EU-Datenschutz-Grundverordnung (DS-GVO)

Das BayLDA auf dem Weg zur Umsetzung der Verordnung

Wichtiger Hinweis zu diesem Dokument:
Die DS-GVO wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Die Aufsichtsbehörden sind aktuell bemüht, durch intensive Abstimmungsrunden eine einheitliche Sichtweise der neu geregelten Grundlagen und Anforderungen an den Datenschutz auf europäischer Ebene zu erzielen. Das BayLDA beteiligt sich deshalb an verschiedenen Arbeitskreisen, die sich dieser Herausforderung auch in Deutschland stellen. In der Zwischenzeit möchte das BayLDA Interessierten einen Einblick gewähren, welche Themenkomplexe der DS-GVO derzeit auch in der bayerischen Aufsichtsbehörde intensiv diskutiert werden. Das BayLDA veröffentlicht deshalb in regelmäßigen Abständen (geplant: zweimal im Monat) ein kurzes Papier zu einem ausgewählten Schwerpunkt. Das BayLDA weist ausdrücklich darauf hin, dass es sich hierbei um keine verbindlichen Auffassungen handelt, sondern um gegenwärtige Interpretationen und Meinungen zur DS-GVO. Kommentare zum dargestellten gegenwärtigen Verständnis nimmt das BayLDA gerne entgegen.

XVIII Datenschutz-Folgenabschätzung (DSFA) - Art. 35 DS-GVO

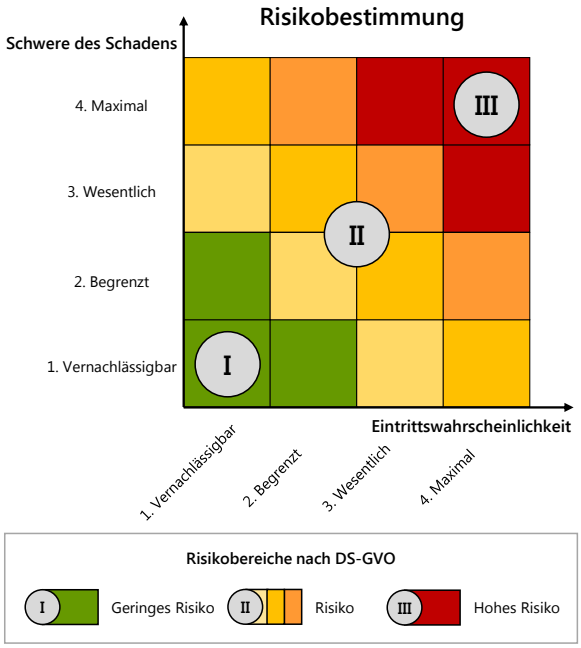
Die Methode einer Datenschutz-Folgenabschätzung (DSFA), englisch Privacy Impact Assessment (PIA) genannt, ist im internationalen Vergleich nicht neu – für den „deutschen" Datenschutz allerdings schon und muss daher schrittweise „erhellt" werden.

Wann ist eine DSFA durchzuführen?

Wenn eine Form der Verarbeitung, d. h. eine konkret durchgeführte Verarbeitungstätigkeit ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringt, ist eine DSFA durchzuführen.

Risikoanalyse

Der Begriff des Risikos zieht sich wie ein *roter Faden* durch die Grundverordnung. Das Risiko soll nach objektiven Kriterien ermittelt werden und Faktoren wie Eintrittswahrscheinlichkeit, Schaden bei der Art, Umfang, Umstände und Zweck einer konkreten Verarbeitung berücksichtigen (ErwGr. 76). Es kann sinnvoll sein, die Faktoren *Eintrittswahrscheinlichkeit* und *Schaden* in wenigen Ausprägungen auszugestalten:



Bei der Festlegung der Eintrittswahrscheinlichkeit muss die Risiko-Quelle, d. h. der „Angreifer" für einen möglichen Schaden für den Betroffenen bestimmt werden – diese hängt jeweils von der konkreten Verarbeitungstätigkeit ab.

Wichtig: Bei der Risiko-Analyse steht der Betroffene im Mittelpunkt der Betrachtung (Datenschutz-Risiko). Der (monetäre) Schaden für die

Organisation (Compliance-Risiko) kann allerdings für die notwendige Motivation sorgen (z. B. Risiko von Sanktionen).

Ebenso wichtig: Ein hoher Schutzbedarf resultiert nicht zwangsweise in einem hohen Risiko (z. B. bei Gesundheitsdaten), da beispielsweise eine geringe Eintrittswahrscheinlichkeit eines Vorfalls vorhanden sein kann.

Was ist unter einem „Schaden bezüglich Rechte und Freiheiten" zu verstehen?

ErwGr. 75 gibt hierzu Hilfestellung: Eine Verarbeitung kann demnach zu physischen, materiellen und immateriellen Schäden führen. Darunter wird beispielsweise verstanden:

- Diskriminierung
- Identitätsdiebstahl
- Finanzieller Verlust
- Rufschädigung
- Hinderung der Kontrolle über eigene Daten
- Profilbildung mit Standortdaten

Risikoreduktion durch geeignete Maßnahmen

Das Risiko einer Verarbeitung muss durch technische, organisatorische und ggf. rechtliche Maßnahmen reduziert werden. Dazu sind im Rahmen einer DSFA in erster Linie sogenannte Datenschutz-Maßnahmen (Privacy Controls) auszuwählen und auf die Risiken einer zulässigen Verarbeitung anzuwenden. Diese ergänzen die Maßnahmen der Sicherheit der Verarbeitung (Art. 32), die ohnehin durchzuführen sind und die ebenfalls das Risiko und primär fahrlässiges und unrechtmäßiges Handeln interner wie externer Risikoquellen berücksichtigen.

Inhalt einer DSFA

Eine Datenschutz-Folgenabschätzung muss eine systematische Beschreibung der Verarbeitungsvorgänge und die Zwecke der Verarbeitung enthalten. Dazu sind (technische) Prozesse, IT-Systeme und Produkte sowie Datenflüsse und Systemgrenzen im Detail zu bewerten. Die berechtigten Interessen des Verantwortlichen, z. B. Sicherheit durch neuartige Videoüberwachung oder Erkenntnisse durch Big-Data-Analysen, sind zu beschreiben sowie die Verhältnismäßigkeit und Notwendigkeit der Verarbeitung festzulegen. Zusätzlich ist eine systematische Risikobeurteilung (Risk assessment) durchzuführen. Durch geeignete Maßnahmen wird das Risiko minimiert – ist das Restrisiko dann immer noch *hoch*, ist die zuständige Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO).

Vorabkontrolle 2.0?

Die Durchführung einer DSFA ist ein nichttrivialer Prozess, der auch für die Nachweispflicht (Accountability) eine zentrale Rolle spielt. Da u.a. eine systematische Vorgehensweise samt sehr ausführlicher Dokumentation bewältigt werden muss, ist eine DSFA nicht mit einer Art „BDSG-Vorabkontrolle 2.0" umzusetzen.

Black-/White-Listen

Die Aufsichtsbehörden müssen Listen von Verarbeitungstätigkeiten veröffentlichen, bei denen eine DSFA durchzuführen ist (*blacklist*). Ebenso können diese auch Listen erstellen, bei denen festgelegt wird, dass keine DSFA gemacht werden muss (*whitelist*). Hieran arbeiten die Aufsichtsbehörden derzeit. Eine Schwellwertanalyse, also die Frage ob eine DSFA durchgeführt werden muss, ist für jede Verarbeitungstätigkeit durchzuführen und zu dokumentieren.

Ausblick

Es kann sich bereits heute lohnen, einen Blick über die deutschen Landesgrenzen zu werfen:

- ISO 29134 Privacy Impact Assessment[1]
- Privacy Impact Assessment der CNIL[2]

Auf europäischer Ebene wird momentan ein Working-Paper zur DSFA abgestimmt. Sobald dieses veröffentlicht ist, wird das BayLDA mit Praxisbeispielen über das wichtige Instrument DSFA auf der eigenen Webseite informieren.

[1] Draft
[2] https://www.cnil.fr/en/node/15798