Erfurt, den 24.04.2024

Prüfschema zur Bearbeitung von

Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO

von öffentlichen und nicht-öffentlichen Stellen

1. Verletzung des Schutzes personenbezogener Daten:

   - geht es um personenbezogene Daten, Art. 4 Nr. 1 DS-GVO?
   - liegt eine Verletzung des Schutzes personenbezogener Daten vor: Eine Verletzung liegt vor, wenn es zu einer Verletzung der Sicherheit kommt, egal ob unbeabsichtigt oder unrechtmäßig, die zur Vernichtung, zum Verlust oder zur Veränderung oder zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Falls nicht, Hinweis an den Verantwortlichen und Vorgang schließen. Andernfalls Eingangsbestätigung.

2. Meldung des Vorfalls binnen 72 Stunden nach Bekanntwerden?
3. Eventuelle Begründung für Verzögerung prüfen.

Falls nicht, Einleitung Owi wegen verspäteter Einreichung prüfen.

4. Durch den Verantwortlichen?
   Der Auftragsverarbeiter muss nur gegenüber dem Verantwortlichen, für den er tätig ist, nach Art. 33 Abs. 2 DS-GVO den Datenschutzverstoß melden. Gegenüber der Aufsichtsbehörde muss der Verantwortliche selbst melden.

Falls nicht, Hinweis an den Meldenden und nachfordern und/oder an zuständige Aufsichtsbehörde verweisen.

5. Vollständige Meldung?
   - Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
   - Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen
   - Name und Kontaktdaten des Datenschutzbeauftragten
   - Beschreibung der wahrscheinlichen Folgen
   - Beschreibung der ergriffenen Maßnahmen
   - Risikoprognose hinsichtlich Art. 34 ([kein]hohes Risiko) mit Begründung

Falls nicht, nachfordern (mit kurzer Frist).

Nachdem die Meldung beim TLfDI eingegangen ist, erfolgt die Eintragung in die Excel-Liste.

6. Ausreichende Maßnahmen?
   Der Verantwortliche teilt dem TLfDI eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen mit. Hierbei ist zu prüfen:

- welche Maßnahmen wurden ergriffen?
- sind die ergriffenen Maßnahmen ausreichend?
- sind die getroffenen Maßnahmen nachvollziehbar?
- sind weitere Maßnahmen erforderlich?

Falls nicht, nachfordern.

7. Benachrichtigung der betroffenen Personen nach Art. 34 DS-GVO erfolgt?
   Wenn nicht,
   - geht der Verantwortliche nicht von einem voraussichtlich hohen Risiko für die betroffenen Personen aus und ist seine Begründung nachvollziehbar oder
   - hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die betroffene Person?
     Ein hohes Risiko besteht in der Regel, wenn eine Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO stattgefunden hat.
     Darüber hinaus auch für andere personenbezogene wie Bankverbindungs- und Kreditkartendaten in den Fällen von physischen, materiellen oder immateriellen Schäden für die Betroffenen, bei dem Verlust der Kontrolle über ihre Daten, Diskriminierung, Identitätsdiebstahl, finanziellen Verlusten, unbefugter Aufhebung von Pseudonymisierung, Rufschädigung und bei Verlust der Vertraulichkeit von Berufsgeheimnissen.
     Eine Benachrichtigung nach Art. 34 DS-GVO ist ebenfalls erforderlich, wenn mit erheblichen Konsequenzen oder schwerwiegenden Beeinträchtigungen wie erhebliche wirtschaftlichen oder gesellschaftlichen Nachteilen zu rechnen ist.
     Sobald betroffene Personen etwas tun können, um ihr Schadensrisiko zu verringern, sind sie zu benachrichtigen.

     Eine Benachrichtigung ist ausnahmsweise dann nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die Verletzung der betroffenen Personen angewandt, insbesondere, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht wurden, etwas durch Verschlüsselung.

Falls nicht, nachfordern.

Kommt der Verantwortliche den Forderungen nicht nach, sind sie in einem Verwaltungsverfahren durchzusetzen.