



HFK RECHTSANWÄLTE LLP • WWW.HFK.DE



Umsetzung datenschutzrechtlicher Anforderungen in der Praxis der eVergabe

Seminar des VSVI e.V.

27. Februar 2019

**Dr. Till Kemper
Rechtsanwalt**

HFK Rechtsanwälte LLP – Kompetenz seit 40 Jahren und über 50 RechtsanwältlNNen

Projektgruppen:

- **Immobilie**
- **Infrastruktur**
- **Industrie**
- **Energie**
- **IT**

Komplexitätsmanagement durch Spezialwissen:

- **Bau- und Werkvertragsrecht**
- **Öffentliches Bau- und Planungsrecht**
- **Immobilienwirtschaftsrecht**
- **Vergaberecht**
- **Streitlösung und Prozessführung**



- Rechtsanwalt
- Fachanwalt für Bau- und Architektenrecht
- Fachanwalt für Verwaltungsrecht
- Fachanwalt für Vergaberecht
- Rechtsausschuss des BIM-Cluster Hessen e. V.
- AG Digitalisierung der Akademie für Raum- und Landschaftsplanung
- Externer Datenschutzbeauftragter
- Geschäftsführer bim2bim GmbH
- Lehraufträge
 - THM-Gießen „Planen und Bauen im Denkmalbestand“
 - Universität Tübingen/Kiel „Denkmalschutzrecht“
- Ständige Seminare beim
 - id-Verlag
 - Vhw



1

Überblick: Die DSGVO und das BDSG-neu

2

Unter welchen Umständen dürfen Daten von Mitarbeitern und Sub-Unternehmern im eVergabeverfahren durch Bieter weitergegeben werden?

3

Was ist im Rahmen einer Auftragsverarbeitung zu beachten?

4

Unter welchen Umständen dürfen personenbezogene Daten ins Ausland übermittelt werden?

1**Übersicht: Die DSGVO und das BDSG-neu**

Verordnung (EU) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung)

„Grundverordnung“:

- **Verordnung ist im Gegensatz zur Richtlinie unmittelbar geltendes Recht (Art. 288 AUEV)**
- **Enthält aber eine Vielzahl von Öffnungsklauseln, die Spielraum für nationales Recht lassen**

Wesentliche Ziele

- Schutz der informellen Selbstbestimmung
- Harmonisierung durch unmittelbare Geltung als VO
- Modernisierung als Antwort auf neue Herausforderungen (Globalisierung, Digitalisierung)

Wesentliche Grundsätze

- Verbotprinzip
- Prinzip der Datensparsamkeit
- Prinzip der Angemessenheit und Erforderlichkeit
- Prinzip der Transparenz und Zweckbindung
- Prinzip der Datensicherheit
- Prinzip der unabhängigen Aufsicht und wirksamer Sanktionierung

Anwendungsbereich

Sachlicher Anwendungsbereich (Art. 2 DSGVO)

Diese Verordnung gilt für die ganz oder teilweise automatisierte **Verarbeitung personenbezogener Daten** sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Ausnahmen:

- Tätigkeit **außerhalb EU-Recht**
- Tätigkeiten natürlicher Personen zur Ausübung ausschließlich **familiärer Art**
- **Gefahrenabwehr** und **Strafverfolgung**
- (...)

Räumlicher Anwendungsbereich (Art. 3 DSGVO)

- Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU
- **Marktortprinzip**: Angebot richtet sich an Markt in der EU oder dient der Beobachtung von Personen in der EU
- Ort, der aufgrund des Völkerrechts dem Recht eines MS unterliegt

Marktortprinzip:
Ausländische Unternehmen
sollen nur Marktzugang zum
Binnenmarkt haben, wenn sie
sich an die DSGVO halten

§ 1 BDSG-neu

Öffentliche Stellen des Bundes:

- Behörden,
- Organe der Rechtspflege
- andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie
- deren Vereinigungen ungeachtet ihrer Rechtsform.

Konkretisierung von Art. 2 und 3 DSGVO

öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

- a) Bundesrecht ausführen oder
- b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt

Behörden, Einrichtungen und sonstigen **öffentlichen Stellen des Landes**, die Gemeinden und -verbände sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen

nicht-öffentliche Stellen:

- für die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten**
- sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Datensystem gespeichert sind oder gespeichert werden
- es sei denn: natürliche Personen bei ausschließlich persönlichen oder familiären Tätigkeiten

DSG der Länder

Art. 1 DSGVO

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

Juristische Personen nicht erfasst; können sich aber auf Recht der informellen Selbstbestimmung berufen!

Art. 4 Nr. 1 DSGVO

Personenbezogene Daten sind alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** („betroffene Person“) beziehen (...).

Art. 9 DSGVO

Besondere Kategorien:

- Daten, aus denen sich die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen
- Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben der der sexuellen Orientierung

Grundprinzipien

**Rechtmäßigkeit der Datenverarbeitung
(Art. 6 DSGVO)**

**Eingeschränkte Übermittlung in
Drittstaaten (Art. 44 – 50 DSGVO)**

**Datensparsamkeit
(Art. 5 Abs. 1 lit. C DSGVO)**

**Betroffenenrechte
(Art. 12 ff. DSGVO)**

**Zweckbindung
(Art. 5 Abs. 1 lit. B DSGVO)**

**Unabhängige Aufsicht
(Art. 51 f. DSGVO)**

**Datensicherheit
(Art. 5 Abs. 1 lit f, Art. 32 DSGVO)**

**Effektive Durchsetzung durch Befugnisse
der Aufsichtsbehörden (Art. 58 DSGVO)
und Sanktionen (Art. 83 DSGVO)**

Wesentliche Neuerungen (1)

**Marktortprinzip
(Art. 3 Abs. 2 DSGVO)**

**Verfahrensvereinfachung und einheitliche
Rechtsanwendung**



„One-Stop-Shop“



**Kohärenzverfahren
(Art. 63, 65 DSGVO)**

Wesentliche Neuerungen (2)

**Privacy by Design/ Privacy by Default
(Art. 25 DSGVO)**

**Datenschutzfolgenabschätzung
(Art. 35 DSGVO)**

**Auftragsverarbeitung
(Art. 28 DSGVO)**

**Pflicht zur Bestellung eines
Datenschutzbeauftragten (Art. 37
DSGVO)**

**Meldung von Datenschutzverletzungen
(Art. 33 DSGVO)**

**Stärkung der Selbstregulierung und
Zertifizierung (Art. 40 ff. DSGVO)**

Wesentliche Rechte der betroffenen Person

- ▶ **Transparente Information (Art. 12 DSGVO)**
- ▶ **Informationspflichten (Art. 13 f. DSGVO)**
- ▶ **Auskunftsrecht (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)**

Wenn Bewerber gegen
Datenschutz verstößt:
Ausschluss wegen
schwerer Verfehlung
möglich (§ 124 Abs. 1 Nr.
3 GlWB)

Sonstige Folgen

- ▶ **Recht auf Schadenersatz (Art. 82)**
- ▶ **Verhängung von Geldbußen (Art. 83 DSGVO)**
- ▶ **Rechts auf Beschwerde bei Aufsichtsbehörde (Art. 77 DSGVO)**

2

Unter welchen Umständen dürfen personenbezogene Daten im eVergabeverfahren verarbeitet werden?

Begründung zur VgV (BR-Drs. 87/16, S. 196) :

eVergabe ist **Paradigmenwechsel**:

- **Neuorganisation der Abläufe**
- **Erhöhte Verantwortung**, die Möglichkeiten der eVergabe bewusst zu nutzen.
- **Verlagerung von Verantwortlichkeiten**, insbesondere von Informationspflichten.

eVergabe

DSGVO, BDSG-neu

Schutz des **informellen Selbstbestimmungsrechts** u.a.

durch **Verbotsprinzip**,

Prinzip der

Datenminimierung,
der **Angemessenheit**
und **Erforderlichkeit**

(u.a.)

Datenschutz

Welche Anforderungen bestehen an die Eignung?

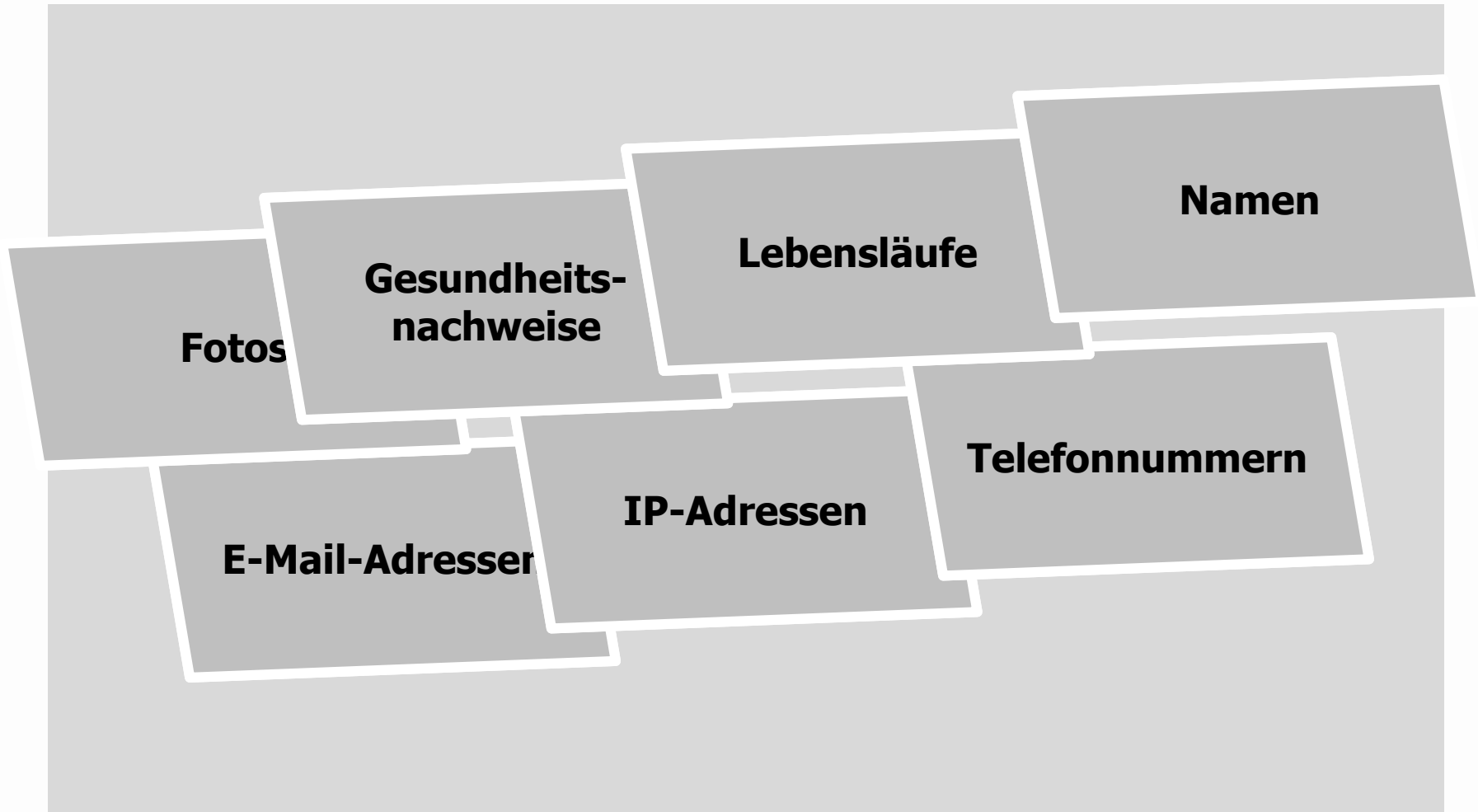


Welche wesentlichen Eignungskriterien und –nachweise kommen in Betracht?

..

	Nichtvorliegen von Ausschlussgründen	Befähigung zur Berufsausübung	Wirtschaftliche und finanzielle Leistungsfähigkeit	Technische und berufliche Leistungsfähigkeit	Qualitäts-sicherung und Umwelt-management
	z.B. • Rechtskräftige Verurteilung • Steuern und Abgaben nicht gezahlt • Insolvenz etc.	• Eintrag in Berufs- und Handelsregister (Anhang XI): • Bestimmte Berechtigung oder Mitgliedschaft in Organisation	Wirtschaftliche und finanzielle Kapazitäten, insb. • Mindestumsatz • Verhältnis von Vermögen und Verbindlichkeiten • Berufshaftpflicht	Personelle und technische Kapazitäten, insb. • Referenzen • Keine Interessenkollision (Art. 24 VRL)	Erfüllung von • Qualitäts-sicherungs-normen • Systemen und Normen für Umwelt-management
	(Art. 57 VRL; §§ 123 ff. GWB)	(Art. 58 I, II VRL; § 44 VgV)	(Art. 58 I, III VRL; § 45 VgV)	(Art. 58 I, IV VRL; § 46 VgV)	(Art. 62 VRL; § 49 VgV)
	• Registerauszug (wie Strafregister) • Behördliche Bescheinigung • Hilfsweise: Eidesstattliche Erklärungen etc.	• Nachweis der Berechtigung oder • Mitgliedschaft	Regelbeispiele: • Bankerklärung • Vorlage Jahresabschluss • Erklärung über Gesamtumsatz • Versicherungsnachweis	• Verzeichnis erbrachter Bau-, Liefer- und Dienstleistungen • Angabe der Fachkräfte • Beschreibung der Ausrüstung (...)	• Bescheinigungen unabhängiger Stellen • oder gleichwertige Bescheinigung
	(Art. 60 II VRL; § 48 VgV)	(Art. 58 VRL)	(Art. 60 III, Anhang XII Teil 1 VRL; § 48 VgV)	(Art. 60 IV, Anhang XII Teil 2 VRL; § 48 VgV)	(Art. 62 VRL; § 48 VgV)

Beispiele:



„Personenbezogene Daten“ (Art. 4 Nr. 1 DSGVO)

Personenbezogene Daten sind alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** („betroffene Person“) beziehen (...).

Beispiele nach § 46 Abs. 3 VgV:

- Personenbezogene **Referenzen** (Nr. 1)
- **Angabe der technischen Fachkräfte** (...), die im Zusammenhang mit der Leistungserbringung eingesetzt werden sollen (Nr. 2)
 - insb. **CV** samt Name, E-Mailadresse, Telefonnummer, Foto etc.
- **Studien- und Ausbildungsnachweise** sowie **Bescheinigungen** über die Erlaubnis zur Berufsausübung für die Inhaberin, den Inhaber oder die Führungskräfte des Unternehmens (Nr. 6)
- (...)

Welche wesentlichen Anforderungen sind zu beachten?

...

Art. 6 DSGVO

Verbot mit Erlaubnisvorbehalt

Verarbeitung ist nur zulässig, wenn

- Betroffene Person **eingewilligt** hat oder
- die Verarbeitung
 - für die **Erfüllung eines Vertrages**, dessen Vertragspartei die betroffene Person ist,
 - zur Durchführung **vorvertraglicher Maßnahmen** erforderlich ist
 - zur Erfüllung einer **rechtlichen Verpflichtung** des Verantwortlichen erforderlich ist
 - für **lebenswichtige Interessen** erforderlich ist
 - für die **Wahrnehmung einer öffentlichen Aufgabe** des Verantwortlichen erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt,
 - der **Wahrung der berechtigten Interessen** erforderlich ist, sofern nicht die Interessen der Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (...)

§ 3 BDSG-neu

Verarbeitung personenbezogener Daten durch öffentliche Stellen

Rechts-
grundlage für
Vergabestellen
(öff. Stelle)

Die Verarbeitung personenbezogener Daten durch eine **öffentliche Stelle** ist zulässig, wenn sie zur **Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe** oder in der Ausübung öffentlicher Gewalt erforderlich ist.

Offenlegung durch Bieter oder Bewerber gegenüber AG?

Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses?

§ 26 BDSG-neu:

- Verarbeitung zulässig, soweit dies für die „Durchführung des Beschäftigungsverhältnisses“ erforderlich ist
- Offenlegung gegenüber Dritten zulässig, wenn dies in der Zweckbestimmung des Arbeitsverhältnisses liegt, also z. B. zur Erfüllung der Arbeitspflicht erforderlich ist

Bei sensiblen Daten
gelten besondere
Anforderungen an
die Einwilligung (§ 26
Abs. 3 BDSG-neu)

Einwilligung?

- freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder **einer sonstigen eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
- Allgemeine Anforderungen an die Einwilligung nach **Art. 7 DSGVO** beachten!
- „Freiwilligkeit“ der Einwilligung: Neben Art. 7 Abs. 4 DSGVO besondere Anforderungen nach **§ 26 Abs. 2 BDSG-neu** beachten

§ 123 GWB

(1) Öffentliche Auftraggeber schließen ein Unternehmen zu jedem Zeitpunkt des Vergabeverfahrens von der Teilnahme aus, wenn sie Kenntnis davon haben, dass eine **Person**, deren Verhalten nach Absatz 3 dem Unternehmen zuzurechnen ist, **rechtskräftig verurteilt** oder gegen das Unternehmen eine Geldbuße nach § 30 des Gesetzes über Ordnungswidrigkeiten rechtskräftig festgesetzt worden ist wegen einer Straftat nach (...)

Art. 10 DSGVO

Die Verarbeitung personenbezogener Daten über **strafrechtliche Verurteilungen und Straftaten** oder damit zusammenhängende Sicherungsmaßnahmen aufgrund von Artikel Art. 6 Abs. 1 DSGVO darf

- nur unter behördlicher Aufsicht vorgenommen werden oder
- wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Art. 5 Abs. 1 lit b) DSGVO

Personenbezogene Daten müssen für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (...) („Zweckbindung“)



Zweckbindung durch Vorgaben zur Eignungsprüfung begrenzt:



§§ 122, 123, 124, 125, 126 GWB



§§ 42 – 51 VgV



§§ 6 ff VOB/A



§§ 45 – 50 SektVO



§§ 25 – 30 KonzVO



§§ 22 – 28 VSVgV

Ist ein Auszug aus dem einschlägigen Register, zum Beispiel aus dem Strafregister, für den öffentlichen Auftraggeber oder Sektorenauftraggeber auf elektronischem Wege erhältlich, kann der Wirtschaftsteilnehmer angeben, wo diese Information aufzufinden ist (z. B. Bezeichnung des Dokumentenarchivs, Internet-Adresse, Angabe der betreffenden Akte oder Datei usw.), so dass der öffentliche Auftraggeber oder Sektorenauftraggeber diese Information einholen kann. Mit diesen Angaben erklärt sich der Wirtschaftsteilnehmer einverstanden, dass der öffentliche Auftraggeber oder Sektorenauftraggeber unter Beachtung der innerstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/46/EG ⁽¹³⁾ über die Verarbeitung personenbezogener Daten, vor allem besonderer Kategorien von Daten wie Daten über Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen, die relevanten Unterlagen abrufen.

Auszug aus:

DURCHFÜHRUNGSVERORDNUNG (EU) 2016/7 DER KOMMISSION

vom 5. Januar 2016

zur Einführung des Standardformulars für die Einheitliche Europäische Eigenerklärung

(Text von Bedeutung für den EWR)

Anhang I, S. 20.

3 Was ist im Rahmen einer Auftragsdatenverarbeitung zu beachten?

Auftraggeber



Auftrag zur Datenverarbeitung

Def. § Art4 Nr. 8 DSGVO:
natürliche oder juristische
Person, Behörde, Einrichtung
oder andere Stelle, die
personenbezogene Daten im
Auftrag des Verantwortlichen
verarbeitet

Auftragnehmer



ggf.

Verantwortlicher



Betroffene Person

Unterauftragnehmer

Bei welchen Aufträgen ist typischerweise besonders an Auftragsverarbeitung zu denken?

..

Beispiele:

Einrichtung und Betrieb eines
Kommunikationsnetzes
2016/S 056-094618

Personaldienstleistungen im Rahmen einer
Arbeitnehmerüberlassung auf dem Gebiet der
Informationstechnologie
2016/S 077-137491

Rahmenvereinbarung über die Durchführung
von elektronischen Einstellungstests
2016/S 090-160144

Rahmenvertrag über die Nutzung eines
Bibliothekssystems als cloudbasierte Software-
as-a-Service Lösung
2016/S 090-161798

Beratung, Entwicklung und Umsetzung der
Online-Kommunikation
2016/S 107-190396

Digitalisierung und Vernichtung von Papierakten
2016/S 121-217134

Art. 28 ff. DSGVO

- AG bleibt maßgeblich verantwortlich
- AN darf personenbezogene Daten nur im Rahmen der Weisungen des AG verarbeiten (Art. 29 DSGVO)
- AG und AN müssen Verzeichnisse über Verarbeitungstätigkeiten führen (Art. 30 Abs. 1 und 2 DSGVO)
- Ausnahme: AG oder AN haben weniger als 250 Mitarbeiter
- Ausnahme der Ausnahme: besonderes Risiko oder sensible Daten nach Art. 9 und 10 DSGVO
- AN muss 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
- Sicherheit der Verarbeitung nach Art. 32 DSGVO beachten

Vertrags-vorgaben
nach Art. 28 Abs. 3
DSGVO!

Kein generell geltendes Sicherheitsniveau, sondern der Gefährdungslage angemessene Maßnahmen (insb. Vor-Ort-Kontrolle nicht immer zwingend!)

Welche Kriterien und Nachweise kommen für die Eignung des AN in Betracht?

...

§ 46 VgV (technische und berufliche Leistungsfähigkeit)

- Geeignete **Referenzen** über früher ausgeführte vergleichbare Aufträge
- Angabe der **technischen Fachkräfte**
- Beschreibung der **technischen Ausrüstung**, Maßnahmen zur Qualitätssicherung
- **Studien- und Ausbildungsnachweise**
- Erklärung, aus der ersichtlich ist, über welche **Ausstattung**, welche Geräte und welche **technische Ausrüstung** das Unternehmen für die Ausführung des Auftrags verfügt

Nachweise nach der DSGVO

- Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder
- eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO

Vor allem: Sicherheitskonzept zu techn. und org. Maßnahmen

§ 10 VgV: Anforderungen an die verwendeten elektronischen Mittel

(...) Elektronische Mittel, die von dem öffentlichen Auftraggeber für den Empfang von Angeboten, Teilnahmeanträgen und Interessensbestätigungen sowie von Plänen und Entwürfen für Planungswettbewerbe verwendet werden, müssen gewährleisten, dass

1. die Uhrzeit und der Tag des Datenempfangs genau zu bestimmen sind
2. kein vorfristiger Zugriff auf die empfangenen Daten möglich ist
3. der Termin für den erstmaligen Zugriff auf die empfangenen Daten nur von den Berechtigten festgelegt oder geändert werden kann,
4. **nur die Berechtigten Zugriff auf die empfangenen Daten oder auf einen Teil derselben haben**
5. **nur die Berechtigten nach dem festgesetzten Zeitpunkt Dritten Zugriff auf die empfangenen Daten oder auf einen Teil derselben einräumen dürfen**
6. **empfangene Daten nicht an Unberechtigte übermittelt werden und**
7. Verstöße oder versuchte Verstöße gegen die Anforderungen gemäß den Nummern 1 bis 6 eindeutig festgestellt werden können.

(...)

§ 11 VgV: Anforderungen an den Einsatz elektronischer Mittel im Vergabeverfahren

(1) Elektronische Mittel und deren technische Merkmale müssen allgemein verfügbar, nichtdiskriminierend und mit allgemein verbreiteten Geräten und Programmen der Informations- und Kommunikationstechnologie kompatibel sein. Sie dürfen den Zugang von Unternehmen zum Vergabeverfahren nicht einschränken. Der öffentliche Auftraggeber gewährleistet die barrierefreie Ausgestaltung der elektronischen Mittel nach den §§ 4 und 12 des Behindertengleichstellungsgesetzes (...) in der jeweils geltenden Fassung.

(2) Der öffentliche Auftraggeber verwendet für das Senden, Empfangen, Weiterleiten und Speichern von Daten in einem Vergabeverfahren ausschließlich **solche elektronischen Mittel, die die Unversehrtheit, die Vertraulichkeit und die Echtheit der Daten** gewährleisten.

(3) Der öffentliche Auftraggeber muss den Unternehmen alle notwendigen Informationen zur Verfügung stellen über

1. die in einem Vergabeverfahren verwendeten elektronischen Mittel
2. die technischen Parameter zur Einreichung von Teilnahmeanträgen, Angeboten und Interessensbestätigungen mithilfe elektronischer Mittel und
3. verwendete Verschlüsselungs- und Zeiterfassungsverfahren

4 Welche Besonderheiten ergeben sich bei Vergabeverfahren mit Auslandsbezug?

Beispiele:

- Fernwartung von Software aus dem Ausland
- Rechnungsabwicklung durch Konzernunternehmen mit Sitz im Ausland
- Auftragnehmer hat Server an einem Standort im Ausland
- Auftragnehmer nutzt selbst Dienstleistungen aus dem Ausland (z.B. Call-Center)

Grundsatz: Art. 44 DSGVO

Jedwede Übermittlung personenbezogener Daten (...) an ein Drittland oder eine internationale Organisation (...), ist nur zulässig, wenn

- der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten
- und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden;

(...). Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Art. 45 DSGVO: Angemessenheitsbeschluss

Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die **Kommission** beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein **angemessenes Schutzniveau** bietet. Eine solche Datenübermittlung bedarf **keiner besonderen Genehmigung**.

Art. 46 DSGVO: Geeignete Garantien

Falls kein Angemessenheitsbeschluss vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation **nur** übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter **geeignete Garantien** vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Als Garantien kommen vor allem in Betracht:

- **Verbindliche interne Datenschutzvorschriften** (Art. 47 Abs. 2 lit. b) DSGVO)
- **Genehmigte Verhaltensregeln** gem. Art. 40 DSGVO
- **Genehmigte Zertifizierungsmechanismen** gem. Art. 42 DSGVO

Art. 49 Abs. 1 DSGVO: Ausnahmen für bestimmte Fälle

- Ausdrückliche Einwilligung; Erfüllung eines Vertrag zwischen betroffener Person und dem Verantwortlichen; Ausübung von Rechtsansprüchen etc.

„Safe-Habour-Mechanismus“

- USA verfügen grundsätzlich nicht über „ausreichendes Datenschutzniveau“
- Zur Überbrückung der Systemunterschiede: Abstimmung zwischen EU und US-FTC (sog. Safe-Harbor-Mechanismus) zu Rechtsrahmen aus datenschutzrechtlichen „Grundsätzen“ und „Häufig gestellten Fragen“ (FAQ)
- Selbstverpflichtung durch 3246 Unternehmen (zB MasterCard, Google, Facebook, Amazon und Microsoft etc.).
- Im Gegenzug: Entscheidung der EU-Kommission, dass Unternehmen, die diese Selbstverpflichtung eingehen, über ein angemessenes Datenschutzniveau verfügten (Entscheidung 2000/520 der EU-Kommission).
- Eine Übermittlung an sie war daher auch ohne zusätzliche Garantien zulässig.

EuGH, Urteil vom 6. Oktober 2015 – Rs. C-362/14 - Schrems

- Entscheidung der Kommission ist ungültig.
- Zwischenzeitlich festgestellt: unangemessener und intransparenter Zugriff durch US-Sicherheitsbehörden auf Daten bei den Unternehmen

„EU-US Privacy Shield“: Zweifel, ob Vorgaben des EuGH erfüllt sind