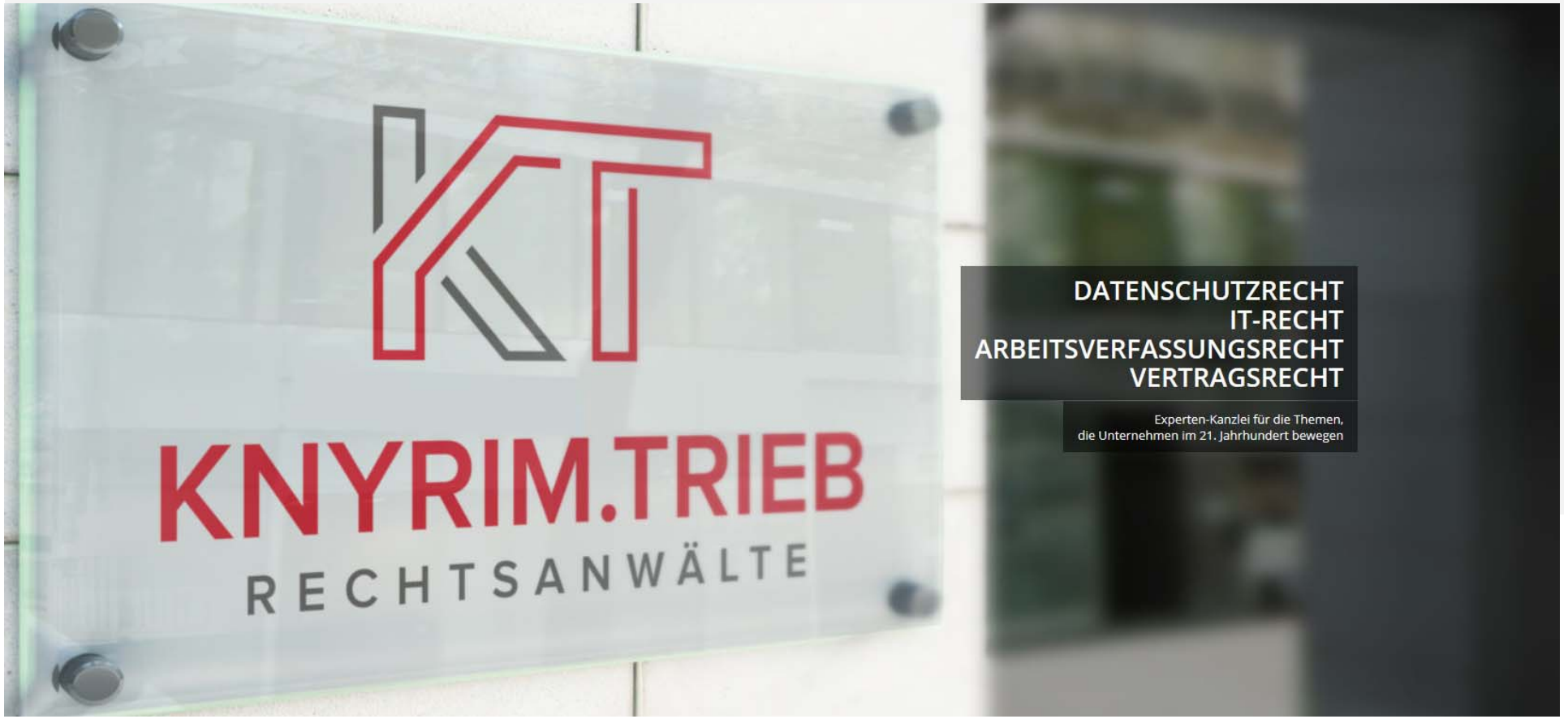
KNYRIM.TRIEB
RECHTSANWÄLTE



KNYRIM.TRIEB
RECHTSANWÄLTE

Datenschutzrechtliche Rahmenbedingungen für ein DPIA – aktuelle Entwicklungen in Österreich und in Europa

Dr. Gerald Trieb, LL.M.

Rechtsanwalt und Partner
Knyrim Trieb Rechtsanwälte, Wien

Österreichs Energie, Informationsveranstaltung Marktprozesse – Data Protection Impact Assessment (DPIA), 7. Juni 2018

KNYRIM.TRIEB RECHTSANWÄLTE

Agenda

1. **Datenschutz-Folgenabschätzung (DSFA = DPIA) – Allgemeines zur „Wiederholung“**
2. Prüfschema zur Frage der Durchführungspflicht
3. Ausnahmen von der DSFA – „White-List“
4. Verarbeitungstätigkeiten mit zwingender DSFA – „Black-List“
5. Ausgewählte Punkte des Datenschutz-Deregulierungsgesetzes

Datenschutz-Folgenabschätzung (DSFA = DPIA) (Art 35 DSGVO)

- Hintergrund der Einführung der DSFA ist der Ersatz der Meldepflicht (insb.: Vorabkontrolle) durch die Datenschutzbehörde (vgl. ErwGr 89 ff DSGVO);

- DSFA 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 erforderlich (wenn ein solcher bestellt ist) → **Durchführung der DSFA ist nach der DSGVO keine Pflicht des Datenschutzbeauftragten!**

- Bei Änderung des Risikos: Überprüfung der Verarbeitung, ob sie gemäß der DSFA durchgeführt wird;

Verantwortliche haben eine DSFA bei hohem Risiko für die Rechte und Freiheiten natürlicher Personen vorab durchzuführen!

Datenschutz-Folgenabschätzung (DSFA = DPIA) (Art 35 DSGVO)

- DSFA 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.

Eine DSFA ist bei automationsunterstützter Entscheidung und bei groß angelegter Verarbeitung „heikler“ Daten erforderlich.

Datenschutz-Folgenabschätzung (DSFA = DPIA) (Art 35 DSGVO)

- Die Aufsichtsbehörde **hat** bekanntzugeben, welche Verarbeitungen jedenfalls einer DSFA bedürfen

  → „**Black-List**“

  - Diese ist in Österreich noch **ausständig,** wird aber **für Herbst 2018 erwartet!**
  - Die Liste ist **nicht abschließend**, sondern **beispielhaft!**

- Die Aufsichtsbehörde **kann** auch bekanntgeben, bei welchen Verarbeitungen keine DSFA durchzuführen ist

  → **„White-List“**

  - Diese **liegt bereits vor**

Agenda

1. Datenschutz-Folgenabschätzung (DSFA = DPIA) – Allgemeines zur „Wiederholung“
2. **Prüfschema zur Frage der Durchführungspflicht**
3. Ausnahmen von der DSFA – „White-List“
4. Verarbeitungstätigkeiten mit zwingender DSFA – „Black-List“
5. Ausgewählte Punkte des Datenschutz-Deregulierungsgesetzes

Pflicht zur Durchführung einer DSFA – Prüfschema

Vorfrage: Verarbeitungstätigkeit steht auf der „Black-List“ der österreichischen Datenschutzbehörde (**Zukunft!**)

→ **DSFA erforderlich**

1. Verarbeitung wurde nach Vorabkontrolle im DVR registriert und unverändert betrieben (siehe § 1 Abs 2 Z 1 Datenschutz-Folgenabschätzung-Ausnahmenverordnung – „DSFA-AV“)

→ **keine DSFA erforderlich**

   a. Datenanwendung (=Verarbeitungstätigkeit) war vorabkontrollpflichtig nach DSG 2000,

   b. wurde erfolgreich im DVR im Verfahren der Vorabkontrolle registriert, und

   c. wurde seither keiner wesentlichen Veränderung unterzogen.

Pflicht zur Durchführung einer DSFA – Prüfschema

2. Verarbeitung entspricht einer ausdrücklich in der DSFA-AV angeführten Datenanwendung oder einer Standard- oder Musteranwendung (siehe § 1 Abs 1 und § 1 Abs 2 Z 2 DSFA-AV)

→ keine DSFA erforderlich

a. DSB hat sich auch in der Anlage an Standard- und Musteranwendungen orientiert, daher

b. Anwendbarkeit allenfalls nur soweit gegeben, als Datenanwendung unter diese Verordnung gefallen ist.

c. Einschränkungen in der Anlage sind zu beachten!

Pflicht zur Durchführung einer DSFA – Prüfschema

3. Verarbeitung führt zu **keinem hohen Risiko** für die Rechte und Freiheiten der betroffenen Personen z.B.: durch Prüfung anhand des Kriterienkatalogs der Richtlinien der Art 29 WP

→ keine DSFA erforderlich

a. Richtlinien zur DSFA der Art 29 WP enthalten Kriterienkatalog für typische hohe Risiken für Rechte und Freiheiten

b. Wenn zwei Kriterien erfüllt sind, ist von Durchführungspflicht auszugehen

c. Durchführung dient auch Dokumentationszweck

Agenda

1. Datenschutz-Folgenabschätzung (DSFA = DPIA) – Allgemeines zur „Wiederholung“
2. Prüfschema zur Frage der Durchführungspflicht
3. **Ausnahmen von der DSFA – „White-List“**
4. Verarbeitungstätigkeiten mit zwingender DSFA – „Black-List“
5. Ausgewählte Punkte des Datenschutz-Deregulierungsgesetzes

Verordnung über die Ausnahmen von der DSFA („DSFA-AV“ = „White-List“) I

- **Enthält Ausnahmen von der DSFA-Pflicht**
- **Auszug aus dem Inhalt des Anhangs:**
  - Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
  - Personalverwaltung
  - Mitgliederverwaltung
  - Kundenbetreuung und Marketing für eigene Zwecke
  - Sach- und Inventarverwaltung
  - Zugriffsverwaltung für EDV-Systeme
  - Zutrittskontrollsysteme

Verordnung über die Ausnahmen von der DSFA („DSFA-AV“ = „White-List“) II

- Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)
- Bild- und Akustikdatenverarbeitung in Echtzeit
- Bild- und Akustikverarbeitungen zu Dokumentationszwecken
- Archivierung, wissenschaftliche Forschung und Statistik
- Förderverwaltung
- Aktenverwaltung (Büroautomation) und Verfahrensführung
- Organisation von Veranstaltungen
- Preise und Ehrungen

Agenda

1. Datenschutz-Folgenabschätzung (DSFA = DPIA) – Allgemeines zur „Wiederholung“
2. Prüfschema zur Frage der Durchführungspflicht
3. Ausnahmen von der DSFA – „White-List“
4. **Verarbeitungstätigkeiten mit zwingender DSFA – „Black-List“**
5. Ausgewählte Punkte des Datenschutz-Deregulierungsgesetzes

Verarbeitungstätigkeiten mit zwingender DSFA – „Black-List“

- Laut Datenschutzbehörde ist eine Black-List in Vorbereitung und für Herbst 2018 zu erwarten
- Andere Behörden in Europa haben bereits Black-Lists veröffentlicht
- Deutsche Datenschutzbehörden haben sich auf 17 Verarbeitungstätigkeiten verständigt, bei denen eine DSFA erforderlich erscheint
- Diese Listen ausländischer Behörden können Anhaltspunkte für österreichische Unternehmen liefern
- Maßgeblich ist aber die **Black-List der österreichischen Datenschutzbehörde**

Agenda

1. Datenschutz-Folgenabschätzung (DSFA = DPIA) – Allgemeines zur „Wiederholung“
2. Prüfschema zur Frage der Durchführungspflicht
3. Ausnahmen von der DSFA – „White-List“
4. Verarbeitungstätigkeiten mit zwingender DSFA – „Black-List“
5. **Ausgewählte Punkte des Datenschutz-Deregulierungsgesetzes**

Ausgewählte Punkte des Datenschutz-Deregulierungsgesetzes

1. (Keine) Änderung der Verfassungsbestimmungen (Schutz von Daten juristischer Personen?)
2. Einschränkungen des Auskunftsrechts (?)
3. Verwarnen statt Strafen durch die Behörde (?)
4. Haftungserleichterung für zur Vertretung nach außen befugte Personen
5. Keine Möglichkeit für Datenschutzorganisationen, Schadenersatz für Betroffene einzuklagen
6. Bestimmungen des ArbVG sind (doch) keine Bestimmungen iSd Art 88 DSGVO – Konsequenz?
7. Keine Verhältnismäßigkeitsprüfung bei der Videoüberwachung?

KNYRIM.TRIEB
RECHTSANWÄLTE

Vielen Dank für die Aufmerksamkeit!

Fragen?

RA Dr. Gerald Trieb, LL.M,

Knyrim Trieb Rechtsanwälte OG

1060 Wien, Mariahilfer Straße 89A

Tel. +43/1/9093070, Fax +43/1/9093639,
E-Mail gt@kt.at; www.kt.at