nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

EU Datenschutz-Grundverordnung

Stichtag: 25.05.2018

11.04.2018

Stefan Sander, LL.M., B.Sc.

SDS Rechtsanwälte
Sander Schöning PartG mbB

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen

sds Rechtsanwälte SANDER SCHÖNING PartG mbB

Zur Person / Zum Thema

- Ihr Referent
  - Rechtsanwalt und Fachanwalt für IT-Recht
  - Software-Systemingenieur
  - Datenschutzbeauftragter (TÜV)

- Verordnung (EU) 2016/679 („Datenschutz-Grundverordnung“)
  - Amtsblatt der Europäischen Union vom 04.05.2016
  - http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.html
  - anzuwenden in allen EU Mitgliedsstaaten ab dem 25.05.2018

Agenda

- Ausgewählte Aspekte:
  - Motivation für Änderungen im Betrieb
  - Sachlicher Anwendungsbereich
  - Der Verantwortliche
  - Allgemeine Pflichten des Verantwortlichen
  - Zulässigkeit der Verarbeitung, insb. Werbung
  - Übermittlungen in Drittländer

Motivation für Änderungen im Betrieb

Motivatoren

- Art. 83 DS-GVO – Geldbußen
  - (1) Geldbußen müssen in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** sein.
  - (4) Bei Verstößen gegen […]
    - „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“
  - (5) Bei Verstößen gegen […]
    - bis zu 20 000 000 EUR oder 4% des Jahresumsatzes
  - (6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde […]
    - bis zu 20 000 000 EUR oder 4% des Jahresumsatzes

Grundsätze für die Verarbeitung, Art. 5

- Abs. 1: „Personenbezogene Daten müssen …“
  - **Rechtmäßigkeit**, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung (inkl. Pflicht zur „Anonymisierung“)
  - Integrität und Vertraulichkeit
- Abs. 2 „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und **muss dessen Einhaltung nachweisen können**.“

Exkurs: Schadensersatz, Art. 82

- Abs. 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**."

- Abs. 3: Vermutung für ein Verschulden
- Abs. 4: Gesamtschuldnerische Haftung **aller Beteiligten**

- kein Haftungsausschluss entspr. § 8 Abs. 2 BDSG
- keine Haftungsbegrenzung entspr. § 8 Abs. 3 BDSG

Von welcher Seite droht Ungemach?

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

- Aufsichtsbehörden
- Datenschutzbeauftragte
- Die betroffenen Personen
- Datenschutzvereine
- Verbraucherschützer
- Betriebsräte
- Konkurrenten

sds
Rechtsanwälte
SANDER SCHÖNING
PartG mbB

Datenschutz als Aufgabe

- Wen trifft die Aufgabe „Datenschutz“
  - den „Verantwortlichen“
    - d.h. Aufgabe des Unternehmens
      - d.h. **Aufgabe der Geschäftsführung**

- Möglichkeiten:
  - Horizontale Delegation
  - Vertikale Delegation

- Wen trifft die Aufgabe „Datenschutz“ nicht?
  - den Datenschutzbeauftragten des Unternehmens
    - **Delegation der Aufgabe an den DSB verboten,** Art. 38 Abs. 6 S. 2 DSGVO

Sachlicher Anwendungsbereich

IT-Sicherheit und Datenschutz

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

- Informationssicherheit ≠ nur sichere Computer
  - Vgl.: Art. 2 Abs. 1 DSGVO: nichtautomatisierte Verarbeitungen
- Vorsicht vor Trugschlüssen: „Schutzbedarf von Daten“ und „sensible Daten“
  - BVerfGE 65, 1 (Volkszählungsurteil)
- Art. 4 Nr. 1 DSGVO: Im Sinne dieser Verordnung bezeichnet der Ausdruck: „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** (im Folgenden „betroffene Person“) beziehen
- Unterschiede in der Perspektive: Wer ist zu schützen?

sds Rechtsanwälte SANDER SCHÖNING PartG mbB

Die Verordnung (EU) 2016/679

- Art. 2 Abs. 1 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.

- Art. 2 Abs. 2 DSGVO
  - Ausnahmen, u.a. lit. c) „Haushaltsausnahme“
    - EuGH, Urt. v. 11.12.2014 - C-212/13

Personenbezogene Daten

- Art. 4 Nr. 1: „Personenbezogene Daten“ sind 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, […], identifiziert werden kann;

- Wissen des Verantwortlichen oder der Welt?

  - ErwG 26: Welche Mittel wird der Verantwortliche oder eine andere Person „**nach allgemeinem Ermessen wahrscheinlich**“ einsetzen? Zu beurteilen anhand aller **objektiven Faktoren**, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, unter Berücksichtigung verfügbarer Technologien und technologischer Entwicklungen.

Identifizierbarkeit betroffener Personen

- Zur Frage, unter welchen Voraussetzungen eine Person identifizierbar ist:
  - EuGH, Urt. v. 19.10.2016 - C-582/14
    Patrick Breyer gegen Bundesrepublik Deutschland
- Auch de facto nicht vorhandenes Kontextwissen wird unterstellt, soweit der Verantwortliche über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die ein Dritter verfügt, bestimmen zu lassen.

Der Verantwortliche

Der Verantwortliche, Art. 4 Nr. 7

- „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **die allein oder gemeinsam mit anderen** über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

- **Inhaltsgleich** mit Art. 2 lit. d RL 95/46/EG
  - Anders noch § 3 Abs. 7 BDSG:
    „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“

“gemeinsam mit anderen”

- OVG Schleswig, Urt. v. 4.9.2014 - 4 LB 20/13
  - Untersagungsverfügung des ULD aufgehoben, mit der Begründung: „Eine Stelle, die weder einen rechtlichen noch tatsächlichen Einfluss auf die Datenverarbeitung hat, ist keine verantwortliche Stelle i.S.v. § 3 Abs. 7 BDSG.“
- BVerwG, Beschl. v. 25.2.2016 – 1 C 28.14
  - **EuGH, C-210/16 (Urteil steht aus)**
    - EuGH, C-40/17 (Urteil steht aus)

Allgemeine Pflichten des Verantwortlichen

Verzeichnis von Verarbeitungstätigkeiten

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

- Art. 30 Abs. 1: „Jeder **Verantwortliche** und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen."

- Art. 30 Abs. 2: „Jeder **Auftragsverarbeiter** und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung."

Technische und organisatorische Maßnahmen

- Art. 24 Abs. 1 DSGVO:
  - entspricht Art. 17 RL 95/46/EG
  - Fortführung von § 9 BDSG
- Art. 25 DSGVO
- Art. 32 Abs. 1 DSGVO
  - „risikobasierter Ansatz“
- Art. 32 Abs. 4, Art. 29 DSGVO
  - Fortführung von § 5 BDSG
- Trifft zunächst nur Auftragsverarbeiter: Art. 28 Abs. 3 S. 2 lit. e) DSGVO

Data Protection by design & by default

- Ablösung des „stumpfen Schwertes“ aus § 3a BDSG durch Art. 25, 83 Abs. 4 (10 Mio. / 2% Jahresumsatz)
- **Art. 25** weist Schnittmengen zu allgemeiner Daten-sicherheit des Art. 32 (= Verpflichtung TOM) auf
- Verpflichtung zum Einsatz datenschutzfreundlicher Techniken (Abs. 1) und Voreinstellungen (Abs. 2)
  - **Techniken**
    - Datenschutzgrundsätze wirksam umzusetzen
    - Anforderungen dieser Verordnung genügen
    - Rechte der betroffenen Personen schützen
  - **Voreinstellungen**
    - Menge der erhobenen personenbezogenen Daten
    - Umfang ihrer Verarbeitung
    - Speicherfristen
    - Zugänglichkeit

weitere ausgewählte Punkte

- Datenschutz-Folgenabschätzung, Art. 35, 36
- Datenschutzbeauftragter, Art. 37 – 39
- Benachrichtigungspflichten bei Datenschutzverstößen, Art. 33, 34
- Wesentliche Anforderung an die innerbetrieblich Organisation und eingesetzte Technik:
  - Ab dem 25.5.2018 müssen die Rechte der betroffenen Personen erfüllt werden, entsprechend **Art. 12 – 23** (und weiteren Einzelbestimmungen in anderen Art.)

Informationspflichten

- Art. 13 DSGVO (Direkterhebung)
  - (1)Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
    - a) Namen und Kontaktdaten des Verantwortlichen
    - b) Kontaktdaten des Datenschutzbeauftragten;
    - c) Zwecke und Rechtsgrundlagen der Verarbeitung
    - d) berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
    - e) gegebenenfalls die Empfänger oder Kategorien von Empfängern, falls Übermittlung beabsichtigt
    - f) Absicht der Übermittlung ins Drittland sowie Rechtsgrundlage

Informationspflichten

- Art. 13 DSGVO (Direkterhebung)
  - (2) Zusätzlich […] stellt der Verantwortliche […] zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung […]:
    - a) Dauer der Speicherung
    - b) Information über das Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung oder Widerspruch gegen die Verarbeitung sowie Rechts auf Datenübertragbarkeit;
    - c) Information über das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen
    - d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

Informationspflichten

- e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Zulässigkeit der Verarbeitung, insb. Werbung

Zulässigkeit der Verarbeitung

- ErwG 171: „Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. **Verarbeitungen, die** zum Zeitpunkt der Anwendung dieser Verordnung **bereits begonnen** haben, sollten **innerhalb von zwei Jahren** nach dem Inkrafttreten dieser Verordnung mit ihr **in Einklang gebracht werden**. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es **nicht erforderlich**, dass die betroffene Person **erneut** ihre **Einwilligung** dazu **erteilt, wenn** die Art der bereits erteilten Einwilligung den Bedingungen **dieser Verordnung entspricht**, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.“

Zulässigkeit der Verarbeitung

- Prüfung auf der **1. Stufe**
  - **Kapitel II – Art. 5 – 11**
    - Art. 5 – Grundsätze (inkl Rechenschaftspflicht)
    - **Art. 6 – Rechtmäßigkeit** der Verarbeitung
      - u.a. Art. 6 Nr. 1: Einwilligung → Art. 7, 8
    - **Art. 9, 10 - Rechtmäßigkeit** der Verarbeitung von „besonderen Arten von pbD"
    - Art. 11 – „anonyme" Verarbeitungen (s.o.)
  - **Kapitel IX – Art. 85 – 91**
- Prüfung auf der **2. Stufe**
  - **Kapitel V - Art. 44 – 50**

Rechtmäßigkeit der Verarbeitung, Art. 6

- Abs. 1: „Die Verarbeitung ist **nur** rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:“
  - **a) Einwilligung**
  - **b) Erfüllung eines Vertrags & vorvertragliche Maßnahmen**
  - **c) Erfüllung rechtlicher Pflichten des Verantwortlichen**
  - d) lebenswichtige Interessen der betroffenen Person oder eines Dritten
  - e) öffentliche Aufgabe & öffentliche Gewalt
  - **f) Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten**
- Abs. 4: Verarbeitungen nach **Zweckänderung**

Rechtmäßigkeit der Verarbeitung, Art. 9

- Abs. 1: „**Die Verarbeitung personenbezogener Daten,** aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt**."

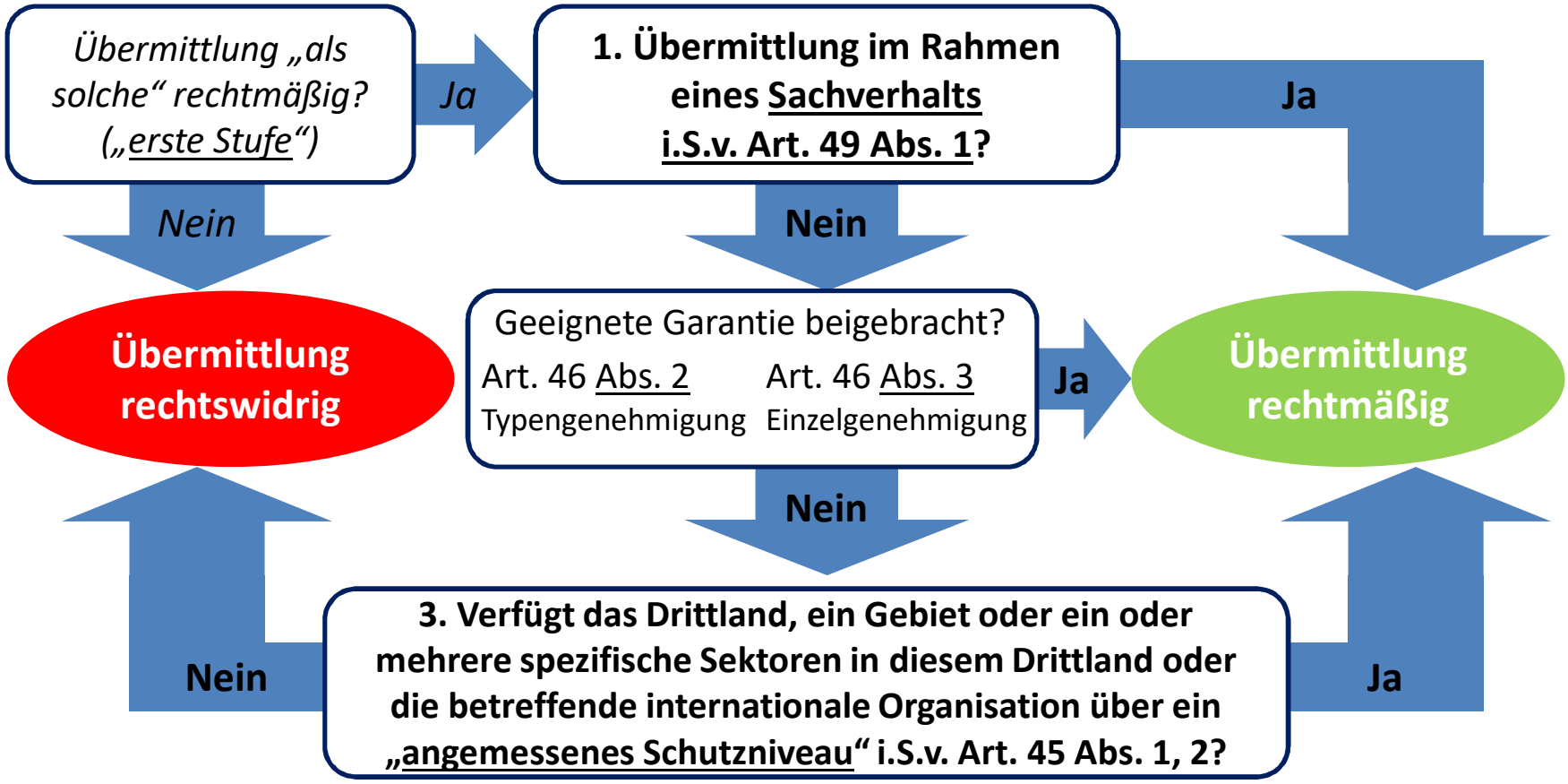
- Abs. 2: „Absatz 1 gilt nicht in folgenden Fällen: […]"
  - eigenständige Regelungen, d.h. keine Rückbezüge auf Art. 6 Abs. 1

Zulässigkeit von Werbung

- ErwG 38: Gewollt ist ein besonderer Schutz für pbD von Kindern im Zusammenhang mit Werbung.
- ErwG 47: „Die Verarbeitung personenbezogener Daten **zum Zwecke der Direktwerbung** kann als eine einem **berechtigten Interesse** dienende Verarbeitung betrachtet werden.“
- ErwG 70: „Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so sollte die betroffene Person jederzeit unentgeltlich insoweit Widerspruch gegen eine solche — ursprüngliche oder spätere — Verarbeitung einschließlich des Profilings einlegen können, als sie mit dieser Direktwerbung zusammenhängt. “
  - In Art. 21 Abs. 2, 3 entsprechend geregelt.

Übermittlungen in Drittländer

Übermittlungen in Drittländer, Art 44 ff.



Was ist zu tun?

Der Weg zur Umsetzung der DSGVO

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

- Die Notwendigkeit von qualifiziertem Personal
  - Verbot der Delegation von Aufgaben an den DSB
- „Strategien des Verantwortlichen“ zur Erfüllung seiner Aufgaben, u.a.:
  - Verzeichnis der Verarbeitungstätigkeiten
  - Informationspflichten
  - Datenschutz-Folgenabschätzung
  - Meldepflichten bei Datenschutzverletzungen
- Rechenschafts- und Nachweispflichten
  - DSMS / ISMS

sds
Rechtsanwälte
SANDER SCHÖNING
PartG mbB

Gibt es noch Fragen?

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Stefan Sander, LL.M., B.Sc.
Rechtsanwalt und Fachanwalt für IT-Recht
Software-Systemingenieur
Datenschutzbeauftragter (TÜV)

@: sander@sds.ruhr
T.: 0203 / 39208900

SDS Rechtsanwälte
Sander Schöning PartG mbB
Harmoniestraße 2a
47119 Duisburg-Ruhrort

www.sds.ruhr

?!

Vielen Dank
für Ihre
Aufmerksamkeit!

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen

sds Rechtsanwälte SANDER SCHÖNING PartG mbB