EU-DATENSCHUTZ-GRUNDVERORDNUNG UND CYBERSECURITY

Rechtsanwältin Julia Dönch, M.A.

BDO LEGAL

VERARBEITUNG PERSONENBEZOGENE DATEN ALS ANKNÜPFUNGSPUNKT

- Art. 4 Nr. 1 DSGVO

  „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

- Art. 4 Nr. 2 DSGVO

  „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen

HAFTUNG UND SANKTIONEN

Haftung

Jede Person, der wegen eines Verstosses gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Sanktionen

Bei Verstößen gegen bestimmte Bestimmungen werden Geldbußen von bis zu EUR 20 Mio. oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

BDO LEGAL

MELDUNG VON DATENSCHUTZVORFÄLLEN

Was sind Datenschutzvorfälle?

- Unrechtmäßige Kenntniserlangung von personenbezogenen Daten durch Unbefugte (z.B. falsche Faxadresse oder E-Mail-Weiterleitung, Übermittlung von Daten oder Zugriffsrechte auf Daten an bzw. bei Unternehmen außerhalb der EU ohne Rechtsgrundlage/Garantie für angemessenes Datenschutzniveau)
- Abhandenkommen von technischem Equipment (Smartphone, Laptop, USB-Stick etc.)
- Zweckfremde Verarbeitung von personenbezogenen Daten
- Verstoß gegen Grundsätze der Datenverarbeitung (z.B. Zugriffskreis nicht nach Need to know-Prinzip, Vorliegen unrichtiger oder unnötiger Daten, Überschreiten der Speicherzeit)
- Technische oder organisatorische Missstände (Prozess der Datenverarbeitung anfällig, Systeme unzureichend)
- etc.

MELDUNG VON DATENSCHUTZVORFÄLLEN

Was ist nach der DSGVO zu tun bei einem Datenschutzvorfall? (1/4)

1. Einschätzung wie hoch die Risiken für die Schutzrechte des Betroffenen sind
2. Ergreifen von Abhilfemaßnahmen
3. Dokumentation der Verletzung des Schutzes personenbezogener Daten einschließlich aller Fakten und Abhilfemaßnahmen und Zuleitung an Datenschutzbeauftragten
   - Beschreibung der Art der Schutzverletzung personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
   - Name und Kontaktdaten des Datenschutzbeauftragten
   - Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
   - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggfs. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

MELDUNG VON DATENSCHUTZVORFÄLLEN

Was ist nach der DSGVO zu tun bei einem Datenschutzvorfall? (2/4)

Meldung an die Aufsichtsbehörde durch den Datenschutzbeauftragten, wenn die Verletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt

- Unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung, andernfalls Begründung für Verzögerung
- Bereitstellung der Informationen auch schrittweise, aber ohne unangemessene weitere Verzögerung möglich

MELDUNG VON DATENSCHUTZVORFÄLLEN

Was ist nach der DSGVO zu tun bei einem Datenschutzvorfall? (3/4)

Unverzügliche Benachrichtigung des von der Verletzung Betroffenen durch Datenschutzbeauftragten, wenn voraussichtlich hohes Risiko für seine persönlichen Rechte und Freiheiten

- Art der Verletzung des Schutzes personenbezogener Daten
- Name und Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggfs. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

MELDUNG VON DATENSCHUTZVORFÄLLEN

Was ist nach der DSGVO zu tun bei einem Datenschutzvorfall? (4/4)

Keine Benachrichtigung des Betroffenen, wenn

- geeignete technische und organisatorische Sicherheitsvorkehrungen auf die personenbezogenen Daten angewandt wurden (z.B. Verschlüsselung),
- nachfolgend Maßnahmen ergriffen wurden, so dass kein hohes Risiko für die Rechte und Freiheiten der betroffenen Person mehr besteht oder
- die Benachrichtigung einen unverhältnismäßigen Aufwand darstellt (dann aber öffentliche Bekanntmachung oder ähnliche Maßnahme zur Information)

TECHNISCHER DATENSCHUTZ NACH ART. 32 DSGVO

Welche Anforderungen an den technischen Datenschutz ergeben sich für ein Unternehmen?

Was regelt Art. 32 DSGVO?

- Regelung verschiedener technischer und organisatorischer Maßnahmen (sog. „TOMs“), zum Schutz personenbezogener Daten
- Nicht abschließend aufgeführt: verschiedene Methoden des Datenschutzes, z.B. Pseudonymisierung der Daten einer Person

➢ Gesetzgeber lässt gewissen Spielraum zur Umsetzung der jeweiligen Maßnahmen und weiterführender Schutzmechanismen (Stand der Technik, die Gefahr für einen Missbrauch der jeweiligen Daten, die Schwere der Folgen, der Zweck der Verarbeitung, die Kosten etc.)

Maßnahmen, die nach Art. 32 DSGVO getroffen werden sollten

➢ Abs. 1 DSGVO: abstrakte Maßnahmen, die ein ausreichendes Schutzniveau für personenbezogene Daten herstellen

➢ Abs. 2 DSGVO: Risikoabwägung (Angemessenheit der Schutzmaßnahmen); fraglich sind Risiken für Rechte und Freiheiten natürlicher Personen; z.B.:

- wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung führen kann,
- wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, verarbeitet werden oder
- wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

TECHNISCHER DATENSCHUTZ NACH ART. 32 DSGVO

Welche Anforderungen an den technischen Datenschutz ergeben sich für ein Unternehmen?

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
  Beispiele: Passwortvergabe, SSL-Zertifikate, VPN
- Dauerhafte Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung
  Beispiele: Regelmäßige IT-Checks, Nutzung der neusten Technologien, Zugriff nur durch autorisiertes Personal, Berechtigungskonzept
- Schnelle Wiederherstellungsmöglichkeit der personenbezogenen Daten bei einem physischen oder technischen Zwischenfall
  Beispiele: regelmäßige Backups, Nutzung einer Cloud, Zugriff auf die Daten von verschiedenen Geräten aus
- Regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen
  Beispiel: Erstellung von jährlichen Tätigkeitsberichten, Dokumentation der Auftragsverarbeitungsverhältnissen, Prüfung des IT-Sicherheitskonzepts, regelmäßige Passwortänderungen

„RISIKOBASIERTER ANSATZ“ DER DSGVO

Erwägungsgrund (EG) 75 DSGVO enthält Auflistung von Risiken, die bei den durch Art. 24 Abs. 1 DSGVO vorgeschriebenen technischen und organisatorischen Maßnahmen des Datenschutzes zu beachten sind:

„Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.”

BDO LEGAL

„RISIKOBASIERTER ANSATZ“ DER DSGVO

- Analyse der Risiken aus EG 75 DSGVO
  - Risikokatalog nicht nur für Maßnahmen gemäß Art. 24 Abs. 1 DSGVO, sondern auch bei anderen Abwägungen und Abschätzungen
  - Abwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO („berechtigte Interessen“)
  - ebenso alle anderen Passagen in DSGVO, in denen auf „Interessen, Grundrechte und Grundfreiheiten“ der Betroffenen abgestellt wird

- Objektiver Maßstab (EG 76 Satz 2 DSGVO)

“Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.”

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Wann ist eine Datenschutz-Folgenabschätzung durchzuführen?

Art. 35 Abs. 1 S. 1 DSGVO: Hat eine Form der Verarbeitung (…) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte (Profiling)
- umfangreiche Verarbeitung besonderer Kategorien
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Was ist bei der Datenschutz-Folgenabschätzung zu prüfen?

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen,
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- die geplanten Abhilfemaßnahmen

IHRE ANSPRECHPARTNER

BDO Legal Rechtsanwaltsgesellschaft mbH

Julia Dönch, M.A.
Rechtsanwältin
Georg-Glock-Straße 8
40474 Düsseldorf
Telefon: +49 211 1371-326
julia.doench@bdolegal.de

BDO Legal Rechtsanwaltsgesellschaft mbH

Anna Kerstin Krüger
Rechtsanwältin
Georg-Glock-Straße 8
40474 Düsseldorf
Telefon: +49 211 1371-186
annakerstin.krueger@bdolegal.de

BDO Legal Rechtsanwaltsgesellschaft mbH

Stephan Wetzel
Rechtsanwalt
Georg-Glock-Straße 8
40474 Düsseldorf
Telefon: +49 211 1371-519
stephan.wetzel@bdolegal.de