die verbleibenden Restrisiken. Wird ein Projekt nach HERMES durchgeführt, so kann auch ein Auszug aus den Instrumenten nach Ziffer 5.2 Absatz 3 beigelegt werden.

2 Ergibt sich die Notwendigkeit zur Durchführung oder Anpassung einer DSFA nach der Ämterkonsultation, so sind die Ergebnisse der DSFA oder ein Auszug aus den Instrumenten nach Ziffer 5.2 Absatz 3 und allenfalls die Stellungnahme des EDÖB den Unterlagen zur nachfolgenden Ämterkonsultation oder zum Mitberichtsverfahren beizulegen.

3 Das federführende Departement und die Bundeskanzlei informieren insbesondere im Antrag an den Bundesrat, im erläuternden Bericht, in der Botschaft und in den Abstimmungserläuterungen über die Ergebnisse der DSFA und allenfalls die Stellungnahme des EDÖB.

4 Die Ausführungen im erläuternden Bericht und in der Botschaft sind gemäss den Vorgaben des Botschaftsleitfadens[8] darzustellen.

6 www.bk.admin.ch > Dokumentation > Sprachen > Hilfsmittel für Textredaktion und Übersetzung
7 SR **235.1**
8 www.bk.admin.ch > Dokumentation > Sprachen > Hilfsmittel für Textredaktion und Übersetzung

5 Koordination mit HERMES

5.1 Risikovorprüfung

[1] Wird ein Projekt nach HERMES durchgeführt, so führt die zuständige Verwaltungseinheit die Risikovorprüfung zur selben Zeit wie die Rechtsgrundlage- und die Schutzbedarfsanalyse durch.

[2] Die Risikovorprüfung wird entweder mit dem Instrument für die Risikovorprüfung oder im Rahmen der Schutzbedarfsanalyse durchgeführt.

5.2 DSFA

[1] Die zuständige Verwaltungseinheit führt die DSFA in der Phase der Lösungsentstehung durch.

[2] Ergibt sich aus der Risikovorprüfung, dass eine DSFA notwendig ist, so liegt ein erhöhter Schutzbedarf im Sinne der Schutzbedarfsanalyse nach den Sicherheitsverfahren der Bundesverwaltung[9] vor.

[3] Die Rechtsgrundlageanalyse und die Instrumente, die bei Vorliegen eines erhöhten Schutzbedarfs erstellt werden[10], bilden Bestandteil der DSFA.

[4] Die zuständige Verwaltungseinheit bewertet in der DSFA zusätzlich die Risiken, die noch nicht mittels der Instrumente nach Absatz 3 bewertet wurden.

[5] Die DSFA wird entweder separat oder zusammen mit den Instrumenten nach Absatz 3 dokumentiert.

6 Inkrafttreten

Diese Richtlinien treten am 1. September 2023 in Kraft.

28 Juni 2023

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

9 www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren > Beurteilung des Schutzbedarfs

10 www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren > Erhöhter Schutz