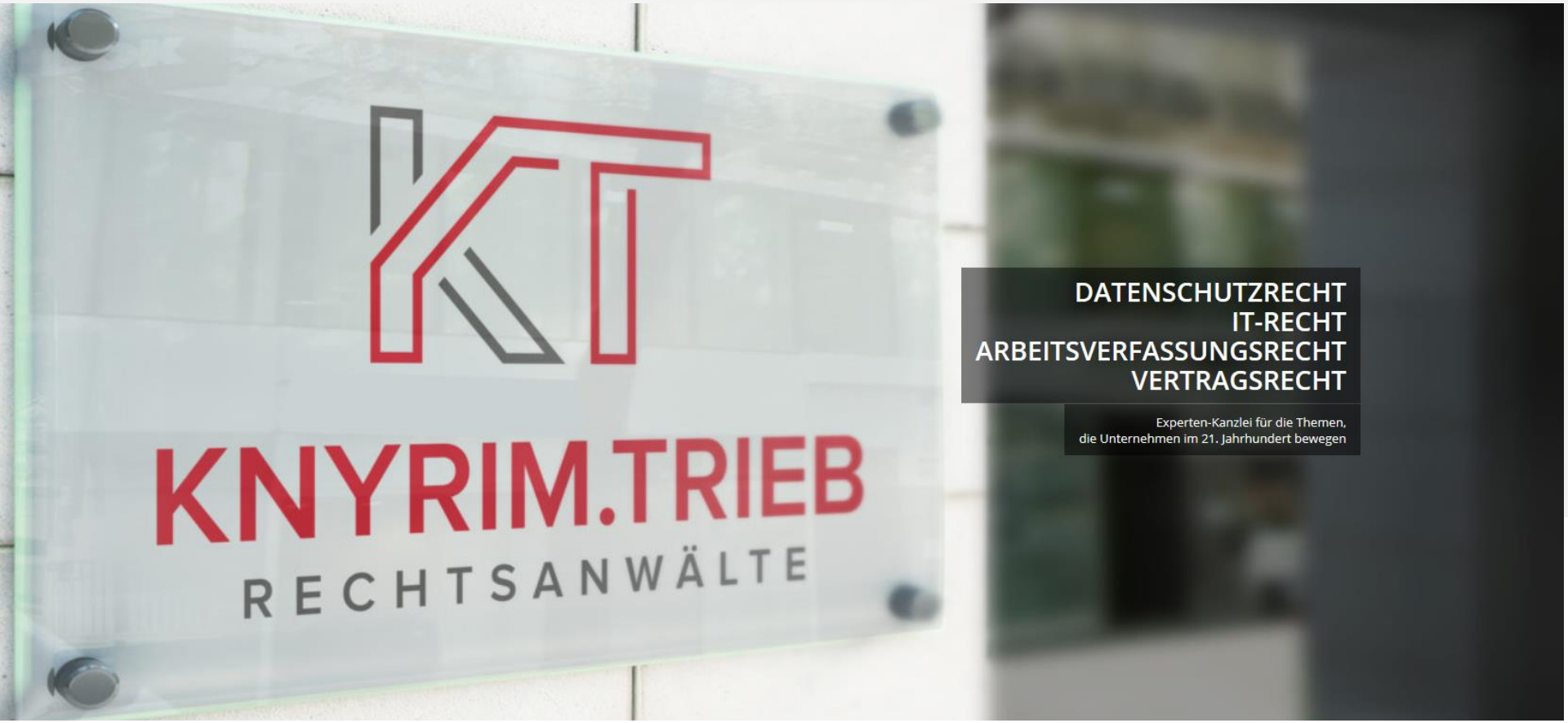
KNYRIM.TRIEB
RECHTSANWÄLTE
DATENSCHUTZRECHT
IT-RECHT
ARBEITSVERFASSUNGSRECHT
VERTRAGSRECHT
Experten-Kanzlei für die Themen,
die Unternehmen im 21. Jahrhundert bewegen

KNYRIM.TRIEB
RECHTSANWÄLTE

Informationsveranstaltung Smart Metering – Data Protection Impact Assessment

Dr. Gerald Trieb, LL.M
Knyrim Trieb Rechtsanwälte

Österreichs Energie, 14.9.2017

DPIA - Definition

- Data Protection Impact Assessment (DPIA oder DSFA) in Art 35f. DSGVO geregelt
- Begriff des DPIA wird in der DSGVO aber nicht definiert;
- Empfehlung der Kommission zur Durchführung eines DPIA für die Einführung von Smart Metern (2014/724/EU):

„Eine Datenschutzfolgenabschätzung ist ein systematisches Verfahren zur Bewertung der potentiellen Auswirkung von Risiken in Fällen, in denen Verarbeitungsvorgänge, die von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter oder von den im Namen des Verantwortlichen handelnden Auftragsverarbeitern durchzuführen sind, aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können.“

DPIA ist “datenschutzrechtliche Risikoanalyse”.

DPIA – Anwendungsbereich I

- DPIA ist immer dann vorab durchzuführen, wenn Art, Umfang, Umstände bzw. Zweck der Verarbeitung oder die Verwendung neuer Technologien voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge haben.
- Einbeziehung des Datenschutzbeauftragten (wenn benannt) erforderlich;
- Bei nachträglicher Änderung des Risikos: Überprüfung, ob zusätzliche Maßnahmen zur Einhaltung der Verarbeitung erforderlich sind
  → regelmäßige Überprüfung erforderlich;
- Wohl allgemein nur für Verarbeitungstätigkeiten durchzuführen, die nach dem 25.5.2018 in Betrieb gehen (dennoch müssen die Verarbeitungstätigkeiten mit der DSGVO in Einklang gebracht werden!)

DPIA – Anwendungsbereich II

- DPIA ist insbesondere durchzuführen bei :
  - automatischer, systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen (einschließlich „Profiling“), die einer Entscheidung zugrunde liegen, die Rechtswirkungen für die Personen entfaltet;
  - umfangreicher Verarbeitung sensibler Daten bzw. Daten über strafrechtliche Verurteilungen und Straftaten;
  - umfangreicher, systematischer Überwachung öffentlich zugänglichen Raums.
- Aufsichtsbehörde hat öffentlich bekannt zu geben, welche Datenanwendungen jedenfalls eines DPIA bedürfen und kann auch bekannt geben, bei welchen kein DPIA durchzuführen ist.

DPIA – Inhaltliche Anforderungen I

- **Mindestanforderungen** an ein DPIA**:**
  - Systematische Beschreibung der Anwendung und ihrer Zwecke (sinnvoll ist auch eine detaillierte graphische Darstellung der Datenflüsse) einschließlich einer Erforderlichkeits- und Verhältnismäßigkeitsprüfung;
  - Bewertung der Risiken für Rechte und Freiheiten der betroffenen Personen;
  - zur Bewältigung der Risiken geplante Abhilfemaßnahmen;
- **Empfohlener Inhalt** eines DPIA:
  - Beschreibung der Datensicherheitsmaßnahmen (Verschlüsselung, Zugriffskonzept, physischer Schutz, etc.);
  - Nach Datenkategorien gegliederte Liste einschließlich der Angabe ihrer Löschfristen;
  - Vollständige Liste von Datenempfängern samt Begründung für die Übermittlung;
  - vollständige Liste von Dienstleistern samt Angabe des Zwecks der Dienstleistung;
  - Sicherstellung der Einhaltung von Betroffenenrechten (einfache und sichere Verfügbarkeit aller aktuell gespeicherten Daten über einen Betroffenen);

DPIA – Inhaltliche Anforderungen II

- **Guidelines der „Art 29 WP“**
  - Internes Abstimmungsgremium der Datenschutzbehörden der EU
  - Empfehlungen und Richtlinien → rechtlich nicht bindend, jedoch faktischer Standard zur Orientierung für Verantwortliche, weil großer Einfluss auf Judikatur der Datenschutzbehörde gegeben.
  - Bislang umfangreichste Kommentierung von Art. 35 DS-GVO
  - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
    DPIA als ein zentrales Compliance-Dokument für risikoreiche Datenverarbeitungen

- Verantwortlicher verfügt über große Flexibilität, um Struktur und Form der DSFA selbst zu bestimmen

- Annex 1 – Verweis auf Beispiele bereits bestehender „Templates“ für die Durchführung von DPIAs.

- Annex 2 - Checklistenartige Zusammenstellung der Kriterien, der ein DPIA zu entsprechen hat.

DPIA - Beurteilungskriterien

1. Wird das Verhalten oder werden die Eigenschaften einer Person durch eine Datenverarbeitung bewertet?
2. Führt die Datenverarbeitung zu automatischen Entscheidungen gegenüber dem Datensubjekt?
3. Findet eine systematische Überwachung von Betroffenen statt?
4. Werden besondere Kategorien von personenbezogenen Daten im Sinne von Art. 9 DS-GVO oder andere sensible Daten verarbeitet?
5. Verfügt die Datenverarbeitung über einen großen Umfang, wobei hierbei die Anzahl der Betroffenen, die Anzahl der Einzeldaten, die Dauer der Datenverarbeitung und die geografische Ausdehnung der Datenverarbeitung berücksichtigt werden soll?
6. Werden Datensätze, die aus zwei oder mehr Quellen stammen, in einer Weise abgeglichen oder kombiniert, mit der die betroffene Person nicht rechnen muss?
7. Werden Daten von besonders schutzwürdigen Personen, wie etwa Kindern verarbeitet?
8. Wird eine neue Technologie oder ein besonders innovatives Verfahren verwendet? Erfolgt ein Datenexport von der EU in Drittstaaten? Wenn ja, wie ist das Datenschutzniveau der Empfängerländer zu beurteilen?
9. Führt die Datenverarbeitung dazu, dass Betroffene davon abgehalten werden, ihre Rechte auszuüben, einen Service in Anspruch zu nehmen oder einen Vertrag abzuschließen (Bonitätsanalyse im Vorfeld eines Vertragsabschlusses)?

- breiter Spielraum für **Interpretationsmöglichkeiten** (Umstände jedes Einzelfalls)
- Daumenregel, nach der ein hohes Risiko immer dann vorliegt, wenn **2 oder mehr der 10 Kriterien** gegeben sind

DPIA – Praxisbeispiele

Beispielsdatenverarbeitung	Mögliche relevante Kriterien	DSFA notwendig?
Ein Krankenhaus verarbeitet genetische Daten und Gesundheitsdaten der Patienten in einem "Hospital Information System“	• Sensible Daten • Besonders schutzwürdige Betroffene	ja
Die Nutzung eines Kamerasystems, um das Fahrverhalten auf einer Straße zu beobachten. Der Verantwortliche plant eine intelligentes Videoanalysesystem einzusetzen, das Fahrzeuge anhand von Nummernschildern identifizieren kann	• Systematische Überwachung von Betroffenen • Verwendung einer neuen Technologie bzw. eines besonders innovativen Verfahrens	ja
Ein Unternehmen beobachtet das Verhalten der Angestellten, insbesondere wird der Angestellte an seinem Arbeitsplatz und seine Internetnutzung beobachtet	• Systematische Überwachung von Betroffenen • Besonders schutzwürdige Betroffene	ja
Die Sammlung von öffentlichen Social Media Profilen, um Adressverzeichnisse für die Privatwirtschaft zu erstellen	• Automatisches Scoring/ automatische Bewertung • Besonders umfangreiche Datenverarbeitung	ja
Eine Online-Zeitschrift verwendet eine Mailing-Liste, um einen allgemeinen täglichen Newsletter an die Abonnenten zu versenden	• Kein Kriterium erfüllt	nicht notwendigerweise
Ein Webshop zeigt Werbung für Ersatzteile für Oldtimer auf Basis von begrenzten Nutzerprofilen, welche das Kaufverhalten auf dieser Webseite berücksichtigen	• Automatisches Scoring/ automatische Bewertung, aber nicht besonders umfangreich	nicht notwendigerweise

Vorherige Konsultation (Art 36 DSGVO)

- Wenn DPIA zeigt, dass eine Verarbeitung ohne Implementierung von Schutzmaßnahmen ein **hohes Risiko zur Folge hat und keine Abhilfemaßnahmen getroffen werden (können)**, ist die Aufsichtsbehörde vor der Verarbeitung zu konsultieren (Vorabgenehmigung);
- Dabei sind der Behörde folgende Informationen bekannt zu geben:
  - Angaben zu Zuständigkeiten innerhalb eines Konzerns – bei der Heranziehung von Auftragsverarbeitern;
  - Zwecke und Mittel der Verarbeitung;
  - ergriffene Schutzmaßnahmen;
  - Ggf. Kontaktdaten des Datenschutzbeauftragten;
  - Ergebnis des DPIA;
  - „**alle** sonstigen von der Aufsichtsbehörde **angeforderten Informationen**“.

Bei hohem Risiko, Pflicht zur Konsultation der Aufsichtbehörden!

Vorherige Konsultation (Art 36 DSGVO)

- Aufsichtsbehörde hat dann bis zu **8 Wochen** (max. 14 Wochen bei komplexen Fällen) Zeit, Empfehlungen zu erteilen bzw. ihre Befugnisse nach Art 58 DSGVO auszuüben
  - Auflagen erteilen;
  - Verarbeitung verbieten;
  - Datenübermittlung in ein Drittland aussetzen;
  - Geldbußen verhängen;
- Bei Verarbeitungen zur Erfüllung von Aufgaben des öffentlichen Interesses (insbes. im Gesundheitsbereich) kann eine vorherige Konsultation durch die Aufsichtsbehörde durch nationale Vorschriften vorgesehen werden;

Beratende und kontrollierende Rolle der Aufsichtsbehörde im Vorfeld der Aufnahme von mit Risiken verbundenen Datenanwendungen!

Datenschutz-Anpassungsgesetz 2018 I

- Funktion: Anpassung des österreichischen Datenschutzgesetz 2000 an die DSGVO
- Beschluss im Nationalrat im Juni ohne Verfassungsmehrheit, Kundmachung im BGBl im Juli, In-Krafttreten mit 25.5.2018
- **Daten zu juristischen Personen in Österreich wohl auch nach 25.5.2018 geschützt, weil Grundrecht auf Datenschutz in § 1 DSG 2000 (= § 1 DSG „neu“) nicht angepasst werden konnte.**
- Laut BKA kein „Betriebsunfall“, sondern bewusste Ausweitung des Schutzes gegenüber der DSGVO
- Wirft zahlreiche Fragen auf, wie etwa:
  - Was sind personenbezogene Daten zu juristischen Personen (Definition in DSGVO → lediglich Daten natürlicher Personen sind geschützt)
  - Welche Anforderungen sind an die Verarbeitung personenbezogener Daten zu stellen? Jene der DSGVO oder „nur“ jene des DSG „neu“?

Datenschutz-Anpassungsgesetz 2018 II

Weitere wichtige Bestimmungen (Auswahl):

- Verpflichtung auf das Datengeheimnis bleibt in § 6 DSG neu erhalten;
- Verarbeitung von Daten im Beschäftigungskontext (ArbVG ist eine Bestimmung iSd Art 88 DSGVO – Pflichten laut ArbVG unterfallen der Strafdrohung der DSGVO!)
- Kennzeichnungspflicht bei Bilddatenverarbeitung: Verantwortliche hat eindeutig hervorzugehen!
- Betroffene können sich zur Durchsetzung Ihrer Rechte von Datenschutzorganisationen (auch vor Gericht?) vertreten lassen.
- Strafen auch nach DSGVO primär über die juristische Person (das Unternehmen) zu verhängen; von der Bestrafung der nach § 9 VStG Verantwortlichen ist abzusehen, wenn schon juristische Person bestraft wurde und keine besonderen Umstände des Einzelfalls entgegenstehen;
- Strafdrohung für Verletzungen von Verpflichtungen des DSG neu EUR 50.000,00.

Vielen Dank für die Aufmerksamkeit!

Fragen?

RA Dr. Gerald Trieb, LL.M,

Knyrim Trieb Rechtsanwälte OG

1060 Wien, Mariahilfer Straße 89a

T +43/1/9093070, F +43/1/9093639
E gt@kt.at, W www.kt.at