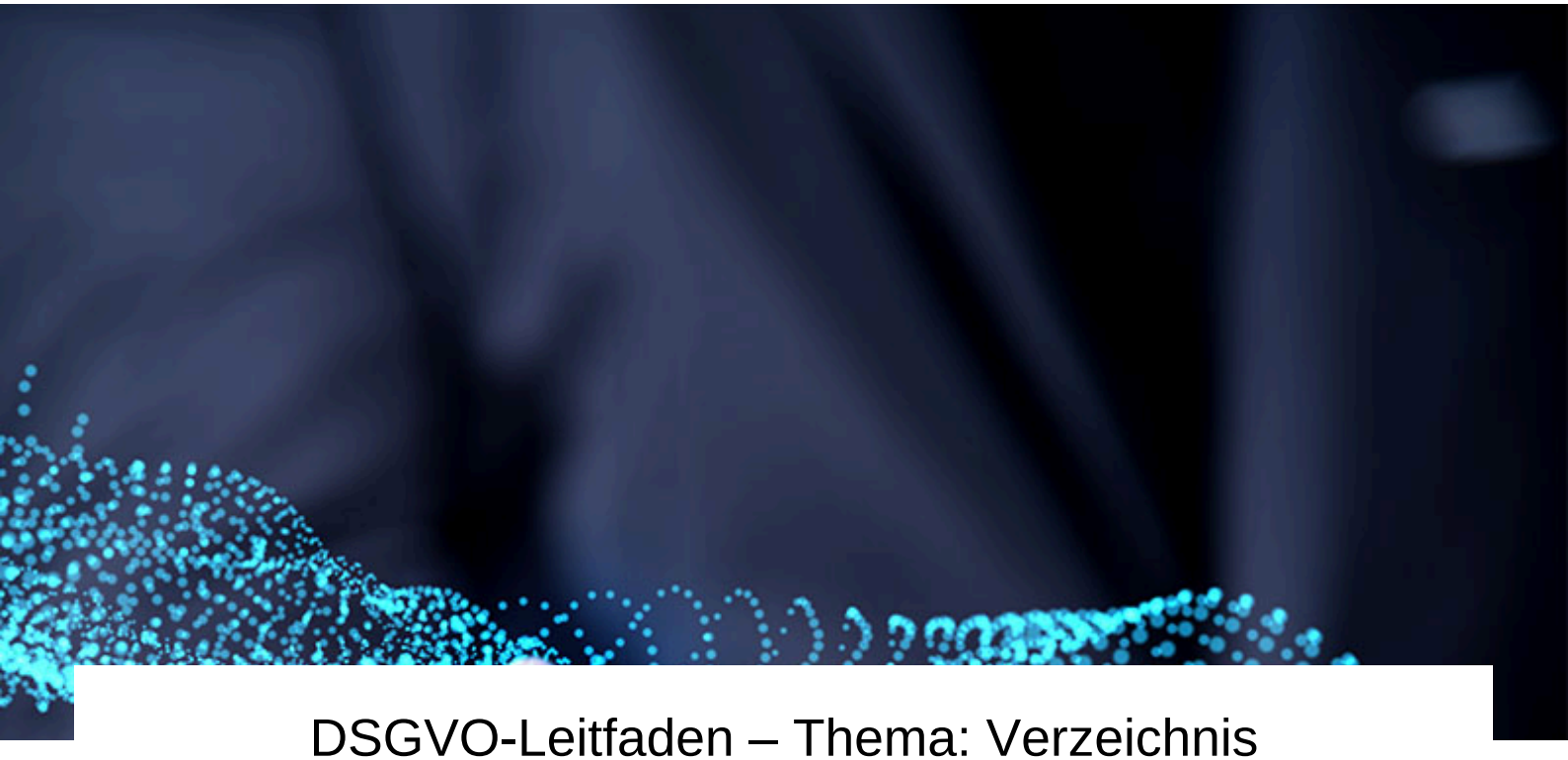
expertenReport



DSGVO-Leitfaden – Thema: Verzeichnis und Datenschutz-Folgenabschätzung

Seit mehr als 100 Tagen gilt nun die Datenschutz-Grundverordnung (DSGVO). Im zweiten Teil des DSGVO-Leitfadens für eine gute Compliance-Strategie geht es um das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) und zur Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

Verzeichnis von Verarbeitungstätigkeiten - Anlage ist Pflicht

Sebastian Karch, Rechtsanwalt / Gesellschaftsrecht, Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft

Das Verarbeitungsverzeichnis ist der Dreh- und Angelpunkt der Datenschutz-Compliance und es ist Pflicht ein solches anzulegen und vorzuhalten. Mit dem Verzeichnis ist nachzuweisen, wie der Datenschutz im Unternehmen beachtet wird. Es dient als Nachweis einer DSGVO-konformen Datenverarbeitung und der Vermeidung von Haftungsfällen. Die Pflicht zum Vorhalten eines Verarbeitungsverzeichnisses resultiert aus dem Grundsatz der Rechenschaftspflicht (Art. 5 DSGVO).

Das Verarbeitungsverzeichnis kann in schriftlicher oder elektronischer Form angelegt werden und muss folgende Pflichtangaben enthalten:

- Name und Kontaktdaten des Verantwortlichen und gegebenenfalls des Datenschutzbeauftragtens
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener und personenbezogener Daten
- Auskunft, ob die Daten in ein Drittland übermittelt werden
- Löschfristen
- Beschreibung der getroffenen TOMs

Vorlagen für Verarbeitungsverzeichnisse gibt es viele, da es keine formelle Vorgabe gibt. Zu empfehlen sind zum Beispiel die vom Bundesverband Deutscher Versicherungsmakler e.V. (BDVM).

Auf einem Vorblatt sind folgende Pflichtangaben auszufüllen:

- Angabe zum Verantwortlichen bzw. Auftragsverarbeiter
- Angaben zu gegebenenfalls einem weiteren gemeinsamen Verantwortlichen beziehungsweise Auftragsverarbeiter
- Angaben zum Vertreter des Verantwortlichen beziehungsweise des Auftragsverarbeiter
- Angaben zur Person des Datenschutzbeauftragten

Auf dem Hauptblatt, was am einfachsten per Excel-Tabelle erstellt wird, werden zu jedem einzelnen Verarbeitungsvorgang die Pflichtangaben des Art. 30 DSGVO abgearbeitet:

- Benennung des Verarbeitungsvorgangs
- Datum der Einführung und Datum der letzten Änderung
- Benennung der verantwortlichen Fachabteilung im Unternehmen
- Angabe des Zwecks der Verarbeitung, zum Beispiel Terminabsprache, Beratungsgespräch
- Rechtsgrundlage: regelmäßig der Maklervertrag: Art. 6 Abs. 1 Buchst. b) DSGVO oder eine Einwilligungserklärung des betroffenen: Art. 6 Abs. 1 Buchst. a) DSGVO
- Beschreibung der Kategorien betroffener Personen: zum Beispiel Interessenten, Kunden
- Beschreibung der Kategorien von personenbezogenen Daten
- Beschreibung der Kategorien von Empfängern, gegenüber denen, die personenbezogenen Daten offen gelegt werden: intern und extern
- Mitteilung, ob personenbezogene Daten in ein Drittland oder an eine internationale Organisation weitergegeben werden: Wenn ja, dann konkrete Benennung
- Fristen für die Löschung der Daten benennen
- Benennung der technisch- organisatorischen Schutzmaßnahmen (TOMs), die jeweils getroffen werden

Wenn im Unternehmen bereits ein Verfahrensverzeichnis nach BDSG existiert, so kann dies als Vorlage genommen werden und ist lediglich um die oben genannten neuen Anforderungen zu ergänzen.

Datenschutz-Folgenabschätzung (DSFA)

Die Datenschutz-Folgenabschätzung steigert das Niveau noch einmal. Dies entspricht der alten „Vorab-Analyse“. Es gilt also bei neuen automatisierten Prozessen vorab zu prüfen, ob der eigene Umgang mit den Daten des Betroffenen voraussichtlich ein hohes Risiko für dessen persönliche Rechte und Freiheiten darstellt. Als Konsequenz der Feststellung eines hohen Risikos ist dieses vor der Datenverarbeitung durch Maßnahmen zu minimieren oder die zuständige Aufsichtsbehörde zu konsultieren und mit dieser abzustimmen, wie Sie sich zu verhalten haben.

Als Anhaltspunkte, wann Sie von einer Pflicht zur DSFA ausgehen sollen, hat die „Artikel 29-Datenschutzgruppe“ (Gremium auf EU-Ebene) unter anderem folgende Fälle benannt:

- Verarbeitung sensibler Daten (zum Beispiel Gesundheitsdaten)
- umfangreiche Verarbeitungsvorgänge
- Verwendung neuer Technologien
- zusammengeführte oder kombinierte Datensätze
- Datentransfers außerhalb der Europäischen Union

Für gleichgelagerte Fälle reicht es aus, wenn nur einmal eine DSFA getroffen wird.

Als weitere Hilfestellung sollte eigentlich eine sogenannten „Black-List“ von Behördenseite zur Verfügung gestellt und in dieser die Prozesse bewertet werden, bei welchen eine Datenschutzfolgeabschätzung durchgeführt werden muss.

https://www.experten.de/2018/09/03/dsgvo-leitfaden-thema-der-datenschutzbeauftragte/

Bilder: (1) © kwanchaift / fotolia.com (2) © Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4945347/dsgvo-leitfaden-thema-verzeichnis-und-datenschutz-folgenabschaetzung/