dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Vorabkontrolle

1 Einleitung

Öffentliche Organe des Kantons Zürich müssen der Datenschutzbeauftragten Projekte und Vorhaben zur Vorabkontrolle vorlegen, wenn sie Datenbearbeitungen beinhalten, die für die betroffenen Personen mit besonderen Risiken für ihre Grundrechte verbunden sind.

Mit der Vorabkontrolle wird die datenschutzkonforme Bearbeitung von Personendaten sichergestellt. Durch eine frühzeitige Prüfung können die erforderlichen Massnahmen eingeleitet werden. Verantwortlich für die Meldung an die Datenschutzbeauftragte ist das Organ, welches das Projekt oder Vorhaben durchführen möchte.

2 Betroffene Datenbearbeitungen

Der Vorabkontrolle durch die Datenschutzbeauftragte unterliegen Vorhaben, wenn sie eine Bearbeitung von Personendaten beinhalten, die mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden sind.
Die besonderen Risiken werden mit dem Formular Datenschutz-Folgenabschätzung identifiziert. Die Ausnahmen von der Pflicht zur Vorabkontrolle sind in Ziffer 4 beschrieben.

Einige besondere Risiken sind in § 24 IDV aufgezählt:
- das Abrufverfahren
- die Sammlung einer Vielzahl besonderer Personendaten
- der Einsatz neuer Technologien
- die gemeinsame Bearbeitung von Personendaten durch mindestens drei verschiedene öffentliche Organe
- eine grosse Anzahl von betroffenen Personen

Weitere besondere Risiken sind:
- automatisierte Einzelentscheidungen
- systematische Überwachung
- Zusammenführen beziehungsweise kombinieren von Personendaten, die durch unterschiedliche Prozesse gewonnen wurden
- Scoring oder Profiling

Beispiele von Vorhaben mit besonderen Risiken sind:
- Einrichten von Online-Zugriffen
- Vernetzen verschiedener Datenbanken
- Zusammenstellen und bearbeiten von Persönlichkeitsprofilen

- Automatisiertes Auswerten zur Analyse wesentlicher persönlichen Merkmale oder Vorhersage persönlicher Entwicklungen
- Verwenden biometrischer Daten
- Verwenden von Gesichtserkennungstechnologie
- Verwenden von Radio Frequency Identification (RFID)
- Verwenden von maschinellem Lernen beziehungsweise künstlicher Intelligenz

3 Ausnahmen

Die Datenschutzbeauftragte kann auf eine Vorabkontrolle verzichten, wenn
- sie im Vorhaben bereits mitgewirkt hat oder mitwirkt, oder
- die beabsichtigte Datenbearbeitung keinen grossen Eingriff in die Grundrechte bewirkt.

Die Datenschutzbeauftragte entscheidet gestützt auf die individuellen Faktoren der beabsichtigten Bearbeitung von Personendaten, ob eine Ausnahme vorliegt.

Die Pflicht zur Vorabkontrolle entfällt immer, wenn in der gesetzlichen Bestimmung, welche die Grundlage für die Datenbearbeitung bildet, die Art der Bearbeitung festgelegt und Schutzmassnahmen vorgesehen sind (§ 24 Abs. 5 IDV).

4 Zeitpunkt

Die Datenschutzbeauftragte ist frühzeitig über eine beabsichtigte Bearbeitung von Personendaten zu informieren oder in ein solches Vorhaben einzubeziehen. Die Vorabkontrolle findet in der Konzeptphase statt. Die Datenschutzbeauftragte vereinbart mit dem öffentlichen Organ den passenden Zeitpunkt. Die Datenschutzbeauftragte sollte schon in der Initialisierungsphase über die bevorstehende Vorabkontrolle informiert werden. Auf jeden Fall müssen grundlegende Informationen zum Projekt vorhanden sein (siehe Ziffer 6 «Einzureichende Unterlagen»).

5 Einzureichende Unterlagen

Für die Vorabkontrolle sind der Datenschutzbeauftragten folgende Unterlagen einzureichen:
1. Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) (nach Hermes)
2. Datenschutz-Folgenabschätzung (DSFA) gemäss Formular der Datenschutzbeauftragten mit einer detaillierten Beschreibung der Bearbeitung von Personendaten
3. Rechtsgrundlagenanalyse

Das ISDS-Konzept enthält unter anderem eine Beschreibung der organisatorischen und technischen Aspekte:
- Übersicht der Anwendungen, Systeme und Netzwerke
- Eingesetzte Technologie
- Sicherheitsstufe gemäss der Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)
- Sicherheitsstrategie, Risikoanalyse, Sicherheitskonzept und -massnahmen
- Rollen- und Berechtigungskonzept
- Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen
- Ausserbetriebnahme / Liquidation
- Notfallkonzept / -planung
- je nach Projekt weitere Detailkonzepte und Massnahmenpläne

Die DSFA enthält unter anderem eine Beschreibung des Projekts oder Vorhabens mit folgenden Angaben:
- die für das Projekt verantwortliche Stelle
- Art der Daten (Datenkategorien)

- Art der Datenbearbeitung (Bearbeitungsvorgänge einschliesslich Erhebung der Daten, weitere Bearbeitung der Daten, Datenbekanntgaben und Aufbewahrung)
- Zweck der Datenbearbeitung
- Umfang der Datenbearbeitung (Anzahl Datensätze, Kreis der betroffenen Personen)
- Risiken und Risikofaktoren der Datenbearbeitung für die Grundrechte
- Bewertung der Risiken
- Geplante organisatorische und technische Massnahmen zur Reduktion der Risiken

Die Rechtsgrundlagenanalyse stellt die Rechtslage dar. Sie verweist auf die Bestimmung mit der gesetzlich umschriebenen Aufgabe, auf die sich die Bearbeitung der Personendaten abstützt (§ 8 Abs. 1 IDG). Werden besondere Personendaten bearbeitet, verweist sie auf die hinreichend bestimmte Regelung im formellen Gesetz, welche die Bearbeitung erlaubt (§ 8 Abs. 2 IDG). Wenn Personendaten bekanntgegeben werden (Zugänglichmachen an andere Stellen durch Einsichtgewähren, Weitergeben oder Veröffentlichen), dann verweist sie auf die rechtliche Bestimmung, die dazu ermächtigt (§ 16 IDG). Werden besondere Personendaten bekanntgegeben, verweist sie auf die hinreichend bestimmte Regelung im formellen Gesetz, die dazu ermächtigt (§ 17 IDG). Fehlen die Rechtsgrundlagen, beschreibt die Rechtsgrundlagenanalyse die zu schaffenden Bestimmungen und zeigt den Zeitplan des Rechtsetzungsprojekts auf. Involviert das Projekt oder das Vorhaben eine Auslagerung (§ 6 IDG), ist die Einhaltung der Geheimhaltungspflichten zu dokumentieren, der Entwurf der Auftragsdatenbearbeitungsvereinbarung beizulegen und die Rechtslage bei einem allfälligen Auslandbezug zu erläutern (zum Beispiel bei grenzüberschreitenden Datenübermittlungen oder bei Anwendbarkeit des US CLOUD Act).

6 Inhalt der Vorabkontrolle

Die Datenschutzbeauftragte prüft die rechtlichen, organisatorischen und technischen Rahmenbedingungen der beabsichtigten Datenbearbeitung. Das Resultat der Vorabkontrolle wird in einem Dokument festgehalten und dem öffentlichen Organ innert angemessener Frist zugestellt.

7 Rechtsgrundlagen

- § 10 IDG (Gesetz über die Information und den Datenschutz, LS 170.4)
- § 24 IDV (Verordnung über die Information und den Datenschutz, LS 170.41)

V 3.0 / Oktober 2023