Pflichten der Verantwortlichen und Auftragsverarbeiter gegenüber der Aufsichtsbehörde (TLfDI)

Nachfolgend erhalten Sie eine Übersicht, welche Pflichten Sie als Verantwortlicher oder Auftragsverarbeiter gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) haben. Ausschließlich die hier aufgeführten Pflichten sind gegenüber dem TLfDI zu beachten. Weitergehende Dokumente übersenden Sie dem TLfDI bitte nur nach Aufforderung.

1. Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO
(Datenpanne)

Die Verletzung des Schutzes personenbezogener Daten liegt vor, wenn ein Sicherheitsdefizit zur Vernichtung, zum Verlust oder zur Veränderung von personenbezogenen Daten führte. Die unbefugte Offenlegung oder der unbefugte Zugang zu personenbezogenen Daten, führt ebenso zur Verletzung des Schutzes personenbezogener Daten, vgl. Art. 4 Nr. 12 DS-GVO.
Eine Meldung ist dann nicht erforderlich, wenn im Einklang mit dem Grundsatz der Rechenschaftspflicht nachgewiesen werden kann, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt** (Art.33 Abs.1 S.1 DSGVO). Diese Prüfung ist vorab durchzuführen und zu dokumentieren.

Beispiele möglicher Schäden:
Verlust der Kontrolle überpersonenbezogene Daten oder Einschränkung der Rechte Betroffener, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

durch zum Beispiel:
Verlust des (Dienst-) Handy‘s, Diebstahl des Rechners, Hackerangriff, Phishing, Diebstahl von Festplatten, u. a.

- **dies ist dem TLfDI unverzüglich und binnen 72 Stunden nach Kenntnisnahme zu melden**
  - (ansonsten tragfähige Begründung der zeitverzögerten Meldung an TLfDI)

- **Auftragsverarbeiter melden die Verletzung des Schutzes personenbezogener Daten dem Verantwortlichen** (Dieser entscheidet, ob Meldung an TLfDI erforderlich ist u. nimmt dann die Meldung beim TLfDI vor.)

Die Meldung an den TLfDI muss nach Art. 33 Abs. 3 DS-GVO zumindest folgende Informationen enthalten:

- Beschreibung der Art der Verletzung
- (Kategorie und Zahl der Betroffenen, Kategorien und Zahl der betroffenen Datensätze)

- Zeitraum/Zeitpunkt des Vorfalls

- Zeitpunkt der Feststellung des Vorfalls

- Namen und Kontaktdaten des Datenschutzbeauftragten oder
- sonstiger Ansprechpartner für weitere Informationen

- Beschreibung der bereits getroffenen oder vorgeschlagenen (technische und organisatorische) Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

- vorgeschlagene oder bereits vorgenommene (technische und organisatorische) Maßnahmen zur Abmilderung der nachteiligen Auswirkungen für die betroffenen Personen

- Wahrscheinliche Folgen der Verletzung des Schutzes personenbezogener Daten

- Angaben zum Zeitpunkt der Benachrichtigung der betroffenen Personen über die Schutzverletzung gemäß Art. 34 DS-GVO

Für eine derartige Meldung nach Art. 33 DS-GVO stellt der TLfDI ein „Formblatt zur Meldung der Verletzung des Schutzes personenbezogener Daten“ auf seiner Webseite unter https://tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx zur Verfügung.

2. Konsultationspflicht bei weiterhin hohem Risiko nach der Datenschutz-Folgenabschätzung
(Art. 36 Abs. 1 DS-GVO)

Nach Art. 35 Abs. 1 DS-GVO führt der Verantwortliche **vorab** eine Datenschutz-Folgenabschätzung (DSFA) durch. Vor jeder Datenverarbeitung ist zu prüfen, ob eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.** Das Ergebnis dieser Prüfung ist zu dokumentieren. Soweit das Ergebnis dieser Prüfung mit „JA“ beantwortet wird, ist eine DSFA durchzuführen.

Außerdem und insbesondere ist eine DSFA durchzuführen, wenn

- eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitungen einschl. Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigt (Profiling, Tracking, Scoring),
- besondere Arten personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DS-GVO verarbeitet werden oder
- eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche stattfindet (Videoüberwachung).

Im Rahmen der DSFA sind Maßnahmen zum Ziel der Eindämmung des Risikos zu ergreifen. Für Informationen wie dies im Einzelnen durchzuführen ist, finden Sie unter https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/ in Kurzpapier Nr. 5 – „Datenschutz-Folgenabschätzung“ und in Kurzpapier Nr. 18 – „Risiko für die Rechte und Freiheiten natürlicher Personen“ der Datenschutzkonferenz (DSK).

Soweit nach vorgenommener DSFA weiterhin ein hohes Risiko besteht, konsultiert der Verantwortliche die Aufsichtsbehörde und stellt folgende Informationen zur Verfügung:

- Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und ggf. der an der Verarbeitung beteiligten Auftragsverarbeiter
- Zwecke und Mittel der beabsichtigten Verarbeitung
- vorgesehene Maßnahmen und Garantien zum Schutz der Rechte und Freiheiten der betroffenen Personen
- Kontaktdaten des Datenschutzbeauftragten
- Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO
- Angaben zu den Kategorien der besonderen Arten personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) der Verarbeitung

Weitere Informationen sind dem TLfDI nach Aufforderung vorzulegen. Auf unserer Website finden Sie eine Liste der Verarbeitungsarten für die eine Datenschutz-Folgenabschätzung durchzuführen ist unter https://www.tlfdi.de/mam/tlfdi/datenschutz/liste_dsfa.pdf.

3. Meldung des Datenschutzbeauftragten
(Art. 37 Abs. 7 DS-GVO und § 38 Abs. 1 BDSG)

Die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz (BDSG) regeln, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter in bestimmten Fällen einen Datenschutzbeauftragten (DSB) zu benennen haben.

Ein DSB ist dann zu benennen, wenn:

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird **oder**
- die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 Abs. 1 Buchst. b) DS-GVO), **oder**
- wenn eine umfangreiche Verarbeitung besonderer Kategorien von Daten (s. Art. 9 DS-GVO, beispielsweise von Gesundheitsdaten) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten durchgeführt wird (s. Art. 10, Art. 37 Abs. 1 lit. c) DS-GVO) **oder**
- wenn der Verantwortliche und der Auftragsverarbeiter zehn oder mehr Personen beschäftigt, die regelmäßig automatisiert personenbezogene Daten verarbeiten (§ 38 Abs. 1 Satz 1 BDSG) **oder**
- wenn der Verantwortliche oder der Auftragsverarbeiter eine Datenschutz-Folgenabschätzung durchzuführen hat (s. a. https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_5_datenschutz-folgenabschatzung.pdf; § 38 Abs. 1 Satz 2, 1. Alternative BDSG) **oder**
- wenn der Verantwortliche oder der Auftragsverarbeiter im Bereich der Markt und Meinungsforschung tätig ist (§ 38 Abs. 1 Satz 2, 3. Alternative BDSG-) **oder**

- wenn der Verantwortliche oder der Auftragsverarbeiter Daten geschäftsmäßig zum Zweck der Übermittlung, auch anonymisiert, verarbeitet (§ 38 Abs. 1 Satz 2, 2. Alternative BDSG).

Der DSB wird auf Grundlage seiner beruflichen Qualifikationen und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt.

Gemäß Art. 37 Abs. 7 DS-GVO teilt der Verantwortliche oder der Auftragsverarbeiter der Aufsichtsbehörde die Benennung des DSB mit. Um der Meldepflicht aus Art. 37 Abs. 7 DS-GVO **nachzukommen** hat der TLfDI zur Vereinheitlichung der Meldungen und zukünftigen Nach-, Um– oder Abmeldungen ein **Formular zur Meldung des Datenschutzbeauftragten** erstellt. Das Formular ist unter https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/ zu finden.
Nach Eingang der Meldung wird vom TLfDI eine schriftliche Eingangsbestätigung erteilt.