Neuerungen der DSGVO
–
Änderungen und Neuerungen zur bisherigen Rechtslage

§§

cyberlegal
NIEDERMEIER & FAULHABER

RAin Dorothea Teichmann

DSGVO – ready or not?
01.03.2018 Würzburg

Agenda

- Vorstellung & Einführung die EU-DSGVO
- Vergleich zur bisherigen Rechtslage
-
- Ende und Diskussion

Vorstellung: Cyberlegal - RAe Niedermeier & Faulhaber

Kanzleigründung 2014

Cyberlegal „Rechtsanwaltsboutique“:

- Datenschutzrecht, IT-Recht und Recht der IT-Sicherheit
  - „Klassische“ Rechtsberatung und anwaltliche Vertretung
  - Stellung eines externen Datenschutzbeauftragten (über 20 Jahre Berufserfahrung als ext. DSB)
  - Gutachten und Stellungnahmen für Geschäftsführung, Betriebsrat und IT-Leitung
  - Unterstützung von Konzern-Datenschutzorganisationen
- Informationssicherheitsberatung (ISMS und DS-Management nach ISO 27xxx)
- Kurze Entscheidungswege und auf den Mandanten zugeschnittene Rechtsberatung
- Beratung von Unternehmen, insb. aus den Sektoren IT, Finanzen, Medizin und Produktion

Pressestimmen

„Unternehmen sind schlecht vorbereitet“: Internationale Dell-Studie*

- mehr als 80%: wenige bis keine Kenntnis der EU-DSGVO
- fast 70%: werden Anforderungen nicht gerecht werden oder keine Kenntnis darüber
- 97%: keinen Plan zur Umsetzung bis Mai 2018

Bitkom Umfrage**

- 32 % kennen die EU-DSGVO haben sich aber noch nicht damit beschäftigt
- 8 % haben 2016 bereits erste Maßnahmen eingeleitet
- 51% verfügen über ein Verfahrensverzeichnis
- 64 % werden externe Hilfe benötigen

“Compliance wird wichtiger, Sanktionen werden härter“***

- „Das Vorgehen ist einfach, die Umsetzung komplex"

* https://www.it-daily.net/analysen/13552-unternehmen-sind-schlecht-vorbereitet-eu-datenschutz-grundverordnung
** https://www.bitkom.org/Presse/Presseinformation/Viele-Unternehmen-haben-Datenschutzreform-nicht-auf-dem-Schirm.html
*** Sueddeutsche Zeitung vom 13.07.2017

EU-DSGVO

Im Amtsblatt veröffentlicht am 04.05.2016

Ziel der EU-DSGVO ist die Vereinheitlichung des europäischen Datenschutzrechts

Die im zweiten Quartal 2018 in Kraft tretende Neuregelung ersetzt die bisherige europäische Datenschutzrichtlinie (DS-RL 95/46/EG) und die darauf basierenden einzelstaatlichen Regelungen, wie das BDSG

Mittels Öffnungsklauseln in der EU-DSGVO wird den Mitgliedsstaaten in vielen Fällen jedoch die spezifische Ausgestaltung überlassen.

Datenschutzrechtliche Regelungen werden daher auch zukünftig in unterschiedlichen Gesetzen zu finden sein, wobei der erste Blick nunmehr in die EU-DSGVO zu erfolgen hat.

Höhere Bußgelder und Freiheitsstrafen

§§ 43, 44 BDSG-Alt	Art. 83 EU-DSGVO / § 42 BDSG-Neu
Bis zu **50.000 €**	Bis zu **10 Mio. €** oder **2 %** des gesamten weltweit erzielten Jahresumsatzes
Bis zu **300.000 €**	Bis zu **20 Mio. €** oder **4 %** des gesamten weltweit erzielten Jahresumsatzes
Bis zu **zwei Jahre** Freiheitsstrafe oder Geldstrafe	Bis zu **drei Jahre** Freiheitsstrafe oder Geldstrafe
Möglichkeit der Gewinnabschöpfung	Geldbuße muss wirksam, verhältnismäßig und **abschreckend** sein

Erweiterte Haftung für Verantwortliche und für Auftragsverarbeiter

§ 7 BDSG-Alt	EU-DSGVO
Verantwortliche Stelle	Verantwortlicher und **Auftragsdatenverarbeiter**
Materielle Schäden	**Immaterielle** und materielle Schäden
	Gesamtschuldnerische Haftung der Beteiligten
Beweislastumkehr hins. Einhaltung der erforderlichen Sorgfalt	Möglichkeit des **Nachweises**, dass in **keinerlei Hinsicht eine Verantwortung** für den Schaden verursachenden Umstand besteht

Stellung und Haftung des DSB

§ 4f BDSG-Alt	Art. 37 IV EU-DSGVO, § 38 BDSG-Neu
Bestellpflicht bei **mehr als 9 Personen**, die ständig mit automatisierter Verarbeitung beschäftigt sind	Bestellpflicht bei **mindestens 10** Personen, die ständig mit der automatisierten Verarbeitung beschäftigt sind
Hinwirkungspflicht, **Überwachung** der ordnungsgemäßen **Anwendung** von Programmen, Schulung MA, Vorabkontrolle	**Unterrichtung und Beratung** des Verantwortlichen oder Auftragsverarbeiters und der Beschäftigten, **Überwachung** der Einhaltung der **DSGVO**, **Überwachung** der internen **Strategien** des Verantwortlichen oder des Auftragsverarbeiters, **Zuweisung** von Zuständigkeiten, Sensibilisierung und **Schulung** von MA und diesbezügliche **Überprüfungen**
Zivilrechtliche Haftung ggü. Verantwortlicher Stelle, bei deliktischem Verhalten ggf. ggü. Betroffenem	Zivilrechtliche Haftung ggü. Verantwortlichem, bei deliktischem Verhalten ggü. Betroffenem; strittig: Überwachungsgarant

Erweiterte Dokumentationspflichten und Nachweispflichten

§§ 9, 4g II 1 BDSG-Alt	Art. 5 II, 24 I EU-DSGVO
TOMs: bisher keine ausdrückliche Dokumentationspflicht, aber zum Nachweis pflichtgemäßen Handelns unerlässlich (vgl. § 7 BDSG-Alt)	**Rechenschaftspflicht**: Der Verantwortliche ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss deren Einhaltung nachweisen können.
Verfahrensübersicht der verantwortlichen Stelle	Verantwortliche muss **nachweisen** können, dass er pD DSGVO-konform verarbeitet. Auftragsverarbeiter müssen dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen.
	Bspw.: TOMs, Datenminimierung, Pseudonymisierung, Transparenz; Verarbeitungsverzeichnis, DS-Folgeabschätzung; Befugnis der ABS Informationen zur Rechtmäßigkeit jeder DV zu verlangen

Datenschutz-Folgeabschätzung

§ 4d V BDSG-Alt	Art. 35, Art. 36 I EU-DSGVO
Keine inhaltlichen Anforderungen an die Vorabkontrolle (VAK)	Inhaltliche Anforderungen in der Verordnung vorgegeben: • Systematische Beschreibung • Bewertung Verarbeitungsvorgänge • Bewertung Risiken • Abhilfemaßnahmen zur Bewältigung von Risiken • Nachweise zur Einhaltung der EU-DSGVO
VAK-Pflicht nur bei automatisierten Verfahren	Betrifft sämtliche Verarbeitungen
VAK-Zuständigkeit beim DSB	Zuständigkeit grundsätzlich beim Verantwortlichen aber Pflicht zur Einbeziehung des DSB; Verantwortlicher muss ggf. ASB vor Aufnahme der Verarbeitung konsultieren

Risikobasierter Datenschutz

BDSG-Alt	EU-DSGVO
Vorabkontrolle	**Generell risikobasierter Ansatz:** Maßnahmen stehen oftmals in direkter Abhängigkeit von den Risiken für die Betroffenen
TOMs nach Stand der Technik	Ein Datenschutzmanagement-System nach dem Vorbild von Compliance-Strukturen kann zweckmäßig sein
	Verknüpfung mit dem ISMS

Globale Anwendung der DSGVO

BDSG-Alt	EU-DSGVO
Sitzprinzip, Niederlassungsprinzip, Territorialprinzip, Transit durch das Inland	Sitzprinzip, Niederlassungsprinzip, **Marktortprinzip**
	Wegen dem Marktortprinzip gilt die EU-DSGVO grundsätzlich unabhängig davon, wo die Datenverarbeitung stattfindet oder wo der Sitz der verarbeitenden Stelle ist
	Bei **global agierenden Unternehmen** kann Pflicht zur Umsetzung der EU-DSGVO auch **in Drittstaaten** erwachsen

Vorrang der DSGVO vor nationalen Vorschriften

BDSG-Alt	EU-DSGVO (Art. 288 II AEUV)
BDSG als **nationale Vorschrift** entfaltet unmittelbare Wirkung gegenüber Bürgern und Unternehmen. BDSG-Alt ist ein „**Auffanggesetz**“	EU-DSGVO geht als europäische **Verordnung** dem nationalen Recht vor
Bei Abweichung von der Richtlinie 95/46/EG ist ggf. eine „richtlinienkonforme“ Auslegung des BDSG erforderlich	Gestaltungspielraum des nationalen Gesetzgebers, soweit die EU-DSGVO eine nationale Regelung vorsieht
	Strittig: EU-DSGVO-Konformität des BDSG-Neu

Erweiterte Transparenzanforderungen

§§ 4 III, 33 BDSG-Alt	Art. 5 I, Art. 13 bis Art. 15, Art. 16 bis 22, Art. 34 EU-DSGVO
Informationspflicht bei der Erhebung beim Betroffenen	**Transparenzgrundsatz** als wesentliches Prinzip der EU-DSGVO: „präzise, transparent, verständlich und in leicht zugänglicher Form in einer klaren und einfachen Sprache“
Informationspflicht bei der Speicherung ohne Kenntnis des Betroffenen	**Informationen** bei der Erhebung beim Betroffenen (Art. 13) oder im Falle einer Erhebung auf anderem Wege (Art. 14) und bei Mitteilungen iRd. Auskunftsrechts (Art. 15)
Informationspflicht bei der Speicherung zu Zwecken der Übermittlung ohne Kenntnis des Betroffenen	Recht auf **Berichtigung** (Art. 16), **Löschung** (Art. 17), **Einschränkung** der Verarbeitung (Art. 18), **Unterrichtungen an Dritte** über Löschung und Einschränkung (Art. 19), **Datenübertragbarkeit** (Art. 20), **Widerspruch** (Art. 21), **Datenpanne** (Art. 34)

Datensicherheit

§ 9 BDSG-Alt inkl. Anlage	Art. 32 EU-DSGVO
Verstoß nicht bußgeldbewehrt	**Bußgeld** in Höhe von 10 Mio. Euro, bzw. 2 % des weltweiten Jahresumsatzes
Vorgabe konkreter Kontrollen in der Anlage zu § 9 BDSG-Alt; Zielsetzung: Vertraulichkeit, Integrität und Verfügbarkeit	**Keine konkreten Kontrollen in der EU-DSGVO**: Pseudonymisierung und Verschlüsselung; Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit; Notfallplanung; Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit **Konkrete Kontrollen im BDSG-Neu:** Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle, Übertragungskontrolle, Eingabekontrolle, Transportkontrolle, Wiederherstellbarkeit, Zuverlässigkeit, Datenintegrität, Auftragskontrolle, Verfügbarkeitskontrolle, Trennbarkeit
Stand der Technik, Verhältnismäßigkeit	Stand der Technik, Verhältnismäßigkeit, **risikobasierter Ansatz**

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

§§ 3a, 9 BDSG-Alt	EU-DSGVO
Datenvermeidung und Datensparsamkeit	IT-Systeme müssen Datengrundsätze nach Art. 5 EU-DSGVO umsetzen, insb. Datenminimierung; IT-Systeme sollen “datenschutzfreundlich“ eingestellt sein (Berücksichtigung des Erforderlichkeitsprinzips)
TOMs gemäß Anlage nach § 9 BDSG	Berücksichtigung bei Entwicklung und Ausgestaltung von IT-Produkten, Diensten und Anwendungen
Nicht bußgeldbewehrt	Verstoß kann mit einem Bußgeld von bis zu 10 Mio. Euro oder 2 % des weltweiten jährlichen Umsatzes geahndet werden

Meldepflichten bei Datenschutzpannen

§ 42a BDSG-Alt	Art. 33 und Art. 34 EU-DSGVO
unrechtmäßige Übermittlung oder Kenntnisnahme; schwerwiegende Beeinträchtigung	**Verletzung des Schutzes** pD (Art. 4 Nr. 12): „Verletzung der Sicherheit, die zur **Vernichtung**, zum Verlust oder zur **Veränderung**, ob **zufällig** oder unrechtmäßig, oder zu unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“; kein geringes Risiko
ASB: Unverzüglich (h.M. ASB: innerhalb von 2 Wochen)	ASB: Unverzüglich und möglichst innerhalb von 72 Stunden
Bußgeldbewehrt: 300.000 Euro	Bußgeldbewehrt: 10 Mio. Euro bzw. 2 % des weltweiten jährlichen Umsatzes

Löschen von Daten und Recht auf Vergessenwerden

§ 35 BDSG-Alt	Art. 17 EU-DSGVO
„sind zu löschen“	“unverzüglich“ (Literatur: idR. innerhalb von 2 Wochen)
	Umfassendere Löschpflichten (bspw. auch bei Widerspruch ohne vorrangige berechtigten Gründe für weitere Verarbeitung, oder bei Direktwerbung)
Bußgeld von bis zu 300.000 Euro	Bußgeld von bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes

Zweckänderung und Vereinbarkeit

§§ 4 I, 28 II BDSG-Alt	Art. 6 IV EU-DSGVO
Für eigene Geschäftszwecke entspr. **Güterabwägung** und bei **öffentl. zugänglichen Daten**	**Vereinbarkeit mit ursprünglichem Zweck**: • Verbindung zwischen ursprünglichem und neuem Zweck • Kontext der Datenerhebung • Art der Daten • Mögliche Folgen der Weiterverarbeitung • Vorhandensein von Garantien (insb. Verschlüsselung und Pseudonymisierung)
	Erwägungsgrund 50: Berücksichtigung der „**vernünftigen Erwartungen** der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“ (ggf. Vorabinformation in Datenschutzrichtlinien)

Erleichterter Datenaustausch im Konzern

BDSG-Alt	Art. 6 I lit. (f) EU-DSGVO
Kein Konzernprivileg: Konzernunternehmen sind untereinander "Dritte"	**Weniger strenge Anforderungen**, aber kein vollständiges Konzernprivileg; Transparenz sollte beachtet werden (vgl. Güterabwägung unten)
	Keine Unterscheidung zwischen Datenverarbeitung zu **eigenen Zwecken** und zur **Wahrung berechtigter Interessen Dritter**
	Erw.Gr. 48: „**Verantwortliche**, die Teil einer **Unternehmensgruppe** [...] sind, die einer **zentralen Stelle zugeordnet** sind, können ein **berechtigtes Interesse** haben, pD innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschl. der Verarb. pD von **Kunden und Beschäftigten**, zu übermitteln."

Koppelungsverbot bei Einwilligungen

§ 28 IIIb BDSG-Alt	Art. 7 EU-DSGVO
Ausdrückliches Koppelungsverbot bei marktbeherrschenden Unternehmen (Adresshandel und Werbung)	Erw.Gr. 32: „Einwilligung sollte durch eine **eindeutige Handlung** erfolgen, mit der **freiwillig**, für den **konkreten Fall**, in **informierter** Weise und **unmissverständlich** beurkundet wird, dass betroffene Person mit der Verarbeitung ihrer personenbezogener Daten einverstanden ist“
Freiwilligkeit zweifelhaft bei großen Ungleichgewicht (früher strittig bspw. bei sog. „Schufa-Klausel“)	Erw.Gr. 43: Einwilligung **nicht freiwillig**: „wenn die Erfüllung eines Vertrages, einschließlich der Erbringung von Dienstleistungen, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

Dokumentationspflichten

Erwägungsgrund 82

- Nachweis der Einhaltung der Verordnung
- Pflicht zur Zusammenarbeit mit Aufsichtsbehörde
  -> Vorlagepflicht auf Anfrage
- Teil der Datenschutz Organisation
- Auch für Auftragsverarbeiter
- Keine Meldepflicht mehr

Demonstrating Compliance

Dokumentationspflichten – was muss dokumentiert werden?

Bisher:

- Meldepflicht automatisierter Verarbeitung oder Führung eines Verfahrensverzeichnisses (wenn DSB bestellt)
- Verfahrensverzeichnis ist öffentlich einsehbar

Neu:

- DS-Managementsystem
- DS-Organisation
- DS-Policies
- Zuständigkeiten
- Verarbeitungsvorgänge = Verfahrensverzeichnis
- Sensibilisierung & Schulung der Mitarbeiter
- Risikobewertungen
- DS-Folgenabschätzung
- DS-Verstöße/Vorfälle
- Implementierte & durchgeführte Kontrollen

Dokumentationspflichten - Verfahrensverzeichnis

- Name + Kontaktdaten des Verantwortlichen, ggfs. DSB
  -> Eindeutige Identifikation
- Zwecke der Verarbeitung
- Kategorien
  - Der betroffenen Personen
  - Der personenbezogenen Daten
- Kategorien von Empfängern, inkl. Empfänger in Drittländern
- Übermittlung von pers.-bez. Daten in Drittland
- Löschfristen zu Datenkategorien
- Allg. Beschreibung der TOM

Zusammenfassung

- Allgemeine Datenschutzgrundsätze werden nicht neu erfunden
- Im Ergebnis zusätzliche und teilweise strengere Anforderungen
- Hohe Anforderungen an Transparenz und Dokumentation
- Massive Verschärfung der Bußgeldtatbestände
- IT-Systeme und Prozesse im Unternehmen müssen überprüft und ggf. angepasst werden
- Einführung eines Datenschutz Management Systems angezeigt
- Dokumentation einführen/ergänzen

problems?

frog me !

RAin Dorothea Teichmann

teichmann@cyberlegal.de

Niedermeier & Faulhaber
Rechtsanwaltskanzlei
Partnerschaft mbB
Maximilanstr. 13
80539 München

http://www.cyberlegal.eu