WIRTSCHAFTSPRÜFERKAMMER

Körperschaft des öffentlichen Rechts

WPK aktuell

Mitgliederinformation

Projektbeispiel: Umsetzung der Anforderungen der DSGVO in der WPK

Projektbeispiel: Umsetzung der DSGVO in der WPK

Projektübersicht

- **Vorstand wurde über die Initiierung und Umsetzung des Projektes anlässlich der 452. VO-Sitzung am 11./12. Juli 2017 informiert.**

- **Geschäftsführung und Datenschutzbeauftragter sowie alle Abteilungen, Referate und Landesgeschäftsstellen der WPK sind in das Projekt eingebunden.**

- **Es erfolgt eine regelmäßige Projektberichterstattung.**

- **Das Projektvorgehen orientiert sich an der einschlägigen Vorgehensweise für die Umsetzung der DSGVO (wie etwa im Kurzpapier Nr. 8 „Maßnahmenplan DSGVO für Unternehmen“ der DSK – Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – beschrieben)**
  → www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Projektbeispiel: Umsetzung der DSGVO in der WPK

Identifizierung von Handlungsbedarf

(1) Datenschutzrechtliche Bestandsaufnahme anhand des Verfahrens-verzeichnisses der WPK

(2) Maßnahmen zur Umsetzung von Betroffenenrechten (Art. 13 – 21 DSGVO), Schwerpunkt: Erst- und Folgeinformationspflichten (Art. 13, 14 DSGVO, §§ 32, 33 BDSG-neu)

(3) Überprüfung des Datenschutzmanagementsystems (DSMS) der WPK

(4) Vertragsanpassungen (Auftragsverarbeiter, andere externe Dienstleister, Anstellungsverträge)

(5) Beachtung der Grundsätze von „privacy by design“ (Datenschutz durch Technikgestaltung) und „privacy by default“ (Datenschutz durch datenschutzfreundliche Voreinstellungen)

Projektbeispiel: Umsetzung der DSGVO in der WPK

(1) Datenschutzrechtliche Bestandsaufnahme

- **Überprüfung Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) – früher Verfahrensverzeichnis:**

  - **Welche gesetzliche Rechtsgrundlage gibt es für Datenerhebung?**
  - **Wenn keine gesetzliche Rechtsgrundlage, gibt es (ausdrückliche) Einwilligung des Betroffenen? → Erwägungsgr. 32 DSGVO: Stillschweigen oder bloße Untätigkeit reicht nicht!**
  - **Wo werden Daten erhoben? (beim Betroffenen oder bei Dritten?)**

- **Überprüfung Vertragsmanagement:**

  - **Welche Verträge mit externen Dienstleistern sind Auftragsverarbeitung (Art. 28 DSGVO)? – entsprechen Vereinbarungen aktuellem Recht?**
  - **Bei welchen anderen Verträgen sind ggf. Vertraulichkeitsklauseln erforderlich?**

(2) Maßnahmen zur Umsetzung von Betroffenenrechten (Art. 13 – 21 DSGVO)

- **Schwerpunkt: Erst- und Folgeinformationspflichten bei Direkt- und Dritterhebung (Art. 13, 14 DSGVO, §§ 32, 33 BDSG-neu): *proaktiv* zu erfüllen (kein Antrag des Betroffenen erforderlich!)**

  - **Welche Informationspflichten gibt es? (nicht, wenn Betroffenem Information bereits bekannt ist oder Gesetzeszweck zuwiderlaufen würde)**
  - **externe Betroffene: Unterrichtung durch Homepage, WPK Magazin und individuell**
  - **interne Betroffene: Unterrichtung durch Datenschutz- und Telekommunikations-richtlinie der WPK**

- **Weitere Betroffenenrechte:**

  - **Auskunft (Art. 15 DSGVO, § 34 BDSG-neu), Löschung/Sperrung (Art. 17 DSGVO, § 35 BDSG-neu), Widerspruch (Art. 21 DSGVO, § 36 BDSG-neu)**

Projektbeispiel: Umsetzung der DSGVO in der WPK

(3) Überprüfung des Datenschutz-Managementsystems (DSMS)

- **Prinzip der „accountability“ (u.a. Art. 5 Abs. 2, 24 Abs. 1 DSGVO): Einhaltung der Datenschutzgrundsätze muss jederzeit durch geeignete Dokumentation und geeignete technisch-organisatorische Maßnahmen (sog. TOMs) nachgewiesen werden können:**

➢ **Aktualisierung und Zusammenführung von Verzeichnis der Verarbeitungstätigkeiten, Datenschutz- und Telekommunikationsrichtlinie, Dienstanweisung zu Schlüsselverwaltung und Türchips, Verzeichnis der IT-Anwendungen u.a. datenschutzrelevanten Dokumenten der WPK**

- **DSMS kann, muss aber nicht IT-gestützt sein!**
  → Beispiel: www.lda.bayern.de/media/leitfaden_krankenhaus.pdf

- **Konkrete Definition von personellen Verantwortlichkeiten (z.B. Geschäftsführung, Abteilungsleiter, Datenschutzbeauftragter)**

Projektbeispiel: Umsetzung der DSGVO in der WPK

(4) Vertragsanpassungen

- **Auftragsverarbeitung i.S.v. Art. 28 DSGVO (früher: Auftragsdatenverarbeitung):**

➢ **Verarbeitung personenbezogener Daten auf Weisung**
➢ **auch: Wartungsverträge (Fern-, Onlinewartung)!**
➢ **Prüfung, ob neue Vereinbarung erforderlich!**

MUSTERVERTRAG: → www.lda.bayern.de/media/muster_adv.pdf

- **Sonstige Verträge (z.B. andere IT-Dienstleistungen, Unterhaltsreinigung)**

➢ **Zweistufige Verpflichtung zur Vertraulichkeit der Datenverarbeitung**

- **Anstellungsverträge**

➢ **Regelungen zur Vertraulichkeit der Datenverarbeitung und Nutzung von Telekommunikationsmitteln des Arbeitgebers**

Projektbeispiel: Umsetzung der DSGVO in der WPK

(5) *Privacy by design / Privacy by default* (Art. 23 Abs. 1, 25 Abs. 2 DSGVO)

- **Datenverarbeitung so auszugestalten, dass Datenschutzgrundsätze wirksam umgesetzt werden, insbesondere Gebot der Datenminimierung**

  - **betrifft nicht nur, aber auch IT!**
  - **IT-Systeme sollten nur zur Zweckerfüllung erforderliche Daten verarbeiten**

- **Maßstab „Stand der Technik“: offen für technisch neue, am Markt verfügbare Produkte (in Abgrenzung zu „Stand von Wissenschaft und Technik“: neueste technisch-wissenschaftliche Erkenntnisse)**

- **Maßnahmen der WPK u.a.:**

  - **Pseudonymisierung von IP-Adressen**
  - **Verschlüsselung von Datenträgern und Datenübermittlung**
  - **Automatisierte Löschung von Telekommunikationsdaten**

Projektbeispiel: Umsetzung der DSGVO in der WPK

Weiterführende Hinweise:

→ **www.wpk.de/mitglieder/praxishinweise/datenschutz/**

→ **www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html**

Vielen Dank für Ihre Aufmerksamkeit!