

A photograph of a modern, multi-story office building with a prominent glass facade and a central tower. The building is set against a clear blue sky. A semi-transparent blue rectangular box is overlaid on the lower-left portion of the image, containing white text.

TÜV Rheinland.
Ihr Partner für Informationssicherheit.

2017

TÜV Rheinland i-sec. Informations- und IT-Sicherheit.

Führender unabhängiger Dienstleister
für Informationssicherheit in Deutschland

Beratungs- und Lösungskompetenz
in ganzheitlicher Informationssicherheit
– von der Steuerungsebene bis ins
Rechenzentrum inkl. betriebsunter-
stützender Leistungen

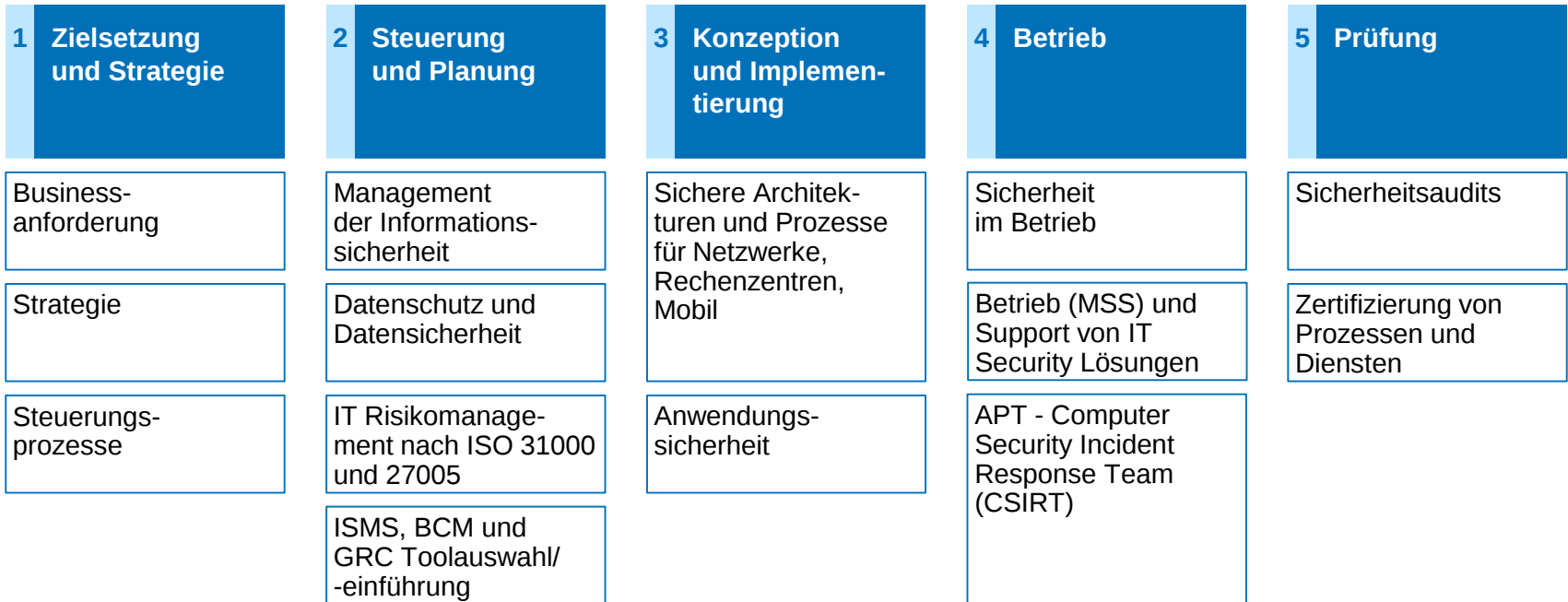
Exzellente Technologie-Expertise,
umfassendes Branchen-Know-how,
Partnerschaften mit Marktführern

International zählen wir im Verbund
mit unserer Schwestergesellschaft OpenSky
zu den wichtigsten unabhängigen Anbietern

Zertifiziert nach ISO 27001 und ISO 9001



Lösungskompetenz. Informations- und IT-Sicherheit.



Abkürzungsverzeichnis

ISMS = Information Security Management System
BCM = Business Continuity Management
GRC = Governance, Risk und Compliance
APT = Advanced Persistent Threat – gezielte Cyberangriffe
MSS = Managed Security Services



! Branchenlösungen, individuelle Konzepte, professionelle Beratung und stark in der Umsetzung.

EU-DSGVO
Anforderungen im Überblick
Roadshow, Mai 2017

Referent

Tilman M. Dralle

Funktion: Security Consultant, TÜV Rheinland

Fachgebiet: Datenschutzrecht



+49 221 56783 832



tilman.dralle@i-sec.tuv.com

Übersicht



Die neue Struktur des Datenschutzrechts in der Europäischen Union



Die Grundpfeiler des alten und neuen Rechts: Was sich **NICHT** ändert



Die wichtigsten Änderungen im Überblick: DSGVO „in a nutshell“



Öffnungsklauseln in der DSGVO: Das BDSG 2018



Ergebnisse

Übersicht



Die neue Struktur des Datenschutzrechts in der Europäischen Union



Die Grundpfeiler des alten und neuen Rechts: Was sich **NICHT** ändert



Die wichtigsten Änderungen im Überblick: DSGVO „in a nutshell“

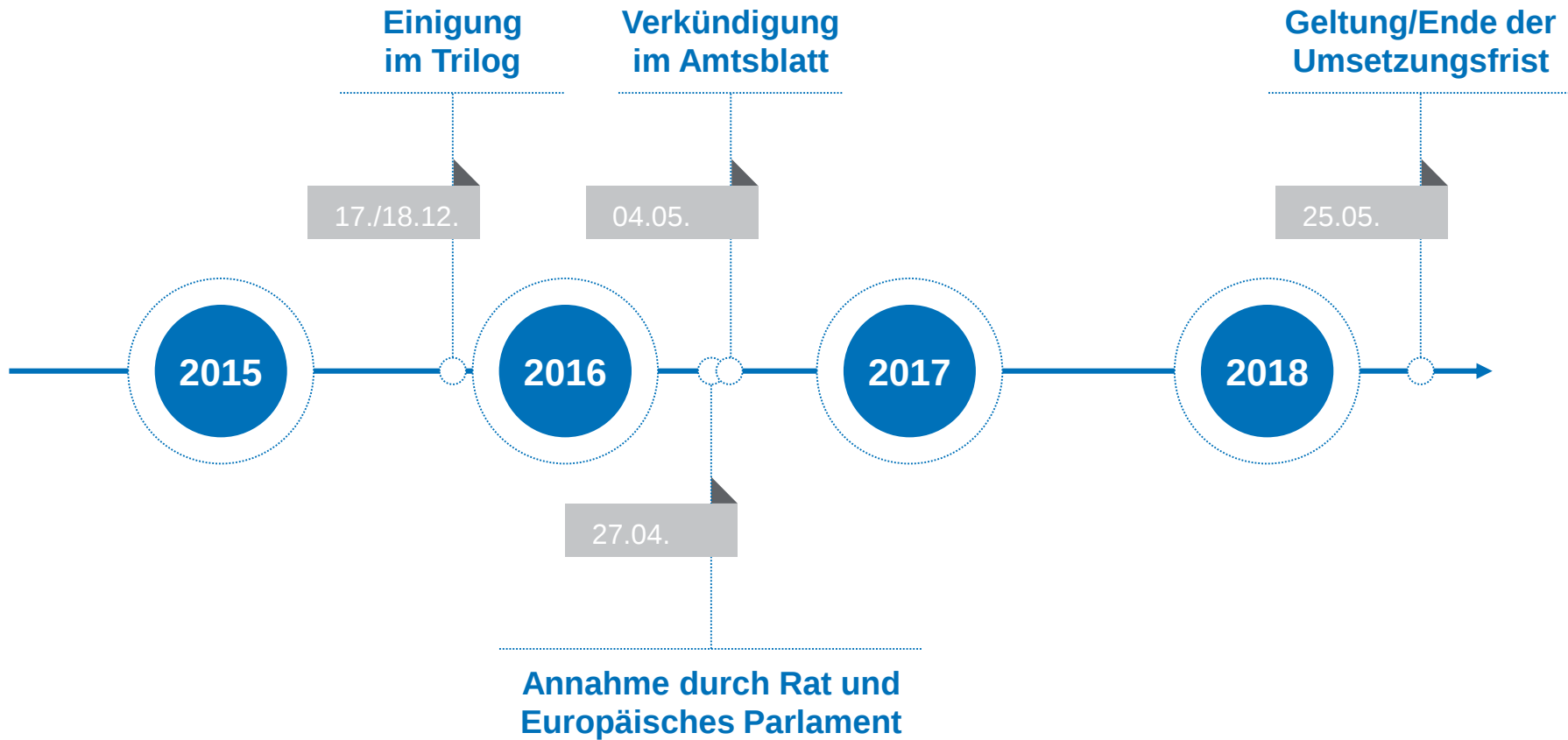


Öffnungsklauseln in der DSGVO: Das BDSG 2018

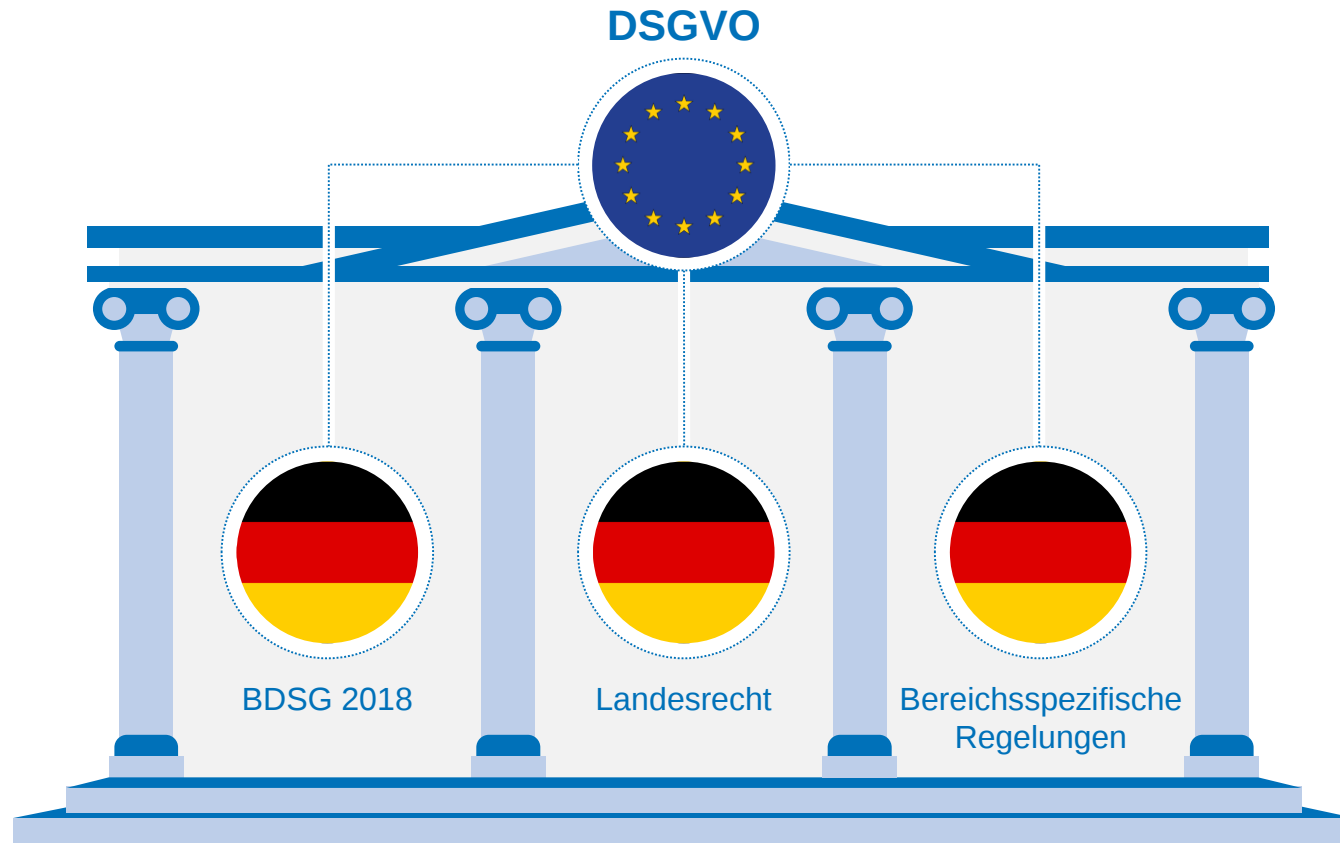


Ergebnisse

DSGVO-Timeline



DSGVO: Deutsches Recht wird abgelöst



Übersicht



Die neue Struktur des Datenschutzrechts in der Europäischen Union



Die Grundpfeiler des alten und neuen Rechts: Was sich **NICHT** ändert



Die wichtigsten Änderungen im Überblick: DSGVO „in a nutshell“



Öffnungsklauseln in der DSGVO: Das BDSG 2018



Ergebnisse

Grundpfeiler bleiben bestehen

An der Grundstruktur des Datenschutzes ändert sich nichts:

Verbotsprinzip mit Erlaubnisvorbehalt

Transparenz gegenüber Betroffenen

Anwendungsbereich: automatisiert
oder dateigebunden verarbeitete pbD

Betroffenenrechte und
Haftungsansprüche

Bestellpflicht eines DSB

Pflicht zur Ergreifung technisch-
organisatorischer Maßnahmen

Grundsätze der Erforderlichkeit
und Zweckbindung

Rolle staatlicher Aufsichtsbehörden
und deren Sanktionsinstrumentarium



Grundpfeiler bleiben bestehen

An der Grundstruktur des Datenschutzes ändert sich nichts:

Verbotsprinzip mit Erlaubnisvorbehalt

Transparenz gegenüber Betroffenen

Anwendungsbereich: automatisiert
oder dateigebunden verarbeitete personenbezogene Daten

Betroffenenrechte und
Haftungsansprüche

Achtung: DSGVO bringt gegenüber bisheriger
Rechtslage erhebliche Veränderungen!

Bestellpflicht eines DSB

technisch-organisatorischer Maßnahmen

Grundsätze der Erforderlichkeit
und Zweckbindung

Rolle staatlicher Aufsichtsbehörden
und deren Sanktionsinstrumentarium

Übersicht



Die neue Struktur des Datenschutzrechts in der Europäischen Union



Die Grundpfeiler des alten und neuen Rechts: Was sich **NICHT** ändert



Die wichtigsten Änderungen im Überblick: DSGVO „in a nutshell“



Öffnungsklauseln in der DSGVO: Das BDSG 2018



Ergebnisse

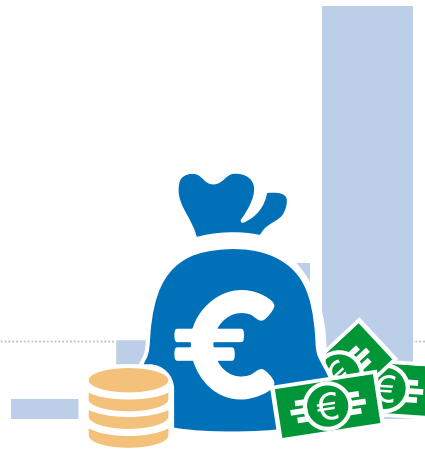
Bußgelder steigen drastisch

Gravierende Verschärfung gegenüber dem alten Recht:

Maximale Geldbuße nach
BDSG: 300.000 EUR

Bußgelder für Unternehmen:

Bis zu 20 Mio. EUR bzw. 4%
des gesamten weltweit erzielten
Jahresumsatzes



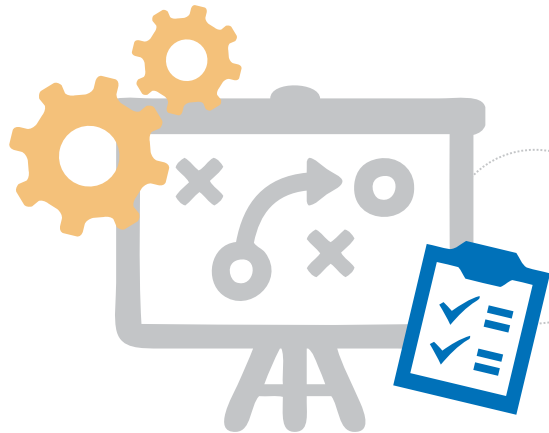
Geldbußen für Verstöße gegen die DSGVO müssen:

„**wirksam**, verhältnismäßig
und **abschreckend**“ sein

Wichtige Kriterien zur Bußgeldbemessung:

U.a.: Frühere Verstöße,
getroffene TOMs, Zusammen-
arbeit mit den Aufsichtsbe-
hörden, Zertifizierungsverfahren

Technische und organisatorische Maßnahmen



Nach DSGVO müssen TOMs ...

- ... das **Risiko für die Rechte und Freiheiten natürlicher Personen** berücksichtigen
- ... **regelmäßig** auf ihre Wirksamkeit hin **überprüft, bewertet und evaluiert** werden
- ... den „**Stand der Technik**“ umsetzen

Neben den klassischen Schutzziele der IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – fordert die DSGVO auch die **Belastbarkeit** von Systemen und Diensten

Verstoß ist **bußgeldbewehrt**
(10 Mio. EUR bzw. 2% des Vorjahresumsatzes)

Rechenschafts- und Dokumentationspflichten



Der Verantwortliche muss geeignete Maßnahmen ergreifen, um den **Nachweis dafür erbringen zu können**, dass die Verarbeitung pbD gemäß den Bestimmungen der DSGVO erfolgt

Erfüllung der Rechenschafts- und Dokumentationspflichten relevant ...

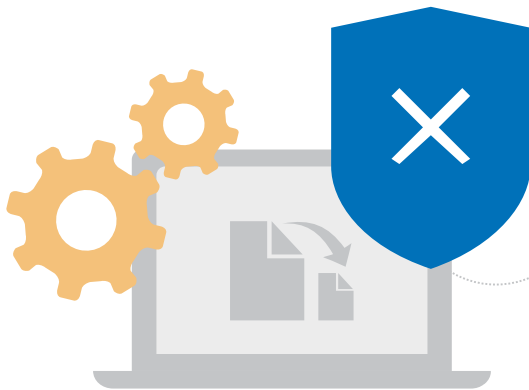
... bei **Prüfungen durch die Aufsichtsbehörden**

... bei der **Geltendmachung von Schadensersatzansprüchen** durch Betroffene

Zusätzliche Pflichten in der DSGVO + Rechenschafts- bzw. Nachweiserfordernisse

➔ Ohne **Datenschutz-Management-System** geht es nicht!

Privacy by design & Privacy by default



Datenschutz durch Technikgestaltung

- Bereits bei der **architektonischen Entwicklung und Gestaltung von Produkten, Diensten und Anwendungen** müssen geeignete TOMs getroffen werden
- **Normadressat** ist die verantwortliche Stelle (!)

Datenschutz durch datenschutzfreundliche Voreinstellungen

- „**Werkseitig**“ **vorgenommene Einstellungen** müssen dem **Gebot der Datenminimierung** entsprechen

„Privacy by design“ und „Privacy by default“ -Vorgaben gelten ab dem **25. Mai 2018 auch für bereits vorhandene Produkte, Dienste und Anwendungen**



Das Recht auf Datenübertragbarkeit
als **neues Betroffenenrecht**

- Betroffene haben das Recht, pbD in einem **strukturierten, gängigen und maschinenlesbaren** Format zu erhalten
- Betroffene haben ferner das Recht zu erwirken, dass die pbD **direkt von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden**

Erhalt und Übermittlung der pbD erfolgen **unentgeltlich**

Recht auf Datenportabilität **auch für mittelständische Unternehmen relevant** – Beispiel: Informationen über Einkäufe mit verschiedenen Kundenkarten

Recht auf Löschung („Vergessenwerden“)



Allgemeine Löschpflicht

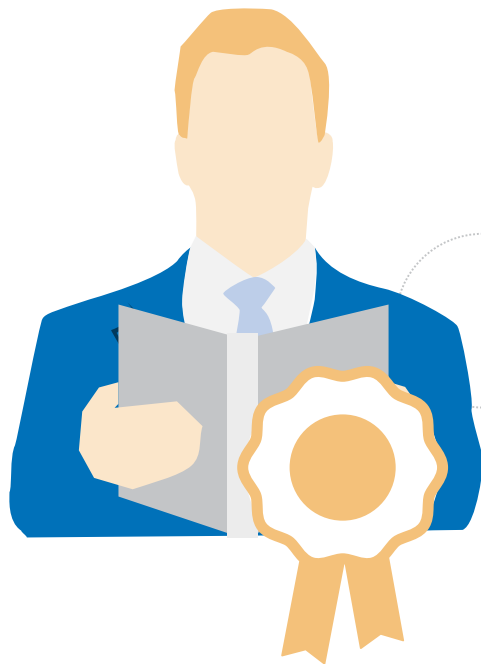
- U.a. bei Zweckverbrauch, Widerruf der Einwilligung, Widerspruch etc.

Neu: „Recht auf Vergessenwerden“

- Ausgangspunkt: EuGH-Entscheidung in der Rs. Google/Spain
- **Dritte müssen** ggf. **über Löschantrag informiert werden**
- Der Verantwortliche muss **angemessene technische und organisatorische Maßnahmen** ergreifen, um die jeweiligen Dritten zu identifizieren

Reichweite des „Rechts auf Vergessenwerden“ unklar:
Erhebliche Unsicherheiten!

Zertifizierungsverfahren



Im **BDSG** war die Möglichkeit eines bundesweiten, freiwilligen Datenschutzaudits bereits angelegt

- Allerdings: entsprechendes **Ausführungsgesetz** wurde **nie erlassen**

DSGVO sieht nun **datenschutzspezifische Zertifizierungsverfahren** vor

- Verantwortliche und Auftragsverarbeiter können darüber künftig den Nachweis erbringen, dass ihre Datenverarbeitung in Einklang mit der Verordnung steht

Zertifizierungen spielen bei der Entscheidung über **das Ob und die Höhe von Bußgeldern** eine wichtige Rolle

Großes Potenzial als **wettbewerbsdifferenzierendes Element**

Übersicht



Die neue Struktur des Datenschutzrechts in der Europäischen Union



Die Grundpfeiler des alten und neuen Rechts: Was sich **NICHT** ändert



Die wichtigsten Änderungen im Überblick: DSGVO „in a nutshell“



Öffnungsklauseln in der DSGVO: Das BDSG 2018



Ergebnisse

Öffnungsklauseln

Deutscher Bundestag

18. Wahlperiode

Drucksache 18/11325

24.02.2017



Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

A. Problem und Ziel

Am 25. Mai 2018 wird die Verordnung (EU) 2016/679 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 Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der Verordnung (EU) 2016/679 ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten (Erwägungsgrund 10). Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die Verordnung (EU) 2016/679 sieht eine Reihe von Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Verordnung (EU) 2016/679 konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergibt sich gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht.

Darüber hinaus dient der vorliegende Gesetzentwurf der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89), soweit die der Richtlinie unterfallenden Staaten nach deren Artikel 63 verpflichtet sind, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen. Die Umsetzung der Richtlinie (EU) 2016/680 wird über die im vorliegenden Gesetzentwurf enthaltenen relevanten Regelungen hinaus auch noch gesondert im Fachrecht erfolgen.

Um ein reibungsloses Zusammenspiel der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 mit dem stark ausdifferenzierten deutschen Datenschutzrecht sicherzustellen, ist es erforderlich, das bisherige Bundesdatenschutzgesetz (BDSG) durch ein neues Bundesdatenschutzgesetz abzulösen. Weiterer ge-

Ziel der Harmonisierung des europäischen Datenschutzrechts nicht vollständig umgesetzt

DSGVO enthält 50 sogenannte „Öffnungsklauseln“: Handlungsspielraum für den nationalen Gesetzgeber

Deutschland: „Datenschutz-Anpassungs- und Umsetzungsgesetz EU“: Grundlage für das neue BDSG 2018

Kosten sparen durch Ausnahmeregelungen oder Bekenntnis zum „Gold-Standard“ der DSGVO?

Öffnungsklauseln

Bereiche, die durch das BDSG 2018 mit-geregelt werden:

Videoüberwachung öffentlich zugänglicher Räume

Informationspflicht, wenn die pbD nicht bei der betroffenen Person erhoben wurden

Verarbeitung besonderer Kategorien pbD

Auskunftsrecht der betroffenen Person

Verarbeitung zu anderen Zwecken

Recht auf Löschung

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Automatisierte Entscheidungen im Einzelfall

Informationspflicht bei Erhebung von pbD bei der betroffenen Person

Datenschutzbeauftragte nicht-öffentlicher Stellen

Strafvorschriften



Übersicht



Die neue Struktur des Datenschutzrechts in der Europäischen Union



Die Grundpfeiler des alten und neuen Rechts: Was sich **NICHT** ändert



Die wichtigsten Änderungen im Überblick: DSGVO „in a nutshell“



Öffnungsklauseln in der DSGVO: Das BDSG 2018



Ergebnisse



- Es wird komplizierter: **„Ein Gesetz geht, zwei Gesetze kommen“**
- Erhebliche Veränderungen gegenüber der bisherigen Rechtslage: **Betroffenenrechte werden gestärkt, Unternehmenspflichten ausgebaut**
- **Bußgeldrahmen steigt drastisch: bis zu 4% des globalen Vorjahresumsatzes;** Fast jede Vorschrift der DSGVO ist bußgeldbewehrt
- Es geht nicht mehr ohne: **Effektive Datenschutz-Management-Systeme sind gefragt**
- Neue Möglichkeiten der datenschutzrechtlichen Compliance: **Datenschutz-Zertifizierung als Chance**

Fragen?

Tilman M. Dralle

Security Consultant

TÜV Rheinland i-sec GmbH

Am Grauen Stein

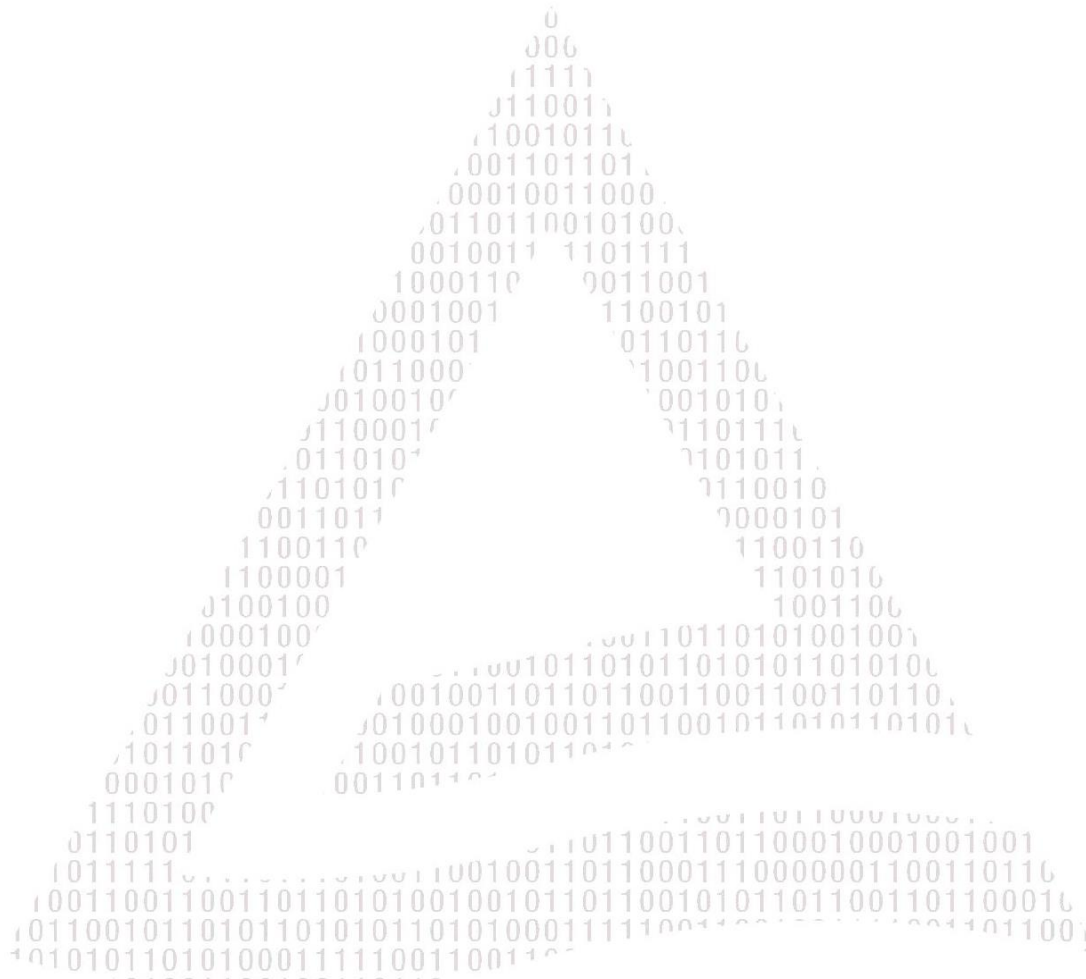
51105 Köln

Tel: +49 221 56783 832

Fax: +49 221 806 1580

tilman.dralle@i-sec.tuv.com

www.tuv.com/informationssicherheit





www.tuv.com/it-sicherheits-kongress

8. IT-Sicherheits-Kongress 2017

Cyber Security und Qualität in der digitalen Transformation

7. – 8. November in Frankfurt am Main