## Mustervorlage für die Durchführung einer Datenschutz-Folgenabschätzung (DSFA)

basierend auf einer Vorlage der britischen Datenschutz-Aufsichtsbehörde ICO (Information Commissioner's Office)

Diese Vorlage ist ein Beispiel, wie Sie Ihren DSFA-Prozess und das Ergebnis durchführen und dokumentieren können. Die Fragen in der Vorlage folgen dem in den DSFA-Leitlinien auf der Internetseite der Datenschutzstelle dargelegten Prozess (<https://www.datenschutzstelle.li/datenschutz/themen-z/datenschutz-folgenabschaetzung>) und sollten zusammen mit diesen Leitlinien und den DSFA-Leitlinien des Europäischen Datenschutzausschusses (<https://www.datenschutzstelle.li/application/files/7915/3623/3270/wp248_rev.01_de.pdf>) gelesen werden.

# Angaben zum Verantwortlichen

|  |  |
| --- | --- |
| Name und Kontaktdaten des Verantwortlichen |  |
| Name und Kontaktdaten des Datenschutzbeauftragten (wenn bestellt) |  |

# Schritt 1: Beschreibung der Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung

|  |
| --- |
| Erläutern Sie ausführlich das angestrebte Projekt und die Art der damit verbundenen Verarbeitung personenbezogener Daten. Sie können dabei auch auf andere Dokumente verweisen oder diese als Link aufnehmen, z.B. eine Projektbeschreibung. Fassen Sie im Anschluss zusammen, warum Sie die Notwendigkeit einer DSFA festgestellt haben. Z.B. weil Sie davon ausgehen, dass die betroffenen Datenverarbeitungsvorgänge Art. 35 Abs. 1 oder 3 DSGVO entsprechen oder in der [Liste der Datenschutzstelle](https://www.datenschutzstelle.li/application/files/3615/5653/8732/Liste_der_Verarbeitungstaetigkeiten_gemaess_Art._35_Abs._4_DSG.pdf) gemäss Art. 35 Abs. 4 DSGVO wiederzufinden sind.  |
|  |

# Schritt 2: Beschreiben Sie die involvierte Datenverarbeitung

|  |
| --- |
| **Beschreiben Sie die geplante Verarbeitung personenbezogener Daten, welche für die Durchführung des Projekts erforderlich ist:** * Wie werden Daten erhoben, verarbeitet bzw. verwendet, gespeichert und gelöscht?
* Woher stammen die Daten?
* Werden die Daten mit jemandem geteilt? Möglicherweise ist es hilfreich, auf ein Flussdiagramm oder eine andere Art der Beschreibung von Datenflüssen zu verweisen.
* Welche Arten der Verarbeitung, bei denen ein hohes Risiko für die Betroffenen zu erwarten ist, sind konkret betroffen?
 |
|  |

|  |
| --- |
| **Beschreiben Sie den Umfang der Verarbeitung:** * Welche Kategorien von personenbezogenen Daten sind betroffen?
* Werden auch besondere Kategorien von personenbezogenen Daten gemäss Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäss Art. 10 DSGVO verarbeitet?
* Beschreiben Sie den Umfang der zu verarbeitenden Daten.
* In welcher Regelmässigkeit findet die Verarbeitung statt?
* Wie lange werden die Daten gespeichert?
* Wie viele Personen sind betroffen?
* Welches geografische Gebiet ist von der Datenverarbeitung betroffen?
 |
|  |

|  |
| --- |
| **Beschreiben Sie den Kontext der Datenverarbeitung:** * In welcher Beziehung stehen Sie als Verantwortliche(r) zu den betroffenen Personen (z.B. Patienten, Kunden, Mitarbeitende, etc.)?
* Sind die betroffenen Personen informiert über die Verarbeitung ihrer Daten?
* Sind personenbezogene Daten von Kindern oder anderen schutzbedürftigen Personen betroffen?
* Gibt es Bedenken oder Sicherheitslücken hinsichtlich dieser Art der Verarbeitung?
* Handelt es sich bei der Verarbeitung um ein neuartiges Verfahren?
* Wird der aktuelle Stand der Technik in diesem Bereich berücksichtigt?
* Gibt es aktuelle Geschehnisse oder eine besondere Sensibilität in der Öffentlichkeit, die Sie berücksichtigen sollten?
* Unterliegt Ihre Institution einem genehmigten Verhaltenskodex oder einer Zertifizierung gemäss Art. 40 DSGVO?
 |
|  |

|  |
| --- |
| **Beschreiben Sie die Zwecke der Verarbeitung:** * Was möchten Sie mit der Verarbeitung erreichen?
* Welche Auswirkung hat die Verarbeitung auf betroffene Personen?
* Was sind die Vorteile der Verarbeitung - für Sie als Verantwortliche/r, die betroffenen Personen und/oder die Allgemeinheit?
 |
|  |

# Schritt 3: Konsultationsprozess

|  |
| --- |
| **Konsultation mit den betroffenen Personen oder weiteren direkt oder indirekt involvierten Stellen:*** Beschreiben Sie, wann und wie Sie Stellungnahmen oder Ansichten von Einzelpersonen oder Institutionen einholen?
* Wenn Sie auf diese Konsultation verzichten, begründen Sie warum dies im vorliegenden Prozess keine Rolle spielt.
* Wen beziehen Sie sonst noch in die Organisation Ihrer Verarbeitungsprozesse ein?
* Beziehen Sie Ihre Auftragsverarbeiter ein und wenn ja, in welcher Form?
* Planen Sie, Informationssicherheitsexperten oder andere Experten zu konsultieren?
 |
|  |

# Schritt 4: Bewerten Sie die Erforderlichkeit und Verhältnsimässigkeit

|  |
| --- |
| **Beschreiben Sie die Massnahmen zur Einhaltung der Datenschutzbestimmungen sowie zur Verhältnismässigkeit der Datenverarbeitung, insbesondere:** * Auf welcher rechtlichen Grundlage beruht die Verarbeitung der personenbezogenen Daten?
* Erreicht die Datenverarbeitung tatsächlich Ihren Zweck?
* Werden ausschliesslich Daten verarbeitet, die erforderlich sind zur Erreichung des angestrebten Zweckes?
* Gäbe es einen anderen Weg/Alternative, um das gleiche Ergebnis (=angestrebten Zweck) zu erzielen?
* Mit welchen Massnahmen stellen Sie die Datenminimierung sicher?
* Mit welchen Massnahmen stellen Sie die Datenqualität sicher?
* Welche Informationen geben Sie den betroffenen Personen zur Verarbeitung ihrer Daten?
* Welche Massnahmen treffen Sie, um die Rechte der betroffenen Personen zu gewährleisten?
* Welche Massnahmen ergreifen Sie, um sicherzustellen, dass die Auftragsverarbeiter die Vorschriften einhalten?
* Wie sichern Sie internationale Datentransfers in einen Drittstaat ab?
 |
|  |

# Schritt 5: Identifizierung und Einschätzung der Risiken

|  |  |  |  |
| --- | --- | --- | --- |
| **Beschreiben Sie die Risikoquelle und die möglichen Auswirkungen auf Individuen.**  | **Wahrschein-lichkeit eines Schadens-eintritts** | **Schwere des möglichen Schadens** | **Insgesamte Risikoein-schätzung**  |
|  | gering, möglich oder wahr-scheinlich | Minimal, bedeutend oder schwer-wiegend | Gering, mittel oder hoch |

# Schritt 6: Identifizierung der Massnahmen zur Risikominimierung

|  |
| --- |
| **Identifizieren Sie zusätzliche Massnahmen, welche einer Reduktion oder Eliminierung eines Risikos dienen könnten, welches Sie in Schritt 5 mit mittel oder hoch eingestuft haben.**  |
| **Risiko**  | **Optionen zur Reduzierung oder Eliminierung des Risikos** | **Auswirkung auf das Risiko**  | **Restrisiko** | **umgesetzte Massnahme** |
|  |  | eliminiert,reduziert,gleichbleibend | niedrig,mittel,hoch | ja/nein |

# Schritt 7: Abschluss und Ergebnis

|  |  |  |
| --- | --- | --- |
| **Gegenstand**  | **Name/Position/date** | **Anmerkungen** |
| Massnahmen genehmigt von: |  | Integrieren Sie die Massnahmen in den Projektplan, legen Sie ein Datum und die Verantwortung für die Umsetzung fest |
| Restrisiko genehmigt von: |  | Wenn ein Restrisiko verbleibt, kontaktieren Sie die Datenschutzstelle zur Konsultation für das weitere Vorgehen |
| Stellungnahme des Datenschutzbeauftragten wurde eingeholt: |  | Der Datenschutzbeauftragte sollte in Bezug auf die Einhaltung der Bestimmungen, Massnahmen in Schritt 6 und die Frage, ob die Verarbeitung fortgesetzt werden kann, angehört werden |
| Zusammenfassung der Stellungnahme des Datenschutzbeauftragten: |
| Die Stellungnahme des Datenschutzbeauftragten wurde berücksichtigt/nicht berücksichtigt: |  | Wenn die Stellungnahme nicht berücksichtigt wurde, führen Sie bitte die Gründe an: |
| Anmerkungen: |
| Die Antworten aus dem Konsultationsprozess wurden analysiert von:  |  | Wenn die Entscheidung von den Rückmeldungen abweicht, bitte führen Sie hier die Gründe an:  |
| Anmerkungen: |
| Die DSFA wird fortlaufend überprüft von: |  | Der Datenschutzbeauftragte sollte ebenfalls in die Überprüfung der fortlaufenden Compliance mit der DSFA eingebunden werden.  |