SÄCHSISCHER
DATENSCHUTZBEAUFTRAGTER

Freistaat
SACHSEN

Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO

für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen durchzuführen ist

Stand: 06.06.2018

Federführend erarbeitet von der Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Basis der Beiträge von Mitgliedern der Unterarbeitsgruppe Datenschutz-Folgenabschätzung (UAG DSFA) des Arbeitskreises Grundsatzes der Datenschutzkonferenz

Redaktion:
Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Promenade 27, 91522 Ansbach
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

A Gesetzliche Grundlage

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (EU-Datenschutz-Grundverordnung – DS-GVO) regelt im Abschnitt 3 „Datenschutz-Folgenabschätzung und vorherige Konsultation" des Kapitels IV „Verantwortlicher und Auftragverarbeiter" die Rahmenbedingungen zur sog. Datenschutz-Folgenabschätzung (kurz: DSFA; im Englischen Data Protection Impact Assessment oder DPIA). Artikel 35 DS-GVO nennt dabei die Grundsätze, bei welchen Fällen eine DSFA durchzuführen ist und was diese enthält. Artikel 36 DS-GVO beschreibt das besondere Verfahren der Konsultation des Verantwortlichen bei der Aufsichtsbehörde bei Fortbestehen hoher Risiken auch nach Anwendung der auf Grundlage der DSFA festgelegten verhältnismäßigen technischen und organisatorischen Maßnahmen.

Grundlage dieses Dokuments ist Art. 35 Abs. 4 DS-GVO:

> *„Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss."*

Die vorliegende unter den Mitgliedern der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (DSK) abgestimmte Liste beinhaltet auch solche Verarbeitungsvorgänge, die mit dem Angebot von Waren und Dienstleistungen für betroffene Personen in mehreren Mitgliedsstaaten verbunden sind. Sie unterliegt daher aufgrund von Art. 35 Abs. 6 DS-GVO dem Kohärenzverfahren gemäß Art. 63 DS-GVO.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in Art. 35 Abs. 3 DS-GVO oder der vorliegenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Art. 35 Abs. 1 DS-GVO von ihren Abhilfebefugnissen gemäß Art. 58 Abs. 2 DS-GVO einschließlich der Verhängung von Geldbußen gemäß Art. 83 Abs. 4 DS-GVO Gebrauch machen. Gegen einen derartigen Beschluss der Aufsichtsbehörde steht der Rechtsweg gemäß Art. 78 DS-GVO offen.

Die in dem Dokument dargestellte Liste wird nachfolgend als „**Muss-Liste**" bezeichnet – gängige Begriffe in anderen Ländern sind hierfür auch „Blacklist" und „Positivliste".

B Ziel dieses Dokuments

Ziel des Dokuments ist es, einen Entwurf für die Liste nach Art. 35 Abs. 4 DS-GVO zu entwickeln, der auch auf europäischer Ebene diskutiert und nach Art. 35 Abs. 6 DS-GVO im Kohärenzverfahren gemäß Art. 63 DS-GVO behandelt werden kann, sofern die Bedingungen hierzu erfüllt sind. Berücksichtigt werden bisherige Veröffentlichungen von anderen Aufsichtsbehörden und Fachgremien, insbesondere das Working Paper 248 rev.01 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"" der Art. 29 Datenschutzgruppe sowie die umfangreichen internen Kommentierungen im Rahmen der UAG DSFA.

Das Dokument hat nicht den Anspruch der Vollständigkeit, wenngleich versucht wird, möglichst viele der DSFA-pflichtigen Verarbeitungsvorgänge zu berücksichtigen. Auf Grund der Schnelllebigkeit im digitalen Umfeld kann dieses Dokument nur als „lebendiges" Papier angesehen werden, das ständigen Änderungskontrollen hinsichtlich der Aufnahme neuer Verarbeitungen in die Liste der Verarbeitungsvorgänge unterliegt. Die DSK wird hierfür einen Prozess erarbeiten, wie Verarbeitungstätigkeiten für die Muss-Liste vorschlagen, beurteilt und aufgenommen werden. Änderungen an Einträgen der Muss-Liste werden dokumentiert, so dass die Muss-Liste eine entsprechende Versionshistorie erhalten wird.

Wichtiger Hinweis:
Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Liste nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass keine DSFA durchzuführen wäre. Stattdessen ist es Aufgabe des Verantwortlichen, im Wege einer Vorabprüfung einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen aufweist und damit die Voraussetzungen des Art. 35 Abs. 1 Satz 1 DS-GVO erfüllt. Zum Begriff des Risikos wird auf die Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248 Rev. 01 17/DE angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017) der Art. 29 Datenschutzgruppe und das Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen" der DSK verwiesen.

C Liste nach Art. 35 Abs. 4 DS-GVO

Maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen sind in der Leitlinie in WP 248 der Art. 29 Gruppe ab Seite 10 ff. wie folgt zu entnehmen:

1. **Bewerten oder Einstufen** (Scoring)
   ("Evaluation or scoring")
2. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
   ("Automated-decision making with legal or similar significant effect")
3. **Systematische Überwachung**
   ("Systematic monitoring")
4. **Vertrauliche oder höchst persönliche Daten**
   ("Sensitive data or data of a highly personal nature")
5. **Datenverarbeitung in großem Umfang**
   ("Data processed on a large scale")
6. **Abgleichen oder Zusammenführen von Datensätzen**
   ("Matching or combining datasets")
7. **Daten zu schutzbedürftigen Betroffenen**
   ("Data concerning vulnerable data subjects")
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
   ("Innovative use or applying new technological or organisational solutions")
9. **Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert**
   ("When the processing in itself prevents data subjects from exercising a right or using a service or a contract")

Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist vielfach ein hohes Risiko gegeben und eine DSFA durch den Verantwortlichen durchzuführen. In wenigen Einzelfällen mag es jedoch auch vorkommen, dass nur eines der genannten Kriterien erfüllt wird und dennoch auf Grund eines hohen Risikos des Verarbeitungsvorgangs eine DSFA notwendig wird.

Das Ergebnis der Vorabprüfung und die zugrunde gelegten Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.

Sämtliche Verarbeitungstätigkeiten, die in der nachfolgenden Liste enthalten sind, können auch durch Anwendung der Kriterien des WP 248 abgebildet werden. Dadurch ist auch ein Abgleich dieser Liste mit weiteren europäischen Listen im Rahmen der Anforderungen nach Art. 35 Abs. 4 DS-GVO gegeben.