Hinweise zur Risikoanalyse

Zur Festlegung der zu treffenden technischen und organisatorischen Datenschutzmaßnahmen verfolgt die EU-DSGVO in Art. 32 einen risikobasierten Ansatz: Die Festlegung der technischen und organisatorischen Datenschutzmaßnahmen muss mittels einer Risikoanalyse erfolgen.
Der Verantwortliche setzt hierfür unter Berücksichtigung der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Risikoanalyse ist zudem Grundlage für die Entscheidung, ob eine Datenschutz-Folgenabschätzung nach Art. 35 EU-DSGVO nötig ist, diese ist durchzuführen, wenn sich ein hohes Risiko ergibt.

Ein Risiko ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, welches selbst einen Schaden darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.

Da die Identifikation von Risiken, deren Eintrittswahrscheinlichkeit usw. immer von der tatsächlichen Verarbeitungsweise abhängt, müssen Sie die Beurteilung im Einzelfall selbst vornehmen.
Für die Beurteilung der Schwere eines Schadens finden Sie unten eine Abschätzung, die Sie für Ihre eigene Risikoanalyse übernehmen können.

Vorgehen:

1. Identifikation von Datenschutzrisiken

Zur Identifikation der Datenschutzrisiken ist es hilfreich, zunächst tabellarisch darzustellen:

- Personen, von denen personenbezogene Daten verarbeitet werden
- Verarbeitete Datenarten bzw. Kategorien personenbezogener Daten

Dann werden hierzu jeweils einzeln die Datenschutzrisiken identifiziert. Dabei helfen folgende **Leitfragen:**

- Durch welche Ereignisse und durch welche Handlungen und Umstände kann es zu einem Schaden kommen?
- Welche Schäden können daraus für natürliche Personen entstehen?

Beispiele von betroffenen Personen:

- Schüler
- Lehrkräfte
- Hausmeister

Beispiele von verarbeiteten Datenarten:

- Name
- Anschrift
- Leistungsbeurteilungen, Noten
- Abbildung einer Person (Foto)

Beispiele möglicher Ereignisse / Handlungen:

- für den Betroffenen intransparente Verarbeitung
- unbefugte Offenlegung der und Zugang zu personenbezogenen Daten
- unbeabsichtigte / unzulässige Übermittlung von personenbezogenen Daten
- Verlust oder Zerstörung der personenbezogenen Daten der betroffenen Person
- unbefugte Veränderung oder Löschung personenbezogener Daten
- Unzulässiges Eindringen in IT-Systeme

Beispiele möglicher Schäden:

- Diskriminierung
- Identitätsdiebstahl
- Imageschäden oder Rufschädigung
- wirtschaftliche oder gesellschaftliche Nachteile
- Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden

Für jeden zuvor identifizierten möglichen Schaden und für jedes Ereignis sind die Eintrittswahrscheinlichkeiten und die Schwere der Folgen bei einem möglichen Eintritt abzuschätzen.

Leitfragen:

- Wie wahrscheinlich ist es, dass die oben identifizierten Risiken tatsächlich eintreten können? Dies hängt wesentlich von der Art und Weise ab, in der personenbezogene Daten verarbeitet werden: so ist es in der Regel riskanter, wenn personenbezogene Daten in einer vom Internet erreichbaren Cloud verarbeitet werden, als in einer vom Internet abgeschotteten Umgebung.
- Wie schwer ist der entstehende Schaden für die betroffene Person und auch für den Verantwortlichen?

Vernachlässigbar? Begrenzt? Wesentlich? Maximal?

Beispiele für eine Bewertung der Schwere des Schadens für die häufigsten Daten:

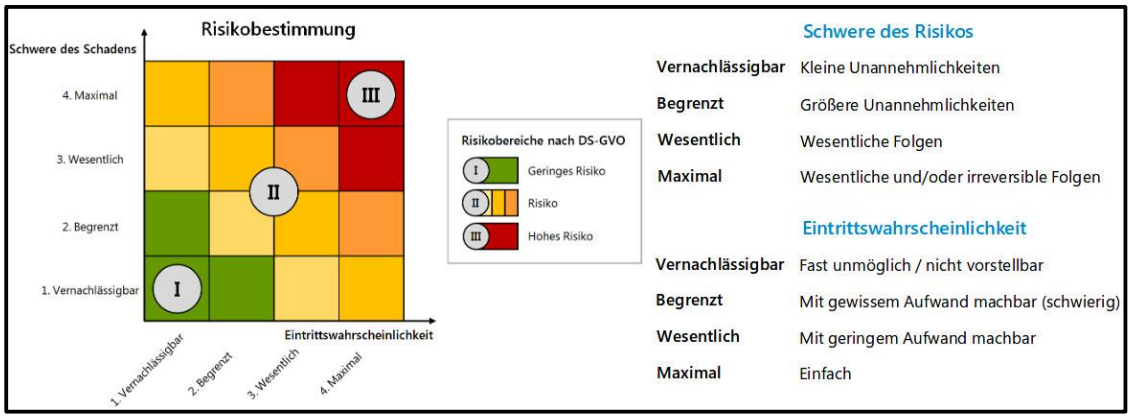
Datenart	**Schwere des Schadens**
Name, Vorname, Klasse	vernachlässigbar
Geburtsort und -Datum, Kontaktdaten (Anschrift, Telefonnummer, Mail-Adresse usw.)	begrenzt
Noten, Leistungs- und Verhaltensbeurteilungen, Kompetenzen, Angaben zum Verhalten, alle Angaben zur Teilnahme am Unterricht und zur Schullaufbahn bzw. Lehrkräftelaufbahn	wesentlich
Daten zu Gesundheitszustand, religiöser Überzeugung oder Religionszugehörigkeit, Herkunftsland, Verkehrssprache in der Familie	maximal

3. Zuordnung zu Risikoabstufungen

Welches Risiko ergibt sich für die verarbeiteten Daten aus der Verarbeitung?

Geringes Risiko, Risiko, hohes Risiko ?

Die Ermittlung des Risikos erfolgt mittels Zuordnung der Schwere des Schadens zur Eintrittswahrscheinlichkeit unter Zuhilfenahme der folgenden Matrix.



Quelle: https://www.lda.bayern.de/media/04_dsfa_praesentation_baylda_iso29134.pdf

4. Eindämmung des Risikos, Festlegung von Datenschutzmaßnahmen

Nachdem die Risiken im Rahmen der Verarbeitung personenbezogener Daten identifiziert und beurteilt sind, müssen angemessene technische und organisatorische Abhilfemaßnahmen nach Art. 32 EU-DSGVO ergriffen werden, welche eine Eindämmung der Risiken bewirken:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Beispiele für Abhilfemaßnahmen:

- Pseudonymisierung (um beispielsweise die Übermittlung von Klarnamen der Schülern an einen Dienstleister zu vermeiden)
- Sperrung von Daten (um beispielsweise für die Dauer einer Aufbewahrungsfrist die personenbezogenen Daten von einer weiteren Verarbeitung auszuschließen)
- Verschlüsselung (z. B. bei Datenspeicherung, dem Transport oder der Übermittlung)
- Einführung eines Rechte- und Rollenkonzeptes
- Zutritts- und Zugangsbeschränkungen (abgeschlossen Räume oder Schränke)
- Protokollierfunktion (Erfassung, welche Person zu welchem Zeitpunkt welche Daten eingegeben, verändert oder gelöscht hat)
- Datensicherung (Backup)

Bei jeder Verarbeitung personenbezogener Daten müssen Datenschutzmaßnahmen getroffen werden. Diese werden über eine Risikoanalyse ermittelt.

Die Durchführung der Risikoanalyse ist zu dokumentieren (Art. 24 Abs. 1 EU-DSGVO).