Checkliste und Prüfschema für eine
Risikovorprüfung
nach den Vorgaben des Schweizer Bundesgesetzes über den Datenschutz (Datenschutzgesetz – DSG)

**Erläuterungen zu dieser Vorlage**

Die Vorlage ist nicht abschliessend und umfasst unter Umständen nicht alle erforderlichen Elemente. Zudem können in der Vorlage Elemente enthalten sein, die auf einzelne Unternehmen nicht zutreffen. Es ist daher stets eine entsprechende Anpassung und Ergänzung der Vorlage durch den jeweiligen Verantwortlichen erforderlich. Hinweise dazu finden Sie ggfs. in den Kommentaren.

**Nutzungshinweise für unser kostenloses Template**

Diese Vorlage wird von den Spezialisten von activeMind.ch erstellt und regelmässig aktualisiert. Das Template kann nicht auf alle denkbaren Spezialfälle eingehen. Eine datenschutzrechtliche oder sonstige anwaltliche Beratung kann und soll es nicht ersetzen.

Jegliche Haftung ist ausgeschlossen!

Alle Rechte an der Vorlage bleiben vorbehalten. Der Einsatz des von uns zur Verfügung gestellten Textes ist Ihnen zu eigenen (auch kommerziellen) Zwecken erlaubt und frei möglich.

Wir bieten für diesen kostenfreien Dienst weder Support noch Beratung an und bitten höflich, von entsprechenden Anfragen abzusehen.

Wenn Sie die Vorlage oder Teile davon veröffentlichen, sind der Hinweis und der Link auf htttps://www.activemind.ch auf jeden Fall im Text zu belassen.

# Checkliste Risikovorprüfung nach Art. 22 DSG

## Ziel der Risikovorprüfung

Die Risikovorprüfung dient dazu, potenzielle Risiken der Datenverarbeitung zu identifizieren und zu bewerten, um festzustellen, ob eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 22 DSG erforderlich ist.

Diese Anleitung ermöglicht es, eine strukturierte und umfassende Risikovorprüfung gemäss den Anforderungen des Schweizer Datenschutzgesetzes (DSG) durchzuführen.

## Vorbereitung

Dokumente und Informationen sammeln:

* Erstellen Sie eine Liste der relevanten Dokumente wie Bearbeitungsverzeichnisse, Datenschutzerklärungen, Datenflussdiagramme und Verträge mit Dienstleistern.
* Beschreiben Sie ausführlich die geplante Datenbearbeitung.
* Überprüfen Sie die technischen und organisatorischen Massnahmen, die in den verarbeiteten Dokumenten beschrieben sind.

Prüfinstrumente

* Verwenden Sie das vom Bundesamt für Justiz entwickelte [Instrument für die Risikovorprüfung](https://www.bj.admin.ch/dam/bj/de/data/staat/datenschutz/instrument-risikovorpruefung.xlsx.download.xlsx/instrument-risikovorpruefung-d.xlsx) oder ein äquivalentes System.

## Schritte der Risikovorprüfung

### Schritt 1: Prüfung auf absolute Risikofaktoren (Art. 22 Abs. 2 DSG)

Nutzen Sie zum Beispiel die Risikobewertung [Instrument für die Risikovorprüfung](https://www.bj.admin.ch/dam/bj/de/data/staat/datenschutz/instrument-risikovorpruefung.xlsx.download.xlsx/instrument-risikovorpruefung-d.xlsx), um die Kriterien für absolute Risikofaktoren wie Datenmengen oder besondere Datenkategorien (z. B. Gesundheitsdaten) zu analysieren:

* Kategorien von Daten: Analysieren Sie, welche Datenkategorien (z. B. Kontaktdaten, Gesundheitsdaten) betroffen sind.
* Umfang der Verarbeitung: Untersuchen Sie die Menge der betroffenen Personen und Daten sowie den geografischen Umfang der Verarbeitung.
* Schlussfolgerung: Dokumentieren Sie, ob ein absoluter Risikofaktor vorliegt.

### Schritt 2: Prüfung auf notorische Risikofaktoren

Identifizieren Sie mögliche notorische Risikofaktoren, wie den Einsatz neuer Technologien oder potenzielle Profilingrisiken:

* Datenverarbeitungszwecke: Beschreiben Sie die spezifischen Zwecke der Datenverarbeitung.
* Technologien: Bewerten Sie den Einsatz neuer oder risikoreicher Technologien.
* Transparenz: Prüfen Sie, ob Betroffene ausreichend informiert sind und die Verarbeitung nachvollziehbar bleibt.
* Schlussfolgerung: Entscheiden Sie, ob ein notorischer Risikofaktor vorliegt.

### Schritt 3: Individuelle Risikoermittlung

Wenn die ersten beiden Schritte kein eindeutiges Ergebnis liefern, sollten Sie beurteilen ob Risiken für Vertraulichkeit, Integrität oder Verfügbarkeit vorliegen. Ergänzen Sie die Bewertung mit Wahrscheinlichkeiten und potenziellen Schadensauswirkungen.

* Vertraulichkeit: Analysieren Sie mögliche Gefährdungen der Datenvertraulichkeit (z. B. unzureichender Schutz vor Hacking).
* Integrität: Prüfen Sie Risiken für die Datenintegrität (z. B. unbeabsichtigte Änderungen).
* Verfügbarkeit: Bewerten Sie die Risiken hinsichtlich Datenverfügbarkeit (z. B. Datenverluste).
* Schlussfolgerung: Bestimmen Sie, ob ein hohes Risiko vorliegt.

## Ergebnisbewertung

Nutzen Sie die Zusammenfassung der Risikobewertung, um eine Gesamteinschätzung vorzunehmen. Entscheiden Sie, ob eine Datenschutz-Folgenabschätzung erforderlich ist, und dokumentieren Sie dies im entsprechenden Abschnitt der Tabelle.

## Massnahmenkatalog

Sollten Risiken identifiziert werden, definieren Sie Massnahmen zur Risikominderung:

* Technische Massnahmen: Implementierung von Verschlüsselung, Zugriffskontrollen oder Authentifizierungsmechanismen.
* Organisatorische Massnahmen: Schulungen für Mitarbeiter, Anpassung von Prozessen.
* Kommunikationsmassnahmen: Aktualisierung und Bereitstellung einer verständlichen Datenschutzerklärung.

## Dokumentation

* Halten Sie alle Schritte, Ergebnisse und Entscheidungen schriftlich fest.
* Dokumentieren Sie, welche Massnahmen umgesetzt wurden, um Risiken zu minimieren.

# Ablaufschema zur Vorprüfung für eine DSFA

|  |  |  |
| --- | --- | --- |
| **Schritt 1: Vorliegen eines absoluten Risikofaktors gem. Art. 22 Abs. 2 DSG?**1. Umfangreiche Bearbeitung besonders schützenswerter Personendaten
2. Systematische und umfangreiche Überwachung öffentlicher Bereiche
 | Ja | Durchführung einer DSFA |
| Nein |  |
| **Schritt 2: Vorliegen eines oder mehrerer notorischer Risikofaktoren, die zu einem hohen Risiko nach Art. 22 Abs. 1 DSG führen können?**Beispiele: 1. Liegt ein Profiling mit hohem Risiko vor?
2. Wird eine automatisierte Entscheidung vorgenommen?
3. Werden neue Technologien eingesetzt? Kommt künstliche Intelligenz zum Einsatz?
4. Werden Personendaten ohne das Wissen der betroffenen Person beschafft?
5. Werden Personendaten zu Überwachungszwecken verwendet?
6. Werden Personendaten zusammengeführt oder abgeglichen, die in Datenbank zu unterschiedlichen Zwecken oder von verschiedenen Verantwortlichen bearbeitet werden?
7. Sollen Personendaten an Dritte bekanntgegeben werden?
8. Ist beabsichtigt Personendaten zu Überwachungszwecken zu verwenden?
 | Ja | Durchführung einer DSFA |
| Nein |  |
| **Schritt 3: Vorliegen weiterer Faktoren, die nach den gesamten Umständen zu einem hohen Risiko nach Art. 22 Abs. 1 DSG führen können?**Beispiel: Subkoordinationsverhältnis? | Ja | Durchführung einer DSFA |
| Nein |  |
| Voraussichtlich keine DSFA nötig  |  |

**nein**

**Durchführung
einer DSFA**

**Ja**

**Schritt 3: Vorliegen weiterer Faktoren, die nach den gesamten Umständen zu einem hohen Risiko nach Art. 22 Abs. 1 DSG führen können?**

Beispiel: Subkoordinationsverhältnis?

**nein**

**Durchführung
einer DSFA**

**Ja**