BREHM & v. MOERS

2. CEMA Online IT.special: EU-Datenschutz-Grundverordnung

Anforderungen an Datenschutz-Compliance insbesondere
bei der Zusammenarbeit mit Großunternehmen

Paul Nottarp, LL.M.
Rechtsanwalt

BvM more than legal

Pflichten aus der DSGVO

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- Nach Art. 30 muss der Verantwortliche ein umfassendes Verzeichnis aller Verarbeitungstätigkeiten führen (schriftlich oder in elektronischer Form)
- Instrument zur Umsetzung der Dokumentationspflichten nach Art. 24 Abs. 1
- Verarbeitungsverzeichnis muss auf Anforderung der Aufsichtsbehörden vorgelegt werden
- Erforderliche Angaben sind in Art. 30 geregelt

➢ **Ausnahme:** Unternehmen mit weniger als 250 Mitarbeitern sind nach Art. 30 Abs. 5 dann von der Pflicht befreit, ein Verzeichnis zu führen, wenn die Verarbeitung weder ein Risiko für die Rechte der betroffenen Personen birgt noch regelmäßig erfolgt noch besondere Datenkategorien i. S. d. Art. 9 Abs. 1 bzw. Art. 10 betrifft.

Pflichten aus der DSGVO

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- **Die folgenden Angaben müssen nach Art. 30 Abs. 1 in dem Verzeichnis enthalten sein:**

- Namen und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Kategorien betroffener Personen und Kategorien personenbezogener Daten
- Kategorien von Empfängern
- Übermittlungen in Drittländer sowie ggf. die Dokumentierung geeigneter Garantien
- vorgesehene Löschfristen
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Pflichten aus der DSGVO

Auftragsdatenverarbeitung, Art. 28

Auftragsdatenverarbeitung ist die Verarbeitung personenbezogener Daten durch einen Dienstleister (Auftragsverarbeiter) auf Weisung des Auftraggebers.

- Der Auftragsverarbeiter muss hinreichend Garantien dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

- Die Auftragsdatenverarbeitung erfolgt auf Grundlage eines **Vertrages**, in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Nach § 82 Abs. 1 haftet auch der Auftragsverarbeiter für durch seine Verarbeitung verursachte materielle und immaterielle Schäden!

Pflichten aus der DSGVO

Auftragsdatenverarbeitungsvertrag, Art. 28 Abs. 3 DSGVO
Der Vertrag (bzw. das Rechtsinstrument) muss die wesentlichen Inhalte der Verarbeitung fixieren, nämlich „Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen“. Der Vertrag (bzw. das andere Rechtsinstrument) muss dem Auftragsverarbeiter insbesondere die folgenden, in Art. 28 Abs. 3 lit. a bis h genannten Pflichten, auferlegen:

- Verarbeitung auf dokumentierte Weisung hin
- Verpflichtung zur Vertraulichkeit bzw. Verschwiegenheit
- Maßnahmen zur Datensicherheit nach Art. 32
- Einhaltung der Vorgaben zum Unterauftrag
- Unterstützung bei der Beantwortung von Anträgen
- Unterstützung bei den Pflichten nach Art. 32 bis 36
- Löschung oder Rückgabe nach dem Ende der Verarbeitungsleistung
- Zurverfügungstellung von Informationen und Ermöglichung von Überprüfungen

➢ **Vertrag hat entscheidende Bedeutung für die Darlegung der Voraussetzungen der Enthaftung nach Art. 82 Abs. 3 DSGVO.**

Regelungen aus der DSGVO

Datenübermittlung in Drittländer

- Übermittlung an Länder außerhalb der EU nur unter Einhaltung der Vorgaben der Verordnung
- Erlaubnistatbestände für die Übermittlung in Drittländer:

    - Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses, Art. 45
    - Datenübermittlung vorbehaltlich geeigneter Garantien, Art. 46
    - Ausnahmen für bestimmte Fälle

Regelungen aus der DSGVO

- **Dokumentation der technischen und organisatorischen Maßnahmen zum Datenschutz und der Datensicherheit**
  Art. 24 Abs. 1 verlangt dem Verantwortlichen „technische und organisatorische Maßnahmen“ ab um sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt. Dieser Begriff findet in verschiedenen Artikeln der DSGVO Verwendung (insbesondere in Art. 5 Abs. 1 lit. f, Art. 25 Abs. 1 u Abs. 2, Art. 28 Abs. 1, Art. 32 Abs. 1, Art. 89 Abs. 1 S. 2).

  - **Technische Maßnahmen** sind alle Vorkehrungen, die sich auf den Vorgang der Verarbeitung von Daten erstrecken, wie z. B. das Wegschließen von Datenträgern, bauliche Maßnahmen, die den Zutritt Unbefugter verhindern sollen, oder Steuerungen des Software- oder Hardwareprozesses der Verarbeitung, etwa durch Maßnahmen der Zugriffs- oder Weitergabekontrolle wie Verschlüsselung oder Passwortsicherung.

  - **Organisatorische Maßnahmen** richten sich insbesondere auf die äußeren Rahmenbedingungen zur Gestaltung des technischen Verarbeitungsprozesses, etwa die Einhaltung des Vieraugenprinzips, Protokollierungen von Tätigkeiten und Stichprobenroutinen. Dazu können auch Schulungen der Mitarbeiter oder Verpflichtungserklärungen, wie sie auch schon § 5 S. 2 BDSG vorsah, gehören.

Regelungen aus der DSGVO

- **Dokumentation der technischen und organisatorischen Maßnahmen zum Datenschutz und der Datensicherheit**
  Auch Art. 32 Abs. 1 verlangt von den Verantwortlichen und Auftragsverarbeitern die Festlegung technischer und organisatorischer Maßnahmen, um ein „angemessenes“ Datenschutzniveau sicherzustellen.

Art. 32 Abs. 1 enthält hierzu einen kurzen, nicht abschließenden Katalog verschiedener technischer und organisatorischer Maßnahmen:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Pflichten aus der DSGVO

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Privacy by design, Art. 25 Abs. 1 DSGVO

- IT-Systeme sollen grundsätzlich so ausgestaltet sein, dass sie die Grundsätze aus Art. 5 wirksam umsetzen
- IT-Systeme sollen gerade so viele Daten erheben, wie zur Erfüllung des Zwecks erforderlich sind

Privacy by default, Art. 25 Abs. 2 DSGVO

- IT-Systeme sollen so voreingestellt sein, dass sie grundsätzlich nur solche personenbezogenen Daten verarbeiten, deren Verarbeitung für den jeweils verfolgten Zweck erforderlich ist
- Daten sollen so schnell wie möglich pseudonymisiert werden

Auch diese Vorschriften sind bußgeldbewehrt!

Pflichten aus der DSGVO

Datenschutzbeauftragter, Art. 37 DSGVO

- Bestellungspflicht nach DSGVO nur unter engen Voraussetzungen
- Falls das Recht eines Mitgliedstaats eine Bestellung vorschreibt, muss ein Datenschutzbeauftragter bestellt werden
- DSAnpUG-EU sieht eine Bestellpflicht vor, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

- Aufgaben des Datenschutzbeauftragten sind in Art. 39 geregelt
    - Unterrichtung und Beratung des Verantwortlichen
    - Überwachung der Einhaltung der Verordnung
    - Schulung der Mitarbeiter
    - Beratung bei der Datenschutz-Folgenabschätzung
    - Anlaufstelle für Aufsichtsbehörde

Regelungen aus der DSGVO

Betroffenenrechte

- Recht auf Auskunft, Art. 15 DSGVO
- Recht auf Berichtigung, Art. 16 DSGVO
- Recht auf Löschung („Recht auf Vergessenwerden“), Art. 17 DSGVO
- Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO
- Recht auf Datenübertragbarkeit Art. 20 DSGVO
- Automatisierte Entscheidung im Einzelfall einschließlich Profiling, Art. 22 DSGVO

Pflichten aus der DSGVO

Datenschutz-Folgenabschätzung, Art. 35 Abs. 1 DSGVO

Art. 35 Abs. 1 DSGVO: *„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Aschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“*

- Bewertung der **Eintrittswahrscheinlichkeit** und **Schwere** des möglichen Risikos
- Prüfung von Maßnahmen, Garantien und Verfahren zur **Eindämmung** des Risikos
- Ergibt die Abschätzung, dass die geplante Datenverarbeitung ein hohes Risiko zur Folge hätte muss die **Aufsichtsbehörde** zu Rate gezogen werden, sofern keine Maßnahmen zur Eindämmung des Risikos getroffen werden.

Da hohe Bußgelder drohen, sollten Strukturen und Prozesse geschaffen werden, um die Anforderungen des Art. 35 zu erfüllen!

Pflichten aus der DSGVO

Melde- und Benachrichtigungspflichten, Art. 33, 34 DSGVO

- Voraussetzung ist das Vorliegen einer **Datenschutzverletzung**:

  „Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob zufällig oder unrechtmäßig, oder zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt gespeichert oder auf sonstige Weise verarbeitet wurden.“

- Meldung an die Aufsichtsbehörde **innerhalb von 72 Stunden**, nachdem dem Verantwortlichen die Verletzung bekannt wurde.
- Keine Meldepflicht, wenn die Verletzung voraussichtlich **nicht zu einem Risiko** für die Rechte und Freiheiten der betroffenen Personen führt
- Benachrichtigungspflicht gegenüber betroffenen Personen falls voraussichtlich ein **hohes Risiko** für deren Rechte und Freiheiten besteht (ohne unangemessene Verzögerung)

Da hohe Bußgelder drohen, sollten Strukturen und Prozesse geschaffen werden, um bei Datenschutzverletzungen richtig und schnell reagieren zu können!

Pflichten aus der DSGVO

Datensicherheit, Art. 32 DSGVO

- Vorschrift enthält Vorgaben zur Datensicherheit
- Zu treffenden Maßnahmen werden nur beispielhaft und vage beschrieben
- Klare Vorgaben der Datenschutzaufsichtsbehörden bleiben abzuwarten

Momentan können Unternehmen sich an den entsprechenden ISO-Normen oder den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) orientieren!

Rechtsfolgen bei Verstößen

Schadensersatzansprüche (materielle und immaterielle Schäden), Art. 82 DSGVO

- Neue Maßstäbe, da nun auch immaterielle Schäden ausdrücklich umfasst

Bußgelder

- Geldbußen von bis zu 20 Mio. EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs

BREHM & v. MOERS

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Paul Nottarp, LL.M.
Rechtsanwalt

Brehm & v. Moers Rechtsanwälte PartG mbB
Wiesenau 1
60323 Frankfurt am Main

Tel.: +49 (0)69 15 20 05 0
Fax.: +49 (0)69 15 20 05 20

paul.nottarp@bvm-law.de
www.bvm-law.de