ERGO

Datenschutz-Folgenabschätzung (DSFA)

Voraussetzungen – Anforderungen – Maßnahmen – Erfahrungen

Intern

69. Treffen GDD Erfakreis Nürnberg / IHK AnwenderClub „Datenschutz und Informationssicherheit“
Nürnberg, 15. Oktober 2019; Malte Kaspar (DSB)

Datenschutz-Folgenabschätzung

ERGO

1. Allgemeines

ERGO am Standort Nürnberg im zeitlichen Ablauf:

1984 Errichtung von Quelle + Partner Lebens- und Sachversicherung

1989 neue Firmierung: Quelle Versicherungen

2002 Verkauf der Quelle Versicherungen an die ERGO Versicherungsgruppe AG

2002 Umfirmierung in KarstadtQuelle Versicherungen

2008 übernimmt die ERGO Versicherungsgruppe AG (heute ERGO Group AG) die restlichen Anteile von KarstadtQuelle Versicherungen

2010 Umfirmierung in ERGO Direkt Versicherungen

2016 Etablierung als Kompetenz-Zentrum Online von ERGO in Deutschland

2019 Gründung der Dienstleistungsgesellschaft ERGO Direkt AG
Die ERGO Direkt AG tritt im äußeren Erscheinungsbild als ERGO auf ⇨ one ERGO

1. Allgemeines

- Diese Präsentation ist als Hinführung / Einstieg zum Thema „Datenschutz-Folgenabschätzung“ zu sehen. Alle aufgezeigten Möglichkeiten sind als Diskussionsgrundlage anzusehen.
- Eine Vollständigkeit zum Thema „Datenschutz-Folgenabschätzung“ kann und soll nicht mit diesem Vortrag gewährleistet werden.
- Die inhaltliche Darstellung greift auf gesetzliche Grundlagen aus der DSGVO und auf Erfahrungen des zurückliegenden Jahres zurück.
- Neben den gesetzlichen Grundlagen diente das GDD-Jahrbuch 2019 (Sonderdruck) mit seinen Inhalten sowie www.lda.bayern.de als Informationsquelle.
- Wenn von der IT gesprochen wird, sind hierunter alle Bereiche der IT subsumiert (Anwendungsentwicklung, Services, Systembetrieb etc.).

2. Hinführung zum Thema DSFA

- Der DSB hat die Verpflichtung der Überwachung der Datenschutzkonformität des Unternehmenshandelns ⇨ DSB als Überwachungsorgan.
- Das führen der Verarbeitungsübersichten obliegt dem jeweiligen Fachbereich, dem Verantwortlichen (Art. 35 DSGVO), in dem die jeweiligen Verarbeitungen stattfinden.
- Die DSFA ist ein Bestandteil der Verarbeitungsübersicht, die es gilt durchzuführen, wenn hohe Risiken bestehen.
- Die betroffenen Fachbereiche und die involvierten Bereiche der IT haben die Verpflichtung sich den Rat des DSB einzuholen (Art. 35 Abs. 2 DSGVO), der DSB ist verpflichtet die Beratung anzubieten und durchzuführen.
- Der DSB prüft, ob eine DSFA überhaupt durchgeführt wird / worden ist.
- Wahrnehmung von Beratungstätigkeiten gem. Art. 39 Abs. 1 Lit. c DSGVO ⇨ diese schauen allerdings derzeit so aus, dass der DSB zusammen mit dem jeweiligen Fachbereich die DSFA durchführt, also ein mehr an Beratung

3. Vorgaben gem. Art. 35 DSGVO unter Berücksichtigung der EWG 84, 89-93

- Eine DSFA sollte eine umfassende Risikobewertung von Verarbeitungsprozessen ermöglichen und deren Nachvollziehbarkeit gewährleisten. Dafür sind mindestens die folgenden Schritte nach Art. 35 Abs. 7 DSGVO notwendig, die allerdings nicht ohne Mithilfe der IT (z. Bsp. AE, Betrieb), die u.a. für die technischen Schutzmaßnahmen zuständig ist, angegangen werden sollten:
  - systematische Beschreibung der Verarbeitungen ⇨ Beschreibung der einzelnen Verarbeitungsschritte einschließlich der getroffenen organisatorischen und technischen Schutzmaßnahmen wird notwendig ⇨ ausführen, wie der Schutz der Persönlichkeitsrechte gewährleistet wird
  - die Zwecke der vorzunehmenden Verarbeitungen sowie die implementierten Schutzmaßnahmen müssen beschrieben werden ⇨ Art. 35 Abs. 7 lit a DSGVO
  - mögliche berechtigte Interessen gem. Art. 6 f DSGVO müssen in nachvollziehbarer Weise dargestellt und dokumentiert werden

3. Vorgaben gem. Art. 35 DSGVO unter Berücksichtigung der EWG 84, 89-93

- Bewertung der Notwendigkeit und Wahrung des Verhältnismäßigkeitsgrundsatzes der zugrunde liegenden Prozesse gem. Art. 35 Abs. 7 lit b DSGVO ⇨ sind alle Daten notwendig zur Erfüllung des vorgesehenen Prozesses ⇨ Stichwort „Datensparsamkeit“ (hier ist die Sensibilität der AE gefragt)
- Bewertung der zugrunde liegenden hohen Risiken hinsichtlich der bestehenden Rechte und Freiheiten des Betroffenen gem. Art. 35 Abs. 7 lit c DSGVO ⇨ verschiedene Methoden möglich
  - bei dem Einsatz neuer Technologien (sind entsprechende technische Maßnahmen implementiert)
  - aufgrund der Art und des Umfangs der zu verarbeitenden Daten (Gesundheitsdaten, besondere Kategorien von Daten), wurden Schutzmaßnahmen wie Pseudonymisierung, Verschlüsselung etc. eingesetzt
  - profiling / scoring
  - biometrische Daten (besonders hoher Anspruch an technische Schutzmaßnahmen)
  - weiträumige Videoüberwachung öffentlicher Bereiche (Beachtung der technischen Vorgaben wie Kamerawinkel, Verpixelung etc.)
  - grundsätzlich Durchführung einer DSFA, wenn der Prozess auf der „blacklist“ geführt wird

4. Zeitpunkt und Inhalte einer DSFA

- Gem. den Vorgaben des Art. 35 Abs. 1 DSGVO hat der Verantwortliche bei Vorliegen eines hohen Risikos für die Rechte und Freiheiten einer natürlichen Person, **vor Einführung** der Verarbeitungsvorgänge bzw. der Prozesse eine DSFA durchzuführen.

  - ➢kein neuer Prozess in der operativen Umgebung, wenn nicht die DSFA abgeschlossen ist ⇨ daraus lässt sich ableiten:

    - rechtzeitige Erstellung eines Fachkonzeptes
    - frühzeitige Einbindung aller betroffenen Bereiche
    - frühzeitige Durchführung einer DSFA um bei einer notwendigen Ansprache der zuständigen Aufsicht genügend Vorlauf zu haben

      - ❖ Behörde hat drei Monate Zeit für die Bearbeitung des Vorgangs
      - ❖ Behörde hat die Möglichkeit der Verlängerung um weitere drei Monate ⇨ Verzögerungen bis zu einem halbe Jahr möglich, wenn Vorgaben der Aufsicht umzusetzen sind kann entsprechend mehr Zeit ins „Land“ gehen

4. Zeitpunkt und Inhalte einer DSFA

- **Achtung:** stellt die Aufsicht fest, dass Prozesse vor Abschluss der DSFA durchgeführt werden, kann es zu einem unmittelbar wirkenden **Verbot der Verarbeitung** kommen
- nach Art. 83 Abs. 4 lit a. DSGVO kann es zu Geldbußen bis zu zehn Mio. Euro kommen, je nachdem welche Art der Verarbeitung von personenbezogenen Daten durchgeführt wird

➢ähnliche Verarbeitungen können in einer DSFA zusammengefasst werden, dies ist jedoch entsprechend kenntlich zu machen (z. B. bei der Videoüberwachung versch. Filialen oder Niederlassungen nach dem gleichen Konzept)

- Überprüfung, ob wirklich ein gleichgelagerter Sachverhalt jeweils vorliegt

4. Zeitpunkt und Inhalte einer DSFA

- Art. 35 Abs. 11 DSGVO schreibt vor, dass regelmäßig Überprüfungen durch den Fachbereich durchzuführen sind, um festzustellen, ob die Verarbeitungen in der Art erfolgen, wie sie in der DSFA dargestellt wurden. Es sind also auch **nachträgliche DSFA** möglich, also auch dann, wenn ein Prozess bereits im operativen Geschäft eingesetzt wird. Möglich ist dies …
  - bei einer nachträglich festgestellten Risikoänderung
  - bei einer nachgeschobenen Veränderung der bestehenden „blacklist“
  - nachholen einer pflichtwidrig unterlassenen DSFA
    - grundsätzlich Verstoß gegen Art. 83 Abs. 4 lit a i. V. m. Art. 35 Abs. 1 DSGVO ⇨ regelmäßige Überprüfungen der Verarbeitungsübersichten können die Möglichkeiten eines Verstoßes minimieren
      - die nachträgliche Durchführung einer DSFA kann im obigen Fall eine Geldbuße entbehrlich machen

4. Zeitpunkt und Inhalte einer DSFA

- Grundsätzliche Inhalte einer DSFA:
  - **Projektbeschreibung**
  - **Identifikation datenschutzrelevanter Aspekte**
  - detaillierte **Beschreibung der Verarbeitung**
  - **Identifikation von Risiken sowie deren Bewertung, Gewichtung und Einschätzung der Eintrittswahrscheinlichkeit**
  - **Risikomanagement**
  - **Compliance-Analyse** durchführen
    ⇨ auf welcher rechtlichen Grundlage findet die Verarbeitung der personenbezogenen Daten statt
  - **Berichtsaufbau** ⇨ Identifizierungsmerkmal der DSFA, Managementsummary, Analyse der Notwendigkeit der Durchführung einer DSFA, Detaillierte Projektbeschreibung, Ergebnisse von Konsultationen, Identifikation und Umgang mit festgestellten Risiken, Analyse und Rechtmäßigkeit der Verarbeitung, Schlussfolgerungen

4. Zeitpunkt und Inhalte einer DSFA

- **Abschlußbericht** ⇨ Darstellung der Risiken und ergriffene Maßnahmen zur Minimierung der Risiken
- **Ergebnisüberprüfung** ⇨ Analyse der umgesetzten Ergebnisse im operativen Geschäft

5. Vorgehensweise bei einer DSFA – Prozessbetrachtung und technische Betrachtung

Organisatorische Betrachtungen zum vorgesehenen **Prozess:**

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und deren Zweck
- genaue Beschreibung der Verarbeitungstätigkeit
- Nennung der maßgeblichen Rechtsgrundlagen zur Vornahme der Verarbeitung(en)
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
- ausführliche Beschreibung der hohen Risiken ⇨ Risikomanagement
- Risikoeinschätzung maßgeblicher Schutzziele
- welche Angreifer und Risikoquellen kommen in Betracht ⇨ benennen
- Risikobewertung für die Rechte und Freiheiten der betroffenen Personen
- Analyse des Datenflusses sowie Betrachtung einzelner Prozessschritte

5. Vorgehensweise bei einer DSFA – Prozessbetrachtung und technische Betrachtung

- Technische Risikobetrachtung der eingesetzten Systeme ⇨ Vorgaben des Art. 32 DSGVO:
  - wird der neuste Stand der Technik berücksichtigt
  - Gewährleistung der Vertraulichkeit
  - Berücksichtigung aller eingesetzten internen und externen Systeme, Datenbanken und Anwendungen
  - Einbringen von Abhilfemaßnahmen
  - Abschließende Risikobewertung
  - Ggf. Konsultation der Aufsichtsbehörde

6. Fazit

- Die DSFA ist eine umfassende langwierige Analyse eines Verarbeitungsprozesses der hohe Risiken für die Freiheiten von Betroffenen beinhaltet.
- Die DSFA ist vor der operativen Einführung des Prozesses/der Anwendung durchzuführen.
- Mit der DSFA sollen hohe Risiken minimiert werden, dafür sind die einzelnen Prozessschritte explizit zu betrachten.
- Die DSFA erfordert generell eine umfassende Beschreibung und Analyse der bestehenden Risiken.
- Die DSFA erfordert risikominimierende Gegenmaßnahmen oder bei weiterhin bestehenden hohen Risiko, die Freigabe der jeweiligen Aufsichtsbehörde.
- Die DSFA ist zeitintensiv und bindet Ressourcen.
- Die DSFA ist nutzbringend für beide Seiten (Betroffene & Verantwortliche).
- Die durchgeführte und dokumentierte DSFA dient der in Art. 5 Abs. 2 DSGVO geforderten Rechenschaft.

Vielen Dank für Ihre Aufmerksamkeit!

Malte Kaspar
Datenschutzbeauftragter

Tel 0911 / 148 – 1614
m.kaspar@ergo.de