Kanton Schaffhausen
Datenschutzbeauftragter
Vorstadt 18
CH-8200 Schaffhausen

Merkblatt

Datenschutz-Folgenabschätzung (DSFA)

Das Merkblatt richtet sich an öffentliche Organe, welche i.S.v. Art. 14b DSG[1] eine Bearbeitung von Personendaten[2] vornehmen wollen und dient als Wegleitung zum zugehörigen Formular DSFA.

1 Was ist eine DSFA?

Das DSFA-Verfahren ermöglicht die Erkennung und Bewertung spezifischer Datenschutzrisiken für die Privatsphäre von Betroffenen, welche sich durch die Bearbeitung von Personendaten ergeben. Durch die DSFA kann eine entsprechende Risikoabschätzung vorgenommen werden; sie beschreibt die Gegenmassnahmen um eine Grundrechtsverletzung zu vermeiden.

Die DSFA unterstützt demnach die öffentlichen Organe bei der Erfüllung der Pflicht zum Schutze der Privatsphäre der Betroffenen.

Art. 14b DSG

[1] Beabsichtigt das öffentliche Organ eine Bearbeitung von Personendaten, die voraussichtlich ein erhöhtes Risiko für die Grundrechte der betroffenen Person mit sich bringt, führt es eine Datenschutz-Folgenabschätzung durch.

[2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Grundrechte der betroffenen Person zu vermeiden.

Mittels einer DSFA sollen Risiken identifiziert und bewertet werden, die durch den Einsatz von neuen Verfahren, Technologien und Systemen im Rahmen der Datenbearbeitung entstehen.

2 Wann besteht die Pflicht zur Erstellung einer DSFA?

1 Kantonales Datenschutzgesetz vom 7. März 1994 (DSG; SHR 174.100).
2 Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 2 Abs. 1 lit. a DSG).

a. Allgemein

Die Erstellung einer DSFA ist gesetzlich vorgeschrieben vor der Aufnahme jeder neuen Datenbearbeitung und bei wesentlichen Änderungen bestehender Bearbeitungen, welche voraussichtlich ein *erhöhtes Risiko* für die Grundrechte der Betroffenen *mit sich bringen können*. Während der Planung und Einführung der neuen oder wesentlich geänderten Bearbeitung ist periodisch zu prüfen, ob die Erkennung und Bewertung von Risiken in der DSFA zu ergänzen oder anzupassen ist.

Ein erhöhtes Risiko ergibt sich insbesondere aus

- der Art
- dem Umfang
- den Umständen
- dem Zweck

der Bearbeitung der Personendaten und besonders dann, wenn neue Technologien verwendet werden. Im Zweifelsfall ist eine DSFA durchzuführen.

b. Bei welchen Bearbeitungsvorgängen liegt insbesondere ein erhöhtes Risiko vor?

Gemäss § 6 der DSV[3] liegt ein erhöhtes Risiko und damit die Notwendigkeit einer DSFA insbesondere dann vor, wenn ein Vorhaben

- **die Sammlung einer Vielzahl besonders schützenswerter Personendaten[4] oder ein systematisches Profiling[5] betrifft**;

  Beispiele:

  - Bearbeitung von Daten bzgl. Mitgliedschaften in Organisationen und Vereinen, Informationen über Krankheiten, Behinderungen, spezifische Erbmerkmale, Finger- oder Handabdrücke, charakteristische Gang- oder Sprechart, Vollzug der Arbeitslosenversicherung, administrative Führerausweisentzüge.
  - Zusammenführung und automatisierte Auswertung grösserer Datenmengen, wodurch etwa besondere Vorlieben und Interessen oder Aufenthaltsorte einzelner Personen ermittelt werden können.

- **mit dem Einsatz neuer Technologien verbunden ist**;

  Beispiele:

  - Nutzung von Cloud-Diensten

[3] Kantonale Datenschutzverordnung vom 23. November 2021 (DSV; SHR 174.101).

[4] Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die ethnische Herkunft, Daten über Massnahmen der sozialen Hilfe, Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, genetische Daten und biometrische Daten, Art. 2 Abs. 1 lit. d DSG.

[5] Die automatisierte Auswertung von Daten, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen, Art. 2 Abs. 1 lit. e DSG.

- Fingerabdrucksensoren, Gesichtserkennung

- **eine grosse Anzahl Personen betrifft;**

  Das Gesetz sieht keine absolute Grenze vor; sie ist aber sicher erreicht, wenn mehr als 100 Personen betroffen sind.

- **die systematische und umfangreiche Überwachung öffentlicher Bereiche enthält.**

  Beispiele:

  - Videoüberwachung
  - Bewegungsprofile

c. Welche Bearbeitungsvorgänge können eine DSFA erfordern?

- Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt (Persönlichkeitsprofil).

  Beispiel:

  - Tracking-Verfahren zum Beispiel mittels GPS
  - Sicherheitsprüfungen, Führungszeugnisse

- Zwei oder mehrere öffentliche Organe bearbeiten Personendaten in einem gemeinsamen elektronischen System.

  Beispiel:

  - Einwohnerregister

- Daten besonders schutzbedürftiger Personen oder Personen in einem Abhängigkeitsverhältnis werden bearbeitet (Patientinnen und Patienten, Minderjährige, Arbeitnehmende).

  Beispiel:

  - Schüler*innendaten
  - Patient*innendossier

- Auftragsdatenbearbeitung (Datenbearbeitung durch Dritte).
- Übermittlung von Personendaten in Länder ohne gleichwertiges Datenschutzniveau (Siehe die jeweils aktuelle Staatenliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten im Internet auf https://www.fedlex.admin.ch/eli/cc/2022/568/de#annex_1).
- Abgleichung, Zusammenführung und Verknüpfung von Datensätzen

Beispiel:

○ Umfangreichere, nicht anonymisierte Bearbeitung von Personendaten im statistischen Bereich

d. Welches sind weitere Indizien, die auf ein erhöhtes Risiko hindeuten?

Folgende Indizien weisen auf ein erhöhtes Risiko hin und können eine DSFA erfordern

- Diskriminierung
- Finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten
- Unbefugte Aufhebung der Anonymisierung/Pseudonymisierung
- Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile
- Wenn betroffenen Personen um ihre Rechte oder Freiheiten gebracht werden oder an deren Ausübung gehindert werden.

3 Wer muss eine DSFA erstellen?

Die Pflicht zur Erstellung einer DSFA liegt beim öffentlichen Organ, welches für die Bearbeitung der Personendaten mit erhöhtem Risiko verantwortlich ist.

4 Wie wird eine DSFA erstellt?

Der Datenschutzbeauftragte stellt ein Formular zur Verfügung.

5 Was ist der Inhalt einer DSFA?

a. Projektbeschrieb

Die geplante neue Bearbeitung von Personendaten oder die wesentliche Veränderung der Bearbeitung ist zu beschreiben. Folgendes ist zu nennen:

- Kategorie der bearbeiteten Personendaten (z.B. Namen, Adressdaten, Gesundheitsdaten)
- Bearbeitungsvorgänge (z.B. Datenerhebung, Aufbewahrung, Weitergabe, Löschung)
- Zweck der Bearbeitung (z.B. Personalverwaltung, Bewilligungserteilung)
- Umfang der Bearbeitung (z.B. Anzahl Datensätze, Anzahl betroffene Personen)
- Prozessbeschreibung
- Gesetzliche Grundlage der Datenbearbeitung bzw. Datenbekanntgabe an Dritte

b. Risikoanalyse

Benennung der Risiken für die Grundrechte der betroffenen Personen (informationelle Selbstbestimmung, Privatsphäre), die mit der Bearbeitung der Personendaten verbunden sind. Die Risiken sind ohne die Berücksichtigung von möglichen Abhilfemassnahmen auszuführen (sog. inhärente Risiken).

Solche Risiken sind beispielsweise:

- Verlust von Daten
- Unverhältnismässige Erhebung von Daten
- Einsicht durch Unbefugte
- Fehlerhafte Daten
- Probleme bei der Verfügbarkeit
- Versehentliche Mitteilung an Aussenstehende
- Übermässige Erhebung von Daten
- Unzulässige Verknüpfung von Daten oder Profilbildung
- Übermässig lange Aufbewahrung von Daten.

c. Identifikation von besonderen Risikofaktoren

Darlegung der Faktoren, die die festgestellten Risiken zur erhöhten Gefährdung von Grundrechten der betroffenen Personen herbeiführen können.

Beispiele für Risikofaktoren:

- Automatisierte Einzelentscheidungen
- Systematische Überwachung
- Bearbeitung von besonderen Personendaten
- Personendaten, die in grossem Umfang bearbeitet werden, beispielsweise bei einer hohen Anzahl der Betroffenen oder einer grossen Menge von Daten
- Zusammenführen/ Kombinieren von Personendaten, die durch unterschiedliche Prozesse gewonnen wurden
- Einsatz neuer Technologien oder biometrischer Verfahren
- Zusammenarbeit von mehr als zwei Amtsstellen
- Scoring/Profiling.

d. Risikobewertung

Die Risiken sind nach Schwere des Eingriffs in die Grundrechte mit gering, mittel und schwer und die Eintretenswahrscheinlichkeit mit niedrig, mittel und hoch zu bewerten.

e. Abhilfemassnahmen

Auflistung der Massnahmen zur Bewältigung der Risiken. Es ist darzulegen, welche Massnahmen bereits ergriffen wurden und welche konkret geplant sind.

f. Bewertung Restrisiko

Eine erneute Risikobewertung jedes Risikos, nach Ergreifen aller geplanten Abhilfemassnahmen. Das allenfalls verbleibende Restrisiko ist erneut nach Schwere des Eingriffs in die Grundrechte und Eintretenswahrscheinlichkeit zu bewerten.

g. Notwendigkeit Vorabkonsultation

Eine Vorabkonsultation ist durchzuführen, wenn die DSFA verbleibende **besondere Risikofaktoren** ergibt, welche ein hohes Risiko für die Grundrechte der betroffenen Personen manifestieren. Es ist in der DSFA entsprechend festzuhalten, dass eine Vorabkonsultation durch den Datenschutzbeauftragten erforderlich ist.[6]

Ergibt die DSFA **kein verbleibendes hohes Risiko** für die Grundrechte der betroffenen Personen, muss die DSFA dem Datenschutzbeauftragten nicht eingereicht werden und es muss entsprechend keine Vorabkonsultation durchgeführt werden.[7]

6 Wem muss die DSFA eingereicht werden?

Die DSFA ist aufzubewahren und periodisch zu überprüfen / zu aktualisieren. Sie unterliegt dem Öffentlichkeitsprinzip. Einzureichen ist die DSFA an den Datenschutzbeauftragten zusammen mit allfälligen weiterführenden Dokumenten, wenn eine Vorabkonsultation erforderlich ist.

V 30/06/2023

[6] Art. 14c DSG.
[7] Art. 14c DSG e contrario.