EU-Datenschutz-Grundverordnung

Herausforderung für Unternehmen

Axel Vogelsang

Datenschutzbeauftragter & IT-Consultant

KÄMMER CONSULTING

Internet-Links

- EU-DSGVO, Erwägungsgründe und BDSG (neu):
  - https://dsgvo-gesetz.de/
- Hinweise und Muster Verfahrensverzeichnis:
  - https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeicnis_und_verfahrensregister_nach_bdsg/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html
- Hinweise und Muster Videoüberwachung
  - https://www.lfd.niedersachsen.de/startseite/dsgvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html
- Kurzpapiere der Datenschutzkonferenz zur DSGVO
  - https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html

KÄMMER CONSULTING

EU-Datenschutz-Grundverordnung

- Veröffentlichung im EU-Amtsblatt am 4. Mai 2016
- Anzuwenden ab dem 25. Mai 2018
- gilt direkt für alle Unternehmen innerhalb der EU

KÄMMER CONSULTING

Datenschutzanpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)

- Enthält das Nachfolgegesetz zum BDSG
- Regelt Öffnungsklauseln der EU-DSGVO
- Zustimmung Bundesrat am 12.05.2017
- Tritt zum 25.05.2018 in Kraft und löst dann BDSG (alt) ab

Auswirkungen auf andere Gesetze

- Anpassungen in verschiedenen Gesetzen notwendig: TKG, TMG, UWG, SGB usw.
- Ersatz der EU-ePrivacy-Richtlinie durch EU-ePrivacy-Verordnung

Personenbezogene Daten

- Personendaten (z. B. Name, Geburtsdatum, Alter …)
- Adressdaten (z. B. Straße, PLZ, Ort, Postfach …)
- Kfz-Kennzeichen, Sozialversicherungs-Nr., Kunden-Nr.
- GPS-Daten (Kfz Tracking), Zutrittsprotokolle
- Ereignisprotokoll Computersysteme (An- und Abmeldung)
- IP-Adressen (Protokoll Web-Server, Firewall)
- Bankdaten, Kreditkartendaten
- Videoaufzeichnung

Dokumentationspflichten

- Rechenschaftspflicht (Art. 5 Abs. 2)
- Beweislastumkehr (Art. 82 Abs. 2)
- Nachweis der Wirksamkeit von Maßnahmen (Art. 32 Abs. 1 lit. d)
- kein Verfahrensverzeichnis → Bußgeldtatbestand
- Dokumentation Grundlage für Arbeit des DSB

Art. 5 Abs.2; Art. 82 Abs. 2; Art. 32 Abs. 1 lit. d DSGVO

KÄMMER CONSULTING

Verzeichnis von Verarbeitungstätigkeiten

- Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen
- Aufbau:
  a. Allgemeine Angaben zum Verantwortlichen
  b. Beschreibung der einzelnen Verfahren
  c. Übergreifende Maßnahmen / IT-Sicherheitskonzept
- Nähere Informationen und Muster auf den Seiten der Landesdatenschutzbeauftragten

Verzeichnis von Verarbeitungstätigkeiten

Allgemeine Angaben

Name und Kontaktdaten

- des Verantwortlichen
- ggf. des Datenschutzbeauftragten

Verzeichnis von Verarbeitungstätigkeiten

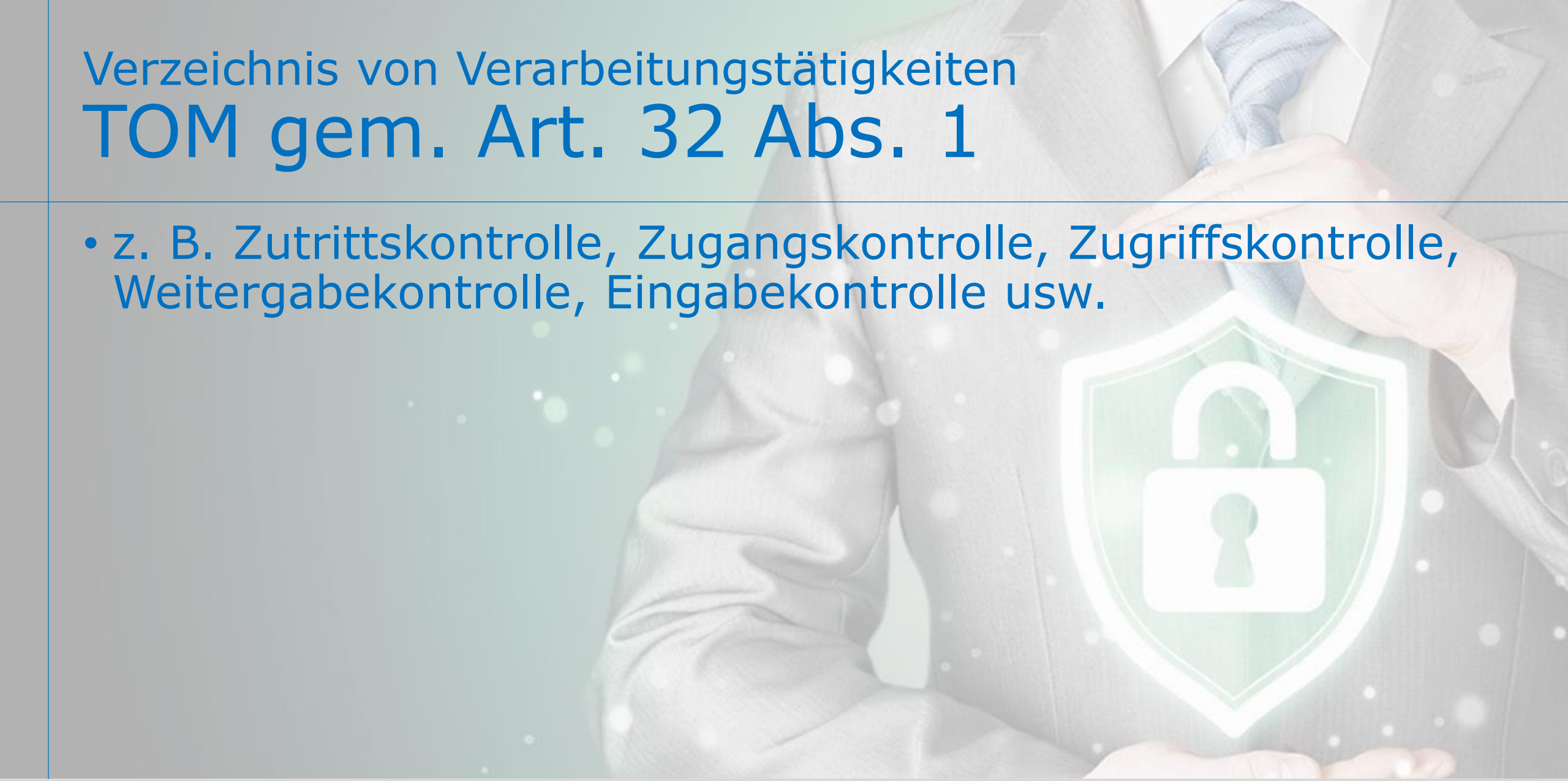
Beschreibung Verfahren

- Zweck der Verbeitung
- Rechtsgrundlage der Verarbeitung (Art. 6 DSGVO)
- Kategorien betroffener Personen und pbDaten
- Kategorien von Empfängern
- ggf. Übermittlung in Drittländer
- Löschfristen

Verzeichnis von Verarbeitungstätigkeiten

TOM gem. Art. 32 Abs. 1

- z. B. Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle usw.



Verzeichnis der Verarbeitungstätigkeiten
Beispiele

- Auftragsabwicklung
- Personalverwaltung
- Zeiterfassung
- Personalabrechnung
- Personalbeschaffung
- E-Mail
- Einkauf

KÄMMER CONSULTING

Privacy-by-Design

- Datenschutz durch Technikgestaltung
- Berücksichtigung: Stand der Technik, Implementierungs-kosten, Zwecke der Verarbeitung …
- z. B. Pseudonymisierung, Anonymisierung

Privacy-by-Default

- Datenschutz durch datenschutzfreundliche Voreinstellung
- geeignete TOM, die sicherstellen, dass durch Voreinstellungen nur die für den bestimmten Verarbeitungszweck benötigten pbDaten verarbeitet werden

Betroffenenrechte

- deutlich umfangreichere Informationspflichten und Auskunftsrechte
- Neue Rechte:
  - Recht auf „Vergessenwerden“
  - Recht auf Datenübertragbarkeit
- Verbindliche Reaktionszeit

Betroffenenrechte - Informationspflicht

- Kontaktdaten des für die Verarbeitung Verantwortlichen
- Falls vorhanden: Kontaktdaten Datenschutzbeauftragter
- Zweck der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- Ggfs. Empfänger oder Kategorien von Empfängern

Betroffenenrechte - Informationspflicht

- ggfs. Drittländer, an die Daten übermittelt werden
- Speicherdauer der Daten
- Hinweis auf Recht auf *Auskunft*, *Berichtigung*, *Löschung*, *Einschränkung der Verarbeitung*, *Widerspruchsrecht* sowie auf *Datenübertragbarkeit*
- Hinweis auf Widerrufsmöglichkeit

Betroffenenrechte - Informationspflicht

- Hinweis,
  - ob die Bereitstellung der pbDaten gesetzlich oder vertraglich vorgeschrieben ist
  - oder ob die Bereitstellung für einen Vertragsabschluss erforderlich ist
  - ob die betroffene Person verpflichtet ist, die Daten bereit zu stellen
  - welche Folgen die Nichtbereitstellung hätte
  - auf das Beschwerderecht bei der Aufsichtsbehörde

- Bei automatisierten Einzelfallentscheidungen
  - Aussagekräftige Informationen über die Logik
  - Tragweite und Auswirkungen der Verarbeitung für die betroffene Person

Betroffenenrecht – Informationspflicht

Wann muss informiert werden

- Werden die Daten bei der betroffenen Person erhoben:

Zum Zeitpunkt der Erhebung

Betroffenenrecht – Informationspflicht

Wann muss informiert werden

- Werden die Daten **nicht** bei der betroffenen Person erhoben:

Innerhalb einer angemessenen Frist, längstens ein Monat

Spätestens zum Zeitpunkt der ersten Mitteilung an die betroffene Person

Art. 14 Abs. 3 DSGVO

KÄMMER CONSULTING

Videoüberwachung

- nur zulässig zur Wahrnehmung des Hausrechts oder
- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
- Name und Kontaktdaten des Verantwortlichen müssen zum frühestmöglichen Zeitpunkt erkennbar gemacht werden
- Daten sind unverzüglich zu löschen, wenn zur Erfüllung des Zweckes nicht mehr erforderlich

Videoüberwachung

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung[1]

Achtung

Videoüberwachung!

Weitere Informationen erhalten Sie:
- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

[1] *Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.*

KÄMMER CONSULTING

Bußgeld

- wirksam, verhältnismäßig und abschreckend
- deutlich höher
  - bis 10.000.000 € oder 2 % des weltweiten Jahresumsatzes
  - bis 20.000.000 € oder 4 % des weltweiten Jahresumsatzes
- Neue Bußgeldtatbestände
  - Verstoß gegen Dokumentationspflichten
  - Privacy-by-Design; Privacy-by-Default

Datenschutzverstöße

- Meldung an Aufsichtsbehörde, wenn Risiko für die Rechte und Freiheiten natürlicher Personen besteht
- Meldung binnen 72 Stunden
- Inhalt der Meldung
  - Beschreibung der Art der Verletzung mit Angabe der Kategorien und ungefähren Anzahl der betroffenen Personen und Datensätze
  - Name und Kontaktdaten des DSB
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der Maßnahmen zur Behebung der Verletzung

Datenschutzverstöße

- unverzügliche Benachrichtigung der betroffenen Personen bei hohem Risiko für Rechte und Freiheiten
- nicht erforderlich, wenn
  - geeignete TOM getroffen wurden um unberechtigten Zugriff zu unterbinden (z. B. Verschlüsselung)
  - durch geeignete Maßnahmen sichergestellt ist, dass das hohe Risiko nicht mehr besteht
  - unverhältnismäßiger Aufwand. In dem Fall öffentliche Bekanntmachung

Was ist zu tun?

- Verfahrensverzeichnisse erstellen/aktualisieren
- AGBs / Datenschutzerklärungen prüfen
- bestehende Einwilligungen Betroffener prüfen
- Prozess zur Wahrung der Betroffenenrechte implementieren
- Prozess zur Meldung von Datenschutzverstößen implementieren

KÄMMER CONSULTING

Was ist zu tun?

- Datenschutz Folgeabschätzung durchführen
- Umsetzung „Privacy-by-Design“ / „Privacy-by-Default“
- Verträge zur Auftragsdatenverarbeitung prüfen
- Dokumentation prüfen / aktualisieren

KÄMMER CONSULTING

Vielen Dank für Ihre Aufmerksamkeit

Axel Vogelsang
Datenschutzbeauftragter

Tel: 0531.702249-0
datenschutz@kaemmer-consulting.de
www.kaemmer-consulting.de