dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Datenschutz-Folgenabschätzung DSFA

1 Einleitung

Das Merkblatt richtet sich an öffentliche Organe. Es dient als Wegleitung zum Formular DSFA. Die Datenschutzbeauftragte steht bei Fragen zur Verfügung.

2 Was ist eine DSFA?

Mit einer DSFA können Datenschutzrisiken erkannt und bewertet werden. Öffentliche Organe sind verpflichtet, Risiken für die Privatsphäre von Betroffenen zu identifizieren und mit geeigneten Massnahmen zu reduzieren. Die DSFA unterstützt sie bei der Erfüllung dieser Pflicht.

Für die DSFA werden in einem Dokument die Risiken der Bearbeitung von Personendaten für die Grundrechte aufgeführt und bewertet. Im Dokument werden Massnahmen definiert, um die Risiken zu reduzieren.

3 Wann besteht die Pflicht zur Erstellung einer DSFA?

– Vor jeder beabsichtigten neuen Bearbeitung von Personendaten ist eine DSFA zu erstellen (zum Beispiel für ein neues Digitalisierungsprojekt).
– Vor einer wesentlichen Änderung der Bearbeitung von Personendaten ist eine DSFA zu erstellen (zum Beispiel, wenn ein neuer Online-Zugriff für eine andere Behörde eingerichtet werden soll).

Während der Planung und Einführung der neuen Datenbearbeitung ist periodisch zu überprüfen, ob die Erkennung und Bewertung von Risiken in der DSFA zu ergänzen oder anzupassen ist und ob die Massnahmen zur Reduktion der Risiken noch angemessen sind.

4 Wer muss eine DSFA erstellen?

Die Pflicht zur Erstellung einer DSFA liegt beim öffentlichen Organ, das für die beabsichtigte neue oder wesentlich veränderte Bearbeitung verantwortlich ist. Die DSFA wird von geschultem Personal (juristisch, organisatorisch-technisch) erstellt.

5 Wie wird eine DSFA erstellt?

Die Datenschutzbeauftragte stellt auf ihrer Website ein Formular für die DSFA zu Verfügung.

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch

6 Was ist der Inhalt einer DSFA?

Beschreibung der beabsichtigten Bearbeitung von Personendaten
Die beabsichtigte neue Bearbeitung von Personendaten oder die wesentliche Veränderung der Bearbeitung ist zu beschreiben. Zu nennen sind:
- die Kategorien der bearbeiteten Personendaten (Namen, Adressdaten, Gesundheitsdaten etc.)
- Bearbeitungsvorgänge (Erhebung, Weitergabe, Analyse, Kombination, Aufbewahrung, Löschung etc.)
- Zweck der Bearbeitung (Personalverwaltung, Bewilligungserteilung etc.)
- Umfang der Bearbeitung (Anzahl Datensätze, Anzahl betroffene Personen, Sensitivität der Informationen über eine Person etc.)

Analyse der Risiken
Die Risiken für die Grundrechte der betroffenen Personen (informationelle Selbstbestimmung, Privatsphäre), die mit der beabsichtigten neuen Bearbeitung verbunden sind, sind zu benennen. Beispiele für Risiken sind:
- fehlerhafte Personendaten
- intransparente Bearbeitung von Personendaten
- übermässige Erhebung von Personendaten (mehr als für den Bearbeitungszweck notwendig)
- Verwendung der Personendaten für nicht vorgesehene Zwecke
- unzulässige Verknüpfung von Personendaten oder Profilbildung
- übermässig lange Aufbewahrung von Personendaten
- unerlaubte Bekanntgabe von Personendaten (andere Behörden, Aussenstehende etc.)
- Einsicht durch Unbefugte (innerhalb und ausserhalb der Amtsstelle)
- Verlust von Personendaten
- Doppelte Datenhaltung

Identifikation von besonderen Risikofaktoren
Die Faktoren sind zu identifizieren, durch die festgestellte Risiken zu einer hohen Gefährdung von Grundrechten betroffener Personen führen können. Beispiele für Risikofaktoren sind:
- 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 drei Amtsstellen
- Scoring/Profiling
- Online-Zugriffe/Abrufverfahren

Risikobewertung
Die Risiken sind nach Schwere des Eingriffs in die Grundrechte und Wahrscheinlichkeit ihres Eintretens zu bewerten, zum Beispiel mit niedrig, mittel, schwer, beziehungsweise niedrig, mittel, hoch.

Massnahmen zur Reduktion der Risiken
Die Massnahmen zur Reduktion der Risiken, die bereits ergriffen wurden oder geplant sind, sind zu erwähnen. Dabei ist zu beschreiben, wie die Massnahmen das spezifische Risiko zu reduzieren vermögen.

Zu den Massnahmen zur Reduktion von Datenschutzrisiken gehören organisatorische als auch technische Möglichkeiten (*privacy by design*).

Entscheid über Vorabkontrolle
Wenn besondere Risikofaktoren vorliegen, ist in der DSFA festzuhalten, dass eine Vorabkontrolle durch die Datenschutzbeauftragte erforderlich ist. Wenn zweifelhaft ist, ob eine Vorabkontrolle erforderlich ist, berät die Datenschutzbeauftragte das öffentliche Organ bei der Entscheidung.

7 Wem muss die DSFA eingereicht werden?

Die DSFA ist aufzubewahren und periodisch zu überprüfen und gegebenenfalls zu aktualisieren.

Die DSFA ist der Datenschutzbeauftragten zusammen mit weiteren Dokumenten einzureichen, wenn eine Vorabkontrolle erforderlich ist. Siehe Merkblatt Vorabkontrolle.

8 Wann folgt auf eine DSFA eine Vorabkontrolle?

Werden in der DSFA besondere Risiken für die Grundrechte betroffener Personen identifiziert, ist die beabsichtigte neue Bearbeitung oder die wesentliche Änderung einer Datenbearbeitung der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten.

Weitere Informationen im Merkblatt Vorabkontrolle.

9 Was ist die Gesetzesgrundlage für die DSFA?

– § 10 IDG (Gesetz über die Information und den Datenschutz, LS 170c.4)
– § 24 IDV (Verordnung über die Information und den Datenschutz, LS 170.c41)

V 2.0 / Oktober 2023