Das neue Datenschutzrecht – Herausforderungen (auch) für Vereine

Dr. Christoph Worms
Rechtsanwalt
Fachanwalt für Verwaltungsrecht

BRANDI
RECHTSANWÄLTE

Inhaltsübersicht

- Die Datenschutzgrundverordnung - Überblick und Anpassungsbedarf
- Risiko-Folgenabschätzung
- Auftragsdatenverarbeitung
- Data Breach Notification
- Verhältnis KUG zur DSGVO

BRANDI
RECHTSANWÄLTE

Die Datenschutzgrundverordnung - Überblick und Anpassungsbedarf

Agenda

- Einleitung
- Überblick DSGVO/Rechtmäßigkeit der Datenverarbeitung
- Sanktionen
- Handlungsbedarf
- Zusammenfassung

BRANDI
RECHTSANWÄLTE

Einleitung

BRANDI
RECHTSANWÄLTE

Einleitung

- **Hintergrund**
  - Harmonisierung der Regelungen in Europa
  - Stärkung des Datenschutzes
  - Schließung von Schlupflöchern, insb. für große Konzerne (Google, Facebook, etc.)
  - Keine Verhinderung des Datentransfers
- **Entstehungsgeschichte**
  - Langer Vorlauf (Erster Entwurf: 2012)
  - Kompromisse im Rahmen des Trilogs, insb. Öffnungsklauseln (Verständigung: 2015)
- **Zeitlinie**
  - Verabschiedet 2016
  - Ab 25. Mai 2018 anzuwenden

Einleitung

I

(Gesetzgebungsakte)

VERORDNUNGEN

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)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

Einleitung

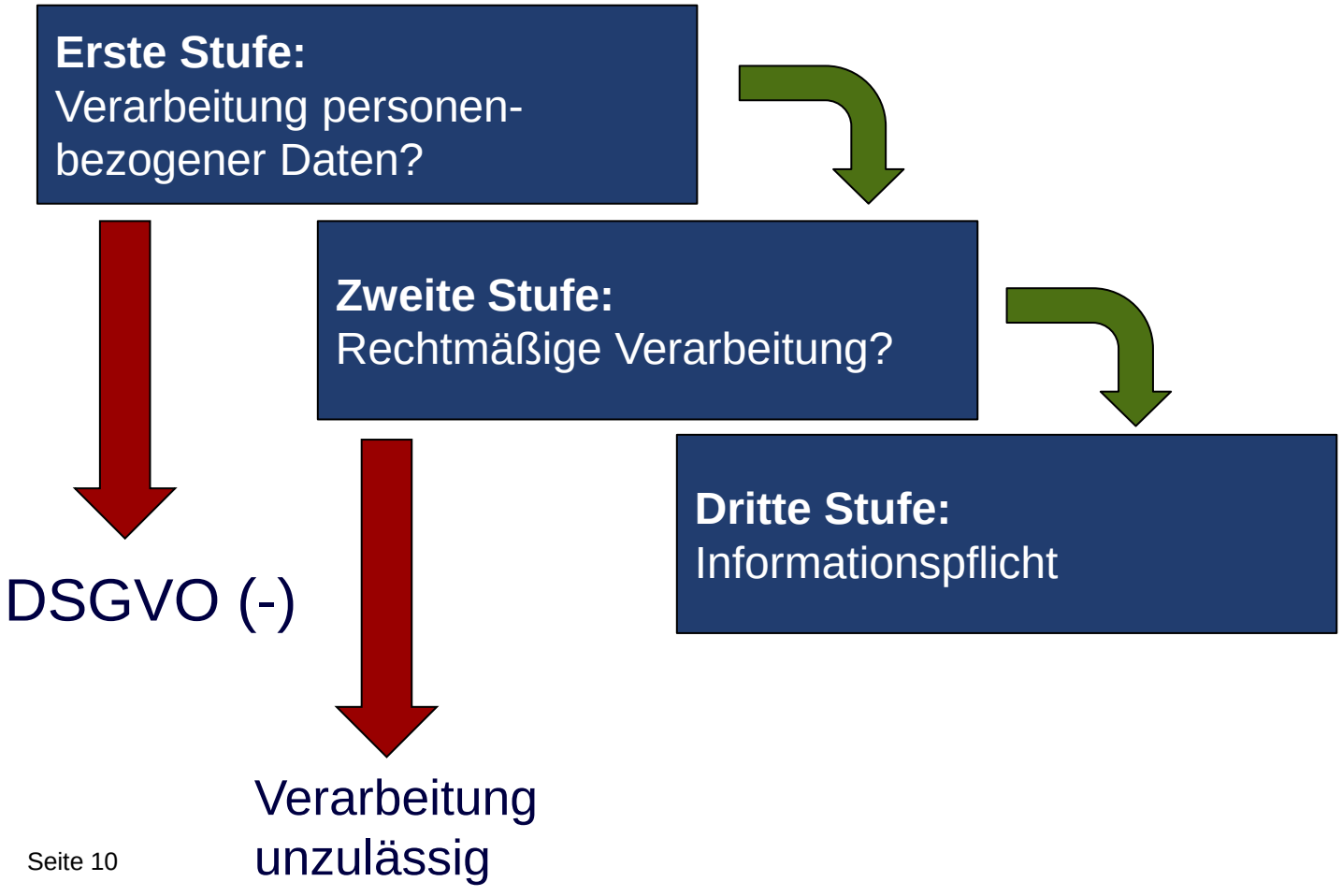
- **Grundstruktur der Verordnung**
  - Unmittelbare Anwendbarkeit
  - Struktur mit Artikeln und Erwägungsgründen
  - Keine nationale Umsetzung erforderlich
  - Öffnungsklauseln können auf nationaler Ebene ausgefüllt werden

- **BDSG neu**
  - Datenschutzbeauftragter
  - Beschäftigtendatenschutz

Überblick DSGVO
Rechtmäßigkeit der Datenverarbeitung

BRANDI
RECHTSANWÄLTE

Überblick


Erste Stufe:
Verarbeitung personen-bezogener Daten?
Zweite Stufe:
Rechtmäßige Verarbeitung?
Dritte Stufe:
Informationspflicht
DSGVO (-)
Verarbeitung unzulässig

Verbot mit Erlaubnisvorbehalt

- **Rechtmäßigkeit der Datenverarbeitung, Art. 5 Abs. 1 DSGVO**
  - Datenverarbeitung ist weiter nur bei Vorliegen einer Ermächtigungsgrundlage möglich
  - Kriterium der Verarbeitung „nach Treu und Glauben“ (engl.: „Fairness“) wird ausdrücklich festgeschrieben
  - Transparenz wird ausdrücklich festgeschrieben
  - Zweckbindung

Definition

- “personenbezogene Daten” = alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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.

Definition

- „Verarbeitung” jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Rechtmäßigkeit der Verarbeitung

- **Datenminimierung**
  - Bislang Grundsätze der Datensparsamkeit und Datenvermeidung

- **Privacy by design / by default**
  - Datenminimierung muss bei Gestaltung / Konzeption berücksichtigt werden
  - Voreinstellungen müssen datenschutzfreundlich gestaltet sein

Rechtmäßigkeit der Verarbeitung

- **Integrität und Vertraulichkeit**
  - BVerfG: „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (Urt. v. 22.07.2008)
  - Schutz durch geeignete technische und organisatorische Maßnahmen
  - Fortführung der Systematik der TOM, aber mit anderer Struktur
    - Stärkere Berücksichtigung von Anonymisierung und Pseudonymisierung
    - Einsatz von Verschlüsselung soll ausgebaut werden

Rechtmäßigkeit der Verarbeitung

- **Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO**
  - Der Verantwortliche muss die Einhaltung der Grundsätze nachweisen können
  - Zur Erfüllung der Nachweispflicht ist eine Dokumentation erforderlich
  - Rechenschaft ist auch für Haftung und Geldbußen relevant
  - Möglichkeiten des Nachweises: Verfahrensübersicht, Datenschutzkonzept, Datenschutzbericht, u.a.

Rechtmäßigkeit der Verarbeitung

- **Weitgehende Informationspflichten, Art. 13, 14 DSGVO**
  - Transparenz
  - Zwecke
  - Rechtsgrundlage
  - Speicherdauer
  - Datenschutzerklärung
    - Internetseite
    - Online-Plattformen
    - Apps

Ermächtigungsgrundlagen

- **Grundlagen der Datenverarbeitung – Ermächtigungsgrundlagen, Art. 6 DSGVO**
  - **Einwilligung**
  - **Vertragserfüllung**
  - Erfüllung rechtlicher Verpflichtungen des Verantwortlichen
    - Konflikte mit anderen rechtlichen Vorgaben werden jetzt korrekt aufgelöst
  - Schutz lebenswichtiger Interessen
  - Wahrnehmung einer Aufgabe im öffentlichen Interesse
  - Verarbeitung zur Wahrung der berechtigten Interesse des Verantwortlichen oder eines Dritten nach **Interessenabwägung**
    - Anwendungsbereich der berechtigten Interesse wird aufgewertet!

Ermächtigungsgrundlagen

- **Einwilligung, Art. 4 Abs. 11, Art. 7 DSGVO**
  - Anforderungen an die Einwilligung
    - In informierter Weise
    - Für den bestimmten Fall
    - Freiwillig
    - Unmissverständlich
  - Anforderungen an wirksame Einwilligung werden weiter verschärft
  - Einwilligung muss nachgewiesen werden können
    - Schriftform ist in der Regel empfehlenswert
  - Kopplungsverbot verbietet bisher übliche Abhängigkeiten

Neue Regelungen

- **Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO**
  - Bisher: Verfahrensverzeichnis, § 4e / § 4g BDSG
  - Öffentliches Verfahrensverzeichnis (Jedermann-Verzeichnis) entfällt insgesamt
  - Interne Dokumentation bleibt bestehen und wird ausgebaut
  - Ausnahmeregelung für Kleinunternehmen
    - Pflicht zur Führung entfällt bei weniger als 250 Mitarbeitern

    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.

Neue Regelungen

- **Datenschutz-Folgenabschätzung, Art. 35 DSGVO**
  - Bisher: Vorabkontrolle, § 4d BDSG
  - Zusätzliche Kontrolle bei besonderen Risiken
    - Verwendung neuer Technologien (etwa Big Data)
    - Art und Umfang der Datenverarbeitung
    - Ausdrücklich genannt: Profiling (auch Matching von Anbieter – Bewerber)
  - Umfassende Risikoabwägung
  - Überprüfung möglicher Schutzmaßnahmen
  - Dokumentation des gesamten Vorgangs erforderlich

Neue Regelungen

- **Datenschutzbeauftragter, Art. 37 ff. DSGVO**
  - Funktion des Datenschutzbeauftragten wird europaweit eingeführt
    - Nach Datenschutz-Grundverordnung keine Anknüpfung an Unternehmensgröße
    - Bestellpflicht hängt zukünftig von Kerntätigkeit eines Unternehmens ab
    - Aber: bisherige Gestaltung wird durch Nutzung von Öffnungsklauseln beibehalten
  - Anforderungen bleiben hoch
    - Berufliche Qualifikation und Fachwissen wird gefordert, Art. 37 Abs. 5 DSGVO
    - Neu wird außerdem auch Bezug auf Datenschutzpraxis genommen
    - Inkompatibilität mit leitenden Aufgaben
    - Besonderer Schutz gegen Benachteiligung
  - Aufgabenkatalog ist leicht modifiziert
    - Datenschutzbeauftragter soll weiterhin beratende Funktion haben und Ansprechpartner sein

Datenschutzbeauftragter

§ 38 Abs. 1 BDSG-neu:

„Ergänzend zu Artikel 37 […] 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. […]“

§ 26 Abs. 8 BDSG-neu: Definition des Beschäftigtenbegriffs.

Im Vergleich zu der bisherigen Definition aus § 3 Abs. 11 BDSG-alt bezieht sich die Definition nunmehr ausdrücklich auch auf Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher und auf Freiwillige, die einen Dienst nach dem Bundesfreiwilligendienstgesetz leisten.

Datenschutzbeauftragter

„Dabei zielt der Wortlaut nicht darauf ab, ob die zehn Personen in einem bezahlten Arbeitsverhältnis stehen, auch Ehrenamtliche zählen dazu. Maßgeblich ist zudem die Zahl der Köpfe, nicht die Zahl der Stellen. Sofern in einem Verein also zehn Übungsleitende oder Lehrkräfte die personenbezogenen Daten ihrer Trainierenden bzw. Schüler in einer Datei auf dem PC verarbeiten, ist ein Datenschutzbeauftragter zu bestellen.“ (Nds. LfDI)

Betroffenenrechte

- Auskunft, Art. 15 DSGVO
- Berichtigung, Art. 16 DSGVO
- Recht auf Vergessenwerden, Art. 17 DSGVO
  - Neue Umsetzung, basierend auf EuGH-Entscheidung
  - Ausführliche Regelung der rechtlichen Voraussetzungen
- Datenportabilität, Art. 20 DSGVO
- Widerspruch, Art. 21 DSGVO
- Verantwortliche Stelle muss über die Rechte informieren
- Klare Fristen zur Bearbeitung (maximal ein Monat)

Checkliste: Erste wichtige Punkte

- ✓Prozesse der Verarbeitung reflektieren (welche externen Dienste werden genutzt, was geschieht mit Mitarbeiterdaten, was mit Mitgliederdaten…)
- ✓ggfls. Verarbeitungsverzeichnis anlegen und führen
- ✓Information der Betroffenen (Website, Mitarbeiter, Mitglieder)
- ✓Datenschutzbeauftragter?
- ✓Verpflichtung der Mitarbeiter auf den Datenschutz
- ✓TOM
- ✓Meldung von Datenpannen umgehend (Verlust von Speichermedien usw.)

Sanktionen

BRANDI
RECHTSANWÄLTE

Sanktionen

- **Haftung und Risiken: Schadensersatzansprüche**
  - Eigenständiger Haftungsanspruch, Art. 82 DSGVO
  - Haftung bei einem Verstoß gegen die DSGVO
  - Verschulden ist nicht erforderlich, maximal Entlastungsmöglichkeit
  - Ersatzfähig ist jeder entstandene Schaden
    - Keine Haftungsbeschränkung vorgesehen/möglich
    - Ausdrücklich: materielle und immaterielle Schäden

- **Haftung und Risiken: Abmahnungen**
  - Datenschutzverstöße als Wettbewerbsrechtsverletzungen

Sanktionen

- **Haftung und Risiken: Geldbußen**
  - Geldbußen, Art. 83 DSGVO
  - Zuständigkeit der bisherigen Aufsichtsbehörden bleibt
  - Haftungsrahmen erhöht sich
    - Geldbußen sollen ausdrücklich „wirksam, verhältnismäßig und abschreckend“ sein
    - **Obergrenze jetzt 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes**
  - Möglichkeiten der Haftungsreduzierung
    - Unterstützung bei der Aufklärung / Aufarbeitung
    - Freiwillige Maßnahmen: Datenschutzbeauftragter, Zertifizierung, Auditierung

Handlungsbedarf

BRANDI
RECHTSANWÄLTE

Handlungsbedarf

- **Umstellung muss frühzeitig erfolgen!**
- **Keine Übergangsfrist!**

  - Umstellung setzt Bestandsaufnahme und Übersicht über Verarbeitungsvorgänge voraus
  - Anhand entsprechender Erkenntnisse kann Handlungsbedarf identifiziert werden
  - Hauptproblem ist vor allem Aktualisierung der Dokumentation
  - Häufig genügen kleinere Anpassungen der vertraglichen Vereinbarungen und Arbeitsabläufe

Handlungsbedarf

- **Wichtigste Sofortmaßnahme: Außenauftritt**
  - Anpassung Datenschutzerklärungen
    - Internetseite
    - Online-Plattformen
    - Apps
    - Einsatz von Social Media
  - Umgang mit Einwilligungen
    - Überprüfung von Alt-Einwilligungen

Handlungsbedarf

- **DSGVO auf der Website:**
  - Prozesse, Plug-Ins usw. ermitteln (Host fragen)
  - Rechtmäßigkeit hinterfragen (brauche ich alle Daten; ist das Plug-In DSGVO-konform?)
  - Informieren über one-click-Lösung auf der Website und jeder Unterseite; verständlich und vollständig
  - https://www.brandi.net/datenschutz/
  - https://www.brakel.de/

Hinweise zur Datenverarbeitung

Einleitung

Die BRANDI Rechtsanwälte Partnerschaft mbB, Rathenaustr. 96, 33102 Paderborn, paderborn@brandi.net (im Folgenden: „Wir“) ist die verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der Mandatsbearbeitung. Wir erfassen, speichern und nutzen Ihre personenbezogenen Daten nur in Übereinstimmung mit den anwendbaren datenschutzrechtlichen Bestimmungen, insbesondere der europäischen Datenschutz-Grundverordnung (DSGVO) und den nationalen Datenschutzbestimmungen.

Art und Umfang der Datenverarbeitung

Wenn Sie uns mandatieren, erheben wir folgende Informationen: Name und Kontaktdaten sowie Informationen, die für die Geltendmachung und Verteidigung Ihrer Rechte im Rahmen des Mandats notwendig sind.

Die Erhebung der Daten erfolgt, um Sie als unseren Mandanten identifizieren zu können, um Sie angemessen anwaltlich beraten und vertreten zu können, zur Korrespondenz mit Ihnen, zur Rechnungstellung.

Die Datenverarbeitung erfolgt auf Ihre Anfrage hin und ist zu den genannten Zwecken für die angemessene Bearbeitung des Mandats und für die beidseitige Erfüllung von Verpflichtungen aus dem Mandat erforderlich. Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten ist die Vertragsabwicklung im Sinne von Art. 6 Abs. 1 lit. b) DSGVO; außerdem kann eine Datenverarbeitung aufgrund unserer berechtigten Interessen im Sinne von Art. 6 Abs. 1 lit. f) DSGVO erfolgen. Soweit die Datenverarbeitung nicht schon zur Vertragsabwicklung erforderlich ist, erfolgt die Speicherung und Nutzung Ihrer Daten durch uns zur effektiven Erledigung unserer Aufgaben und Optimierung unserer Leistungen.

Die personenbezogenen Daten werden in jedem Fall bis zur Vertragsbeendigung und dem Ablauf aller Fristen zur Geltendmachung vertraglicher Ansprüche aufbewahrt. Danach erfolgt die Aufbewahrung unter Beachtung der bestehenden Aufbewahrungs- und Dokumentationsfristen, die sich sowohl aus den berufsrechtlichen Vorgaben für Rechtsanwälte als auch aus dem Handels- oder Steuerrecht ergeben können. Eine längere Speicherung kann außerdem erfolgen, wenn Sie hierin eingewilligt haben.

Eine Übermittlung Ihrer personenbezogenen Daten an Dritte zu anderen als den nachfolgend aufgeführten Zwecken findet nicht statt, insbesondere nicht zu Werbezwecken. Soweit zur Mandatsbearbeitung erforderlich, werden Ihre personenbezogenen Daten an Dritte weitergegeben, insbesondere an Verfahrensgegner und deren Vertreter sowie an Gerichte und andere öffentliche Behörden zum Zwecke der Korrespondenz sowie zur Geltendmachung und Verteidigung Ihrer Rechte. Das Anwaltsgeheimnis bleibt unberührt. Soweit es sich um Daten handelt, die dem Anwaltsgeheimnis unterliegen, erfolgt eine Weitergabe an Dritte nur in Absprache mit Ihnen.

Eine automatisierte Entscheidungsfindung auf Basis Ihrer personenbezogenen Daten und eine Weitergabe der personenbezogenen Daten in Drittstaaten außerhalb der Europäischen Union finden nicht statt.

Betroffenenrechte

Bezüglich der Verarbeitung Ihrer personenbezogenen Daten stehen Ihnen umfangreiche Rechte zu. Zunächst haben Sie ein umfangreiches Auskunftsrecht und können gegebenenfalls die Berichtigung und/oder Löschung bzw. Sperrung Ihrer personenbezogenen Daten verlangen. Sie können auch eine Einschränkung der Verarbeitung verlangen und haben ein Widerspruchsrecht. Im Hinblick auf die uns von Ihnen übermittelten personenbezogenen Daten steht Ihnen außerdem ein Recht auf Datenübertragbarkeit zu.

Eine einmal von Ihnen erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft frei widerrufen werden. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Sofern die Verarbeitung Ihrer personenbezogenen Daten nicht auf einer Einwilligung beruht, sondern aufgrund einer anderen Rechtsgrundlage erfolgt, können Sie dieser Datenverarbeitung widersprechen. Ihr Widerspruch führt zu einer Überprüfung und gegebenenfalls Beendigung der Datenverarbeitung. Sie werden über das Ergebnis der Überprüfung informiert und erhalten – soweit die Datenverarbeitung dennoch fortgesetzt werden soll – von uns nähere Informationen, warum die Datenverarbeitung zulässig ist.

Wir haben einen Datenschutzbeauftragten bestellt, der uns in datenschutzrechtlichen Themen unterstützt. Für Fragen bezogen auf unseren Umgang mit personenbezogenen Daten stehen Ihnen unser Datenschutzbeauftragter und sein Team unter datenschutz@brandi.net zur Verfügung. Wenn Sie der Auffassung sind, dass die Verarbeitung Ihrer personenbezogenen Daten durch uns nicht im Einklang mit den anwendbaren Datenschutzbestimmungen erfolgt, steht Ihnen ein Beschwerderecht bei einer Aufsichtsbehörde zu. Sie können sich auch bei unserem Datenschutzbeauftragten beschweren; der Datenschutzbeauftragte wird die Angelegenheit dann prüfen und Sie über das Ergebnis der Prüfung informieren.

Stand dieser Datenschutzhinweise: Juli 2018

BRANDI
RECHTSANWÄLTE

Risiko-Folgenabschätzung

Inhaltsverzeichnis

Ende der Vorabkontrolle

- Bisher: Pflicht zur Vorabkontrolle - §§ 4d, 4e BDSG
  - Grundsatz: Meldepflicht
  - Ausnahme: Betrieb hatte eigenen Datenschutzbeauftragten
    - Kontakt zur Aufsichtsbehörde bei Zweifel der Vereinbarkeit mit BDSG

- i.d.R. keine inhaltliche Prüfung durch Aufsichtsbehörde bei Vorabmeldung

- Abschaffung der Vorabkontrolle
  - Erheblicher bürokratischer Aufwand entstanden
  - Die Meldung allein führt zu keiner Sicherstellung der Freiheitsrechte

NEU: Risiko-Folgenabschätzung

- Datenschutz-Folgenabschätzung, Art. 35 DSGVO
  - Ausprägung des Grundsatzes: Privacy by Design

„*Hat eine Form der Verarbeitung* [...] *aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.* [...]“

- Ziel: Vereinbarkeit der Datenverarbeitung mit DSGVO
- Pflicht zur generellen Meldepflicht entfällt
- Zuständigkeit liegt beim „**Verantwortlichen**“
  - nicht beim Datenschutzbeauftragten

Erforderlichkeit der Vornahme

- Erforderlichkeit insb., wenn
  - Einsatz neuer Technologien
  - Profiling als Grundlage automatisierter Entscheidungen
  - Verarbeitung großer Datenmengen
  - Überwachung öffentlich zugänglicher Bereiche

- ABER: Ausnahme in Art. 35 Abs. 10 DSGVO
  - Verarbeitung auf Grundlage einer Rechtsvorschrift

- Überprüfung gem. Art. 35 Abs. 11 DSVGO
  - nach Implementierung - Einhaltung der Anforderungen? (**Check**)
  - bei Veränderungen - Anpassung der Verarbeitung! (**Act**).

(Mindest-) Inhalt der Folgenabschätzung 1/2

- Mindestinhalt in Art. 35 Abs. 7 DSGVO bestimmt
  - Systematische Beschreibung der geplanten Verarbeitung und ihrer Zwecke
  - Bewertung der Notwendigkeit und der Verhältnismäßigkeit
  - Bewertung der Risiken für Freiheitsrechte
  - Maßnahmen zur Bewältigung der Risiken

- Zusätzlich zu berücksichtigen: Allgemeine Grundsätze der Verarbeitung personenbezogener Daten
  - Risiko Folgenabschätzung ≙ Art. 5 Abs. 1 + Elemente der „Risikobewertung“ und „Sicherheitsmaßnahmen“:

(Mindest-) Inhalt der Folgenabschätzung 2/2

- **Checkliste** für die Praxis:
  - Prüfung Art. Artikel 5 Abs. 1 lit. a-f DSGVO
    - Rechtmäßigkeit der Verarbeitung; Verarbeitung nach Treu und Glauben; Transparenz; Zweckbindung; Datenminimierung; Richtigkeit; Speicherbegrenzung; Integrität und Vertraulichkeit
  - Prüfung Art. Artikel 35 Abs. 7 DSGVO:
    - Beschaffenheit der Datenverarbeitung; Beschreibung des Vorhabens; Dokumentation; berechtigten Interessen vorhanden?; Interessenabwägung; Verhältnismäßigkeit; Risikoanalyse; Risikobewertung
    - Können die identifizierten Risiken mit Garantien oder Sicherheitsvorkehrungen beherrscht werden?
      - Abhilfemaßnahmen; Sicherheitskonzept; Dokumentation dieser

(Weiterer) Inhalt der Folgenabschätzung 1/2

- Berücksichtigung von Verhaltenskodizes - Art. 35 Abs. 8 DSGVO
  - Wenn diese von Interessenverbänden ausgearbeitet und von Aufsichtsbehörde genehmigt wurden
- Ggf. Einholung des Standpunktes der Betroffenen - Art. 35 Abs. 9 DSGVO
  - Kein Betroffenenrecht
  - Gem. Art. 22 Abs. 3 DSGVO vor allem bei Profiling

Weiterer) Inhalt der Folgenabschätzung 2/2

- Checkliste für die Praxis
  - Prüfung, ob ein Branchen-Code of Conduct vorliegt.
  - Wurden die datenschutzrelevanten Geschäftsprozesse akkreditiert?
  - Beinhaltet Datenverarbeitung eine Bezugnahme auf die Bewertung persönlicher Aspekte (Profiling)?
  - Gibt es einen Code of Conduct, der den Standpunkt der betroffenen Personen bereits abgefragt hat?
  - Wenn kein Profiling: Kann das Einholen der Betroffenenstandpunkte eine risikominimierende Maßnahme darstellen?

Konsultationspflicht – Art. 36 DSGVO (1/2)

- Konsultationspflicht, wenn:
  - Ergebnis der Prüfung, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

- Prüfungsmaßstab der Aufsichtsbehörde:
  - Steht geplante Verarbeitung im Einklang mit der Verordnung?

- Wenn nein, Erteilung schriftlicher Empfehlungen
  - Innerhalb von 8 Wochen – Verlängerung um 6 Wochen möglich
  - **Bemerkenswert**: keine Mitteilungspflicht bei Konformität
    - Aber: Ausbleiben einer Mitteilung ist keine Konformitätsbestätigung

Konsultationspflicht – Art. 36 DSGVO (2/2)

- **Checkliste** für die Praxis:
  - Verarbeitung = hohes Risiko für die Rechte der Betroffenen?
  - Kann das Risiko eingedämmt werden?
  - Wenn nicht:
    - Wurde die Aufsichtsbehörde kontaktiert?
    - Wenn ja, wann wurde sie kontaktiert? Wurde die Kontaktaufnahme dokumentiert (ggf. Beweissicherung)?
    - Berechnung der Frist
    - Hat die Aufsichtsbehörde innerhalb der Frist reagiert? Liegt eine Fristverlängerung vor?
    - Falls keine Reaktion: Vergewissern, dass die Vorgaben der DSGVO eingehalten, insb., dass Folgenabschätzung ordnungsgemäß durchgeführt wurde; ggf. proaktive Kontaktaufnahme mit der Aufsichtsbehörde.

Aufgaben des Datenschutzbeauftragten

- Gem. Art. 35 Abs. 2 DSGVO ist der behördliche oder betriebliche Datenschutzbeauftragte zu beteiligen
  - Nicht seine Aufgabe, diese anzustoßen, durchzuführen oder ein Ergebnis zu beurteilen - Aufgabe des Verantwortlichen!
  - Gem. Art. 39 DSGVO Überwachungs- und Beratungsaufgabe
    - Assistenz des Verantwortlichen – beinhaltet eine aktive Teilnahme
  - Der Verantwortliche muss nicht zwingend dem Rat des Datenschutzbeauftragten folgen

- Aufgabe des Datenschutzbeauftragten
  - Insbes. Wann ist eine Folgenabschätzung durchzuführen und welche Methode ist bei der Durchführung anzuwenden?

Sanktionen

- Im Fall eines Verstoßes gegen Pflichten des Art. 35 DSGVO
  - Geldbußen von bis zu 10.000.000 EUR
  - oder von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs

- Öffnungsklausel in Art. 83 Abs. 7 DSGVO
  - Bußgelder gegenüber öffentlichen Stellen
  - Möglichkeit der Mitgliedsstaaten Vorschriften dafür festzulegen, ob Geldbußen gegen Behörden und öffentliche Stellen
  - Hiervon hat der Bundesgesetzgeber in § 43 BDSG Gebrauch gemacht – keine Geldbußen gegen Behörden und sonstige öffentliche Stellen

Vorteile und Kritik

- Selbständige Evaluierung der Prozesse, mit Blick auf die Betroffenenrechte
  - Schaffung eines gesteigerten Bewusstseins für Risiken der Verarbeitung
  - Weitere Verankerung des Datenschutzes in Unternehmen
- Frühwarnsystem – systematisches Nachdenken über neue Technik/Prozesse
- Förderung von Vertrauen
- Zumindest theoretisch erfolgt ein grundlegender Wandel für den Umgang mit personenbezogenen Daten

- Vorgaben bisher zu allgemein
- Privilegierung von staatlichen Institutionen durch die Ausnahmeregelung
- bislang kein allgemein akzeptierter Standard für Durchführung
- In D wohl eher Erhöhung des bürokratischen Aufwandes

Auftragsdatenverarbeitung

Inhalt

I. Die Auftragsverarbeitung
   1. Das Instrument
   2. Grundlagen nach der DSGVO
   3. Änderungen
   4. Mindestinhalt

II. (Auftrags-)Verarbeitung im Ausland

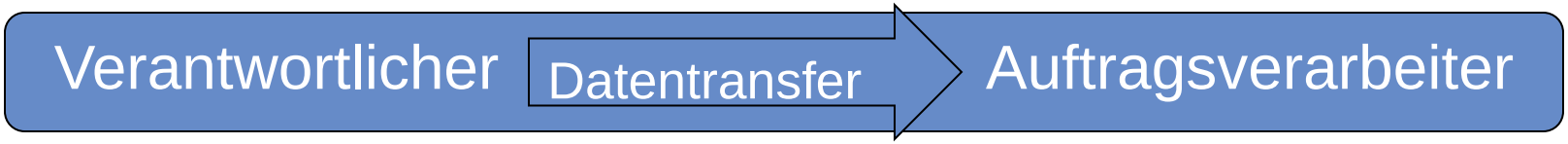
1. Das Instrument

Begriff: Auftragsdatenverarbeitung (§ 11 BDSG) heißt nach der DSVO **Auftragsdatenverarbeitung** (Art. 28 DSGVO)

Ausgangspunkt:

Datenübermittlung an einen Dritten

Datenverarbeitung im Auftrag



1. Das Instrument

Bei der Auftragsverarbeitung findet eine Übertragung von Daten an Dritte nicht statt bzw. ist diese privilegiert. Der Verantwortliche bleibt Herr der Daten.

Bisher:

Auftragsverarbeitung → Auftragnehmer nicht Dritter/ Keine Übermittlung von Daten = keine Rechtfertigung nötig (§ 3 Abs. 3, 8 BDSG)

DSGVO:

Auftragsverarbeitung → Auftragnehmer nicht Dritter/ **ABER:** Übermittlung von Daten = Rechtfertigung? Privilegierung? (Art. 28 DSGVO)

1. Das Instrument

Da die Auftragsverarbeitung nicht mehr ausdrücklich dem Begriff der Datenverarbeitung entzogen ist, wird diskutiert, ob Art. 28 DSGVO eine Privilegierungsfunktion hat oder nicht. In letztgenanntem Fall würden alle Anforderungen der DSGVO gelten (Rechtfertigung nach Art. 6, 9 DSGVO), in erstgenanntem nicht (vgl. zu dieser Debatte etwa Schmidt/Freund, ZD 2017, 14 ff.).

Nach richtiger Auffassung liegt der (erfolgreichen) Auftragsverarbeitung nach wie vor eine „interne“ Datenverarbeitung zugrunde, sodass es keiner gesonderten Rechtfertigung bedarf (Anforderungen des Art. 28 DSGVO und die Erwägungsgründe legen dieses Verständnis nahe).

1. Das Instrument

„(79)Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer ***klaren Zuteilung der Verantwortlichkeiten*** *durch diese Verordnung.“*

Um diese Privilegierung der Auftragsverarbeitung zu rechtfertigen, muss der Verantwortliche die Kontrolle und den maßgebenden Einfluss auf die Daten behalten. Sichergestellt wurde und wird dies durch einen umfangreichen Katalog von Anforderungen an die Ausgestaltung der Abreden zwischen Auftraggeber und Auftragnehmer.

Nach außen ist dann – jedenfalls bisher – allein der Verantwortliche Ansprechpartner der Aufsicht, der Betroffenen und sonstiger Dritter.

1. Das Instrument

Bisher: § 11 BDSG hält einen Katalog mit Anforderungen an die Auftrags(daten)verarbeitung bereit:

„Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen **sorgfältig auszuwählen**. Der Auftrag ist **schriftlich** zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1.der Gegenstand und die Dauer des Auftrags,

2.der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

3.die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

4.die Berichtigung, Löschung und Sperrung von Daten,

I. Die Auftragsverarbeitung

5.die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

6.die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

7.die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8.mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9.der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10.die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags“.

2. Grundlagen nach der DSGVO

Neu: Die Auftragsverarbeitung ist nun im Wesentlichen in Art. 28 DSGVO geregelt. Im Kern bliebt es bei den Anforderungen, die bisher an die Beauftragung gestellt wurden.

Erwägungsgrund 81

„Damit die Anforderungen dieser Verordnung […] eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. […]“

Erwägungsgrund 81 (Fortsetzung)

„Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen […]“

2. Grundlagen nach der DSGVO

In Art. 4 Nr. 8 DSGVO ist definiert, wer Auftragnehmer sein kann:

„Auftragsverarbeiter" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

Damit kann bspw. auch auf beiden Seiten des Auftrags eine öffentliche Stelle stehen. Die Übertragung von Daten etwa an einen Zweckverband zur Speicherung und Wartung von Daten kann danach über eine Auftragsverarbeitung gelöst werden (hier ist § 25 BDSG-neu regelmäßig wohl nicht hilfreich, weil die Vorgaben des § 23 BDSG-neu nicht erfüllt sein dürften)

3. Änderungen

a) Wartung technischer Systeme

Bisher § 11 Abs. 5 BDSG:

„Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.“

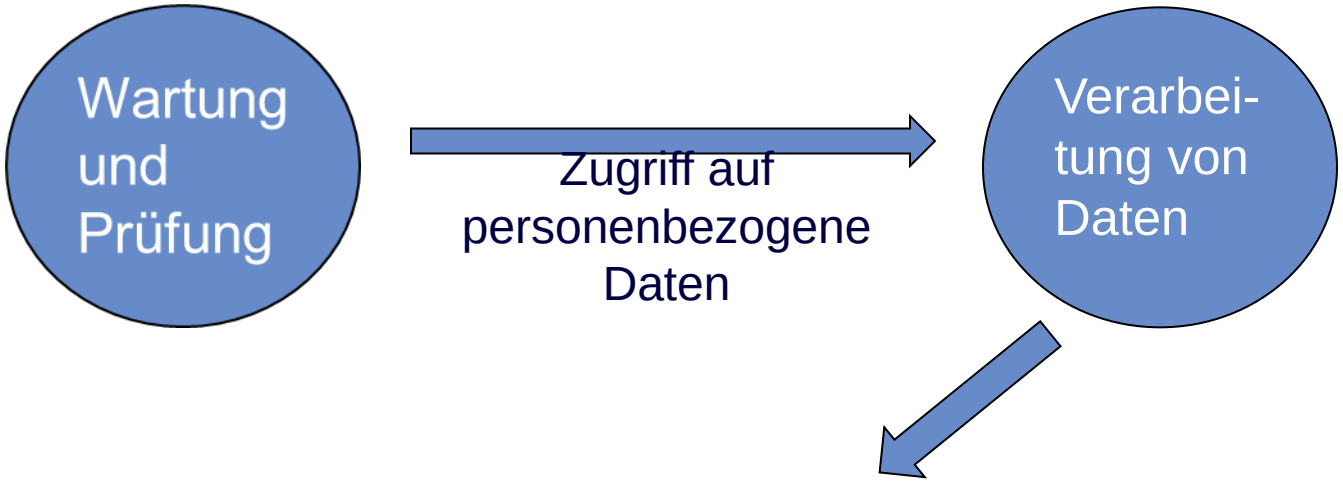
In der DSGVO fehlen Regeln zur Prüfung und Wartung technischer Systeme.
Folge?

- Kein datenschutzrechtlich relevanter Vorgang oder
- Nicht der Auftragsverarbeitung zugänglich oder
- Rechtfertigung über Art. 6, 9 DSGVO notwendig?

3. Änderungen

a) Wartung technischer Systeme

Wohl richtig dürfte sein:



Rechtfertigung, Art. 6, 9 DSGVO oder
Auftragsverarbeitung, Art. 28 DSGVO

3. Änderungen

b) Auswahl des Auftragnehmers

Der Auftraggeber muss sicherstellen, dass der Auftragnehmer zuverlässig seine Leistungen datenschutzkonform erbringt. Eine Zertifizierung o.Ä kann hier hilfreich sein (Art. 42 DSGVO).

Was für eine technische Umsetzung dieser Anforderungen zu verlangen ist, ist nicht abschließend verbindlich vorgegeben. Art. 32 DSGVO regelt Grundlagen wie Pseudonymisierung, Verschlüsselung usw.

Neu: technisch-organisatorische Maßnahmen für die Systemwiederherstellung (Art. 32 Ab. 1 lit. d) DSGVO)

3. Änderungen

b) Auswahl des Auftragnehmers

Abzuschließen ist eine Vereinbarung mit den – im Wesentlichen bekannten – Inhalten.

Neu: die Vereinbarung muss ausdrücklich nicht schriftlich, sie kann auch in elektronischer Form abgeschlossen werden (Art. 28 Abs. 9 DSGVO)

Die elektronische Form soll der Transparenz dienen. Ob sie auch die Echtheit des Dokuments belegen muss, ist strittig. Daher wird zum Teil eine elektronische Signatur verlangt, zum Teil die einfache elektronische Form für ausreichend gehalten.

3. Änderungen

c) (Neue) Pflichten und Obliegenheiten

Durch die Einschaltung eines Auftragverarbeiters bleibt der Verantwortliche grds. Adressat datenschutzrechtlicher Pflichten und Obliegenheiten und Ansprechpartner Dritter. Dennoch sind die Pflichten des Auftragnehmers nunmehr stärker als bisher unmittelbar in Art. 28 DSGVO normiert (Mitteilung von Datenschutzverstößen, Weisungsrecht des Auftraggebers usw.).

Weiterhin besteht nach Art. 28 Abs. 2 DSGVO die Pflicht des Auftragnehmers gesondert Einwilligungen einzuholen, wenn er einen Subunternehmer beauftragen will. Ist die Gestattung bereits in dem Auftrag erfolgt, besteht eine Informationspflicht mit Widerspruchsmöglichkeit.

3. Änderungen

c) (Neue) Pflichten und Obliegenheiten

In deutlich erweitertem Umfang als bislang folgt aus der direkten normativen Pflichtenstellung des Auftragnehmers seine Haftung gegenüber Betroffenen nach Art. 82 Abs. 2 DSGVO:

„Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. 2Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat“

3. Änderungen

c) (Neue) Pflichten und Obliegenheiten

Der Exzess des Auftragnehmers führt ebenso zu seiner eigenen Haftung. Er gilt dann als nach außen Verantwortlicher. Art. 28 Abs. 10 DSGVO lautet:

„Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.“

4. Mindestinhalt

„Nach Art. 28 Abs. 3 S. 2 DSGVO ergeben sich 8 Regelungsmaterien als Mindestinhalt:

- Pflicht des Auftragnehmers zur Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung in ein Drittland oder eine internationale Organisation (Art. 28 Abs. 3 S. 2 lit. a DSGVO)
- Verpflichtung der zur Verarbeitung der personenbezogenen Daten befugten Personen auf die Vertraulichkeit, sofern keine angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; (Art. 28 Abs. 3 S. 2 lit. b DSGVO)
- Maßnahmen der Sicherheit der Verarbeitung iSv Art. 32 DSGVO (Art. 28 Abs. 3 S. 2 lit. c DSGVO)
- Die in Art. 28 Abs. 4 DSGVO genannten Vorgaben für die Beauftragung von Subunternehmern („weitere Auftragsverarbeiter“) durch den Auftragnehmer („Auftragsverarbeiter“) (Art. 28 Abs. 3 S. 2 lit. d DSGVO)

4. Mindestinhalt

- „Verpflichtung des Auftragnehmers den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von der Rechte der Betroffenen nach Artt. 12 ff. ff. DS-GVO zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO)
- Verpflichtung des Auftragnehmers den Auftraggeber bei der Einhaltung der in den Artt. 32 DSGVO (Sicherheit der Verarbeitung), 33/34 DSGVO (Meldung von Verletzungen des Schutzes personenbezogener Daten), 35 DSGVO (Datenschutz-Folgenabschätzung) und 36 DSGVO (vorherige Konsultation) zu unterstützen (Art. 28 Abs. 3 S. 2 lit. f DSGVO)
- Löschung oder Rückgabe der personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen (Art 28 Abs. 3 S. 2 lit. g DSGVO)
- Dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen (Art. 28 Abs. 3 S. 2 lit. h DS-GVO)“ (Eckhardt, CCZ 2017, 111,115)

II. (Auftrags-)verarbeitung im Ausland

Die bisherige Privilegierung der Datenverarbeitung im Ausland über § 3 Abs. 8 S. 3 BDSG auf EU-Staaten ist weggefallen. Nunmehr ist eine zweistufige Prüfung durchzuführen:

1. •Rechtfertigung oder Privilegierung der Datenübermittlung (Art. 6, 9, 28 DSGVO)
2. •Zulässigkeit der Übertragung ins Ausland (Art. 44 ff. DSGVO)

II. (Auftrags-)verarbeitung im Ausland

Art. 44 DSGVO

[1]Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, 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; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. [2]Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Art. 45 DSGVO: Erlaubnis wegen eines Angemessenheitsbeschlusses

[1]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. [2]Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

Art. 46 DSGVO: Erlaubnis wegen eines besonderer Garantien

Ohne Angemessenheitsbeschluss müssen besondere Garantien für einen datenschutzkonformen Umgang mit den Daten bestehen. Diese können sein:

- rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen,
- verbindliche interne Datenschutzvorschriften,
- Standarddatenschutzklauseln,
- von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln,
- genehmigte Verhaltensregeln zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland
- ein genehmigtes Zertifizierungsmechanismus

Art. 49 DSGVO: weitere Ausnahmen

- die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt,
- die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,
- die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,
- die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,
- die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,
- die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich,
- die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist.

Data Breach Notification

Data Breach Notification

- Risiken
- Adressaten
- Entstehung
- Inhalt
- Fristen
- Dokumentationspflicht
- Folgen

Was ist ein Data Breach?

- Hackerangriff
- Diebstahl/Verlust Smartphone
- Versehentliches Onlinestellen von Daten
- Versenden von Daten an eine falsche Adresse
- Vernichten von Daten
- Missbrauch personenbezogener Daten durch Mitarbeiter

Folgen

- Rufschädigung
- Erpressung
- Identitätsdiebstahl
- Spam
- Zugang zu weiteren Konten
- finanzielle Risiken

Adressaten

Auftragsverarbeiter

Art. 33 Abs. 2 DSGVO

Verantwortlicher

Aufsichtsbehörde

Art. 33 Abs. 1 DSGVO

Betroffene Person

Art. 34 Abs. 1 DSGVO

Adressaten – Sonderfall:
Gemeinsam für die Verarbeitung Verantwortliche

Verantwortlicher 1

Verantwortlicher 2

Art. 26 Abs. 1 S. 2 DSGVO

Aufsichtsbehörde

Art. 33 Abs. 1 DSGVO

Betroffene Person

Art. 34 Abs. 1 DSGVO

Erfasste Daten

Alle Arten personenbezogener Daten

Entstehen der Pflichten

Verletzung des Schutzes personenbezogener Daten

+

Risiko für die Rechte und Freiheiten natürlicher Personen

Entstehen der Pflichten

Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO)

Verletzung der Sicherheit, die

ob unbeabsichtigt oder unrechtmäßig, zur **Vernichtung**, zum **Verlust**, zur **Veränderung** oder

zur unbefugten **Offenlegung** von bzw. zum unbefugten **Zugang** zu

personenbezogenen Daten führt, die **übermittelt**, **gespeichert** oder auf **sonstige Weise verarbeitet** wurden

Entstehen der Pflichten

Risiko für die Rechte und Freiheiten natürlicher Personen

- **Aufsichtsbehörde**

Grundsatz: Meldung

Ausnahme: Voraussichtlich kein Risiko (Beweislast beim Verantwortlichen)

- **Betroffene Person**

Grundsatz: Keine Benachrichtigung

Ausnahme: Voraussichtlich hohes Risiko und keine Ausnahme nach Art. 34 Abs. 3 a) oder b) DSGVO

Inhalt

Meldung an die Aufsichtsbehörde (Art. 33 Abs. 3 DSGVO)	Benachrichtigung an den Betroffenen (Art. 34 Abs. 2 DSGVO)
▪ Beschreibung der Art der Verletzung, soweit möglich mit Angabe – Angabe der Kategorien – ungefähre Zahl der betroffenen Personen, Kategorien, Datensätze	▪ Beschreibung der Art der Verletzung in **klarer und einfacher Sprache**
▪ Name und Kontaktdaten des Datenschutzbeauftragen oder sonstigen Anlaufstelle	▪ Name und Kontaktdaten des Datenschutzbeauftragen oder sonstigen Anlaufstelle
▪ Beschreibung der wahrscheinlichen Folgen	▪ Beschreibung der wahrscheinlichen Folgen
▪ Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen	▪ Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen

Fristen

„Unverzüglich“

- an **Aufsichtsbehörde**
  - spätestens 72 Stunden nach Bekanntwerden
  - falls später, Begründung erforderlich
- an **betroffene Person** und **Auftragsverarbeiter** an Verantwortlichen

Dokumentationspflicht

Art. 33 Abs. 5 S. 1 DSGVO

„Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.“

Folgen

- **Bußgelder** (Art. 83 Abs. 4 a) DSGVO)

  bis zu 10.000.000 € oder

  im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres

- **Schadensersatz** (Art. 82 DSGVO)

Fazit

- Alle Arten personenbezogener Daten werden erfasst
- Auftragsverarbeiter trifft eigene Verantwortlichkeit
- Schwelle zur Meldung an die Aufsichtsbehörde abgesenkt
- Meldefrist beachten
- Dokumentationspflichten

- **Abläufe optimieren!**

Verhältnis KUG zur DSGVO

Problemaufriss

- Zu den personenbezogenen Daten zählen auch Bildnisse im Sinne des KUG, sodass die DSGVO anwendbar ist
  - Somit : Anwendungsvorrang der DSGVO
  - jederzeitiger Widerruf einer Einwilligung in die Anfertigung und Veröffentlichung ohne Angabe von Gründen möglich
  - Nach KUG Widerruf nur unter erschwerten Voraussetzungen und nur für die Veröffentlichung

- Die Bundesregierung steht auf dem Standpunkt, dass das KUG für Bildveröffentlichungen auch weiterhin anwendbar ist
  - Problem: ob und inwieweit die DSGVO die Vorschriften des KUG im Bereich der Veröffentlichung von Bildnissen verdrängt.

Problemaufriss

- Vor Inkrafttreten der DSGVO: **Subsidiaritätsklausel** des § 1 BDSG
  - DSGVO beinhaltet keine solche Klausel
- Umstritten, ob KUG noch anwendbar
  - Im Rahmen von Artikel 85 DSGVO kann das KUG im journalistischen, wissenschaftlichen und künstlerischen Kontext aufrechterhalten werden
  - **Streitig**, ob Öffnungsklausel auch eine Regelungsbefugnis für die Nutzung von Bildnissen beispielsweise im Rahmen der Werbung oder privater Meinungsäußerungen einräumt
  - Unklar, ob Artikel 85 DSGVO Regelungsbefugnis für Datenverarbeitungen zu anderen Zwecken einräumt (Bsp. für Öffentlichkeitsarbeit von Vereinen)
- Rechtsunsicherheit

Stellungnahme BMI

- „*Die Datenschutz-Grundverordnung führt zu keinen wesentlichen Veränderungen der bisherigen Rechtslage im Umgang mit Fotografien.* […] *Wie bisher auch dürfen Fotos nur verarbeitet werden, wenn die betroffene Person eingewilligt hat oder eine Rechtsgrundlage dies erlaubt.* […] “
- „*Für die Veröffentlichung von Fotografien enthält das Kunsturhebergesetz (KunstUrhG) ergänzende Regelungen, die auch unter der ab dem 25. Mai 2018 anwendbaren Datenschutz-Grundverordnung fortbestehen. Das Kunsturhebergesetz stützt sich auf Artikel 85 Absatz 1 der Datenschutz-Grundverordnung, der den Mitgliedstaaten nationale Gestaltungsspielräume bei dem Ausgleich zwischen Datenschutz und der Meinungs- und Informationsfreiheit eröffnet. Es steht nicht im Widerspruch zur Datenschutz-Grundverordnung, sondern fügt sich als Teil der deutschen Anpassungsgesetzgebung in das System der Datenschutz-Grundverordnung ein.* “

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?

Dr. Christoph Worms

T +49 5251 7735 - 0
F +49 5251 7735 - 99
E christoph.worms@brandi.net

www.brandi.net

BRANDI
RECHTSANWÄLTE