DSGVO

-Wesentliche Regelungen-

Kurzvortrag GVKN-Netzwerktreffen
26.7.2018

Siegmund Schäfer

1. Gesetzeszweck

Art. 1 DSGVO Gegenstand und Ziele

1. Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten** und zum freien Verkehr solcher Daten.

2. Diese Verordnung schützt die **Grundrechte und Grundfreiheiten natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.

3. ……

2. Was sind personenbezogene Daten?

Art. 4 DSGVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche** Person (im Folgenden „betroffene 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;

3. Zulässigkeit der Verarbeitung

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

1. auf **rechtmäßige** Weise, nach **Treu und Glauben** und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden; ……..
2. für festgelegte, eindeutige und **legitime Zwecke** erhoben werden ……..
3. dem Zweck **angemessen** und **erheblich** sowie auf das für die Zwecke der Verarbeitung **notwendige Maß** beschränkt sein („Datenminimierung“);
4. sachlich richtig und **erforderlichenfalls** auf dem **neuesten Stand** sein; es sind alle **angemessenen Maßnahmen** zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
5. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur **so lange** ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist; personenbezogene Daten dürfen **länger** gespeichert werden, soweit die personenbezogenen Daten **vorbehaltlich** der Durchführung **geeigneter** technischer und organisatorischer Maßnahmen, …….. („Speicherbegrenzung“);

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

1. Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
2. die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
3. die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
4. die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

4. Hinweispflichten

Art. 12 DSGVO Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

1. Der Verantwortliche trifft geeignete Maßnahmen, um …….. alle Informationen …… in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache** zu übermitteln; …….

Art. 13 DSGVO Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

1. Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
    1. ……..
2. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:
3. …….
4. Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Folge: Datenschutzerklärung bzw. Datenschutzhinweise

5. Formelle Anforderungen der DSGVO

Art. 30 DSGVO Verzeichnis von Verarbeitungstätigkeiten

a) Verzeichnis der Verarbeitungsvorgänge

1. Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
   …….
2. Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:
   ……
3. ……..
4. Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen **der Aufsichtsbehörde** das Verzeichnis auf Anfrage zur Verfügung.
5. Die in den Absätzen 1 und 2 genannten Pflichten **gelten nicht** für Unternehmen oder Einrichtungen, die **weniger als 250 Mitarbeiter** beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die **Verarbeitung erfolgt nicht nur gelegentlich** oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

Art. 32 DSGVO Sicherheit der Verarbeitung

b) Beschreibung der technischen und organisatorischen Massnahmen (TOM’s)

1. Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der **Art**, des **Umfangs**, der **Umstände** und der Zwecke der Verarbeitung sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere** des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten; diese Maßnahmen **schließen gegebenenfalls unter anderem** Folgendes ein:
   ……

Art. 28 DSGVO Auftragsverarbeiter

c) ADV-Vertrag bei Weitergabe der Verarbeitung von pbD an Dritte oder bei Verarbeitung von Daten Dritter

1. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet**.**
2. .....
3. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der **Grundlage eines Vertrags**.

Hinweis: Vorsicht bei „Haftungsfreistellungsklauseln“ und bei „Vergütungsklauseln“

6. Meldepflicht

Art. 33 DSGVO Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und **möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.
2. ……..
3. Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:
   ……
4. Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten ……. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

7. Datenschutzbeauftragter

§ 38 BDSG Datenschutzbeauftragte nichtöffentlicher Stellen

1. Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.
   ……

Art. 37 DSGVO Benennung eines Datenschutzbeauftragten

1. Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
    1. die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, ……
2. die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, …… oder ……

Hinweis: Abberufung nur aus wichtigem Grund möglich;

DSB genießt **Kündigungsschutz!**

Haftung: Es gelten die arbeitsrechtlichen Beschränkungen, d.h.: Volle Haftung nur bei externem DSB

8. Haftung und Bußgelder

Art. 82 DSGVO Haftung und Recht auf Schadenersatz

1. Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein **materieller oder immaterieller Schaden** entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
2. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.
   ……
3. ……
4. Ist **mehr als ein Verantwortlicher** oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt …….. **so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, ……..**
5. ……

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall **wirksam**, **verhältnismäßig** und **abschreckend** ist.
    1. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt: 1.-11. …….
    2. Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:** …….
    3. Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **20 000 000 EUR** 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: ……..