Auftragsdatenverarbeitung unter der DSGVO

5.5.2017

Axel Anderl, Felix Hörlsberger, Nino Tlapak

DORDA

WIR SCHAFFEN KLARHEIT.

Agenda

- Grundbegriffe / Rollenverteilung nach Art 28 DSGVO
- Rechtsvergleich DSG / DSGVO
  - Auswahl des Auftragsverarbeiters
  - Grundlage der Beauftragung
  - Inhalt der Beauftragung
- Hinzuziehung von Subunternehmern
  - Grenzüberschreitender Datenverkehr
- Erweiterte Pflichten / Haftung
- Praktischer Handlungsbedarf

Grundbegriffe / Rollenverteilung nach Art 28 DSGVO

- Verarbeitung personenbezogener Daten einer natürlichen Person
- durch Auftragsverarbeiter
- im Auftrag und nach Weisung des Verantwortlichen

- schriftlicher Vertrag in dem
  - Gegenstand und Dauer der Verarbeitung
  - Art und Zweck der Verarbeitung
  - die Art der personenbezogenen Daten
  - die Kategorien betroffener Personen und
  - die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Rechtsvergleich – Auswahl des Auftragsverarbeiters

Vorgaben bei der Auswahl durch den Verantwortlichen

- § 10 DSG
  - ausreichende Gewähr für rechtmäßige und sichere Datenverwendung

- Art 28 DSGVO
  - hinreichende Garantie durch den Auftragsverarbeiter zur Durchführung geeigneter technischer und organisatorischer Maßnahmen,
    - dass Verarbeitung im Einklang mit Anforderungen der DSGVO
    - und Schutz der Betroffenenrechte gewährleistet ist

Rechtsvergleich – Auswahl des Auftragsverarbeiters

Prüfung durch den Verantwortlichen in der Praxis

- Auswahl zertifizierter Auftragsverarbeiter

- "Faktor" für Nachweis geeigneter Garantien (Art 28 Abs 5)
  - Einhaltung genehmigter Verhaltensregeln nach Art 40
  - Einhaltung genehmigtes Zertifizierungsverfahren nach Art 42

- Zusätzlicher Nutzen eines derartigen Nachweises
  - Nachweis Einhaltung Verantwortung (Art 24 Abs 3)
  - Nachweis Privacy by design / by default (Art 25 Abs 3)
  - Nachweis Einhaltung Sicherheitsmaßnahmen (Art 32 Abs 3)
  - Ermöglichung Datenübermittlung in Drittländer (Art 46 Abs 2)
  - Milderung der Strafen (Art 83 Abs 2)

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Rechtsvergleich – Auswahl des Auftragsverarbeiters

Exkurs: Erbringung des Nachweises

- Genehmigte Verhaltensregeln (Art 40)
  - Entwurf durch Verbände, Unternehmen
  - Genehmigung/Veröffentlichung durch zuständige Aufsichtsbehörde (ev unter Mitwirkung anderer Mitgliedstaaten)
  - Kommission kann allgemeine Gültigkeit erklären

- Genehmigtes Zertifizierungsverfahren (Art 42)
  - Zertifizierungsverfahren, Datenschutzsiegel und –prüfzeichen
  - Erteilung durch akkreditierte Zertifizierungsstellen
  - Veröffentlichung der Verfahren durch Ausschuss
  - Freiwillige Unterwerfung/Verleihung für 3 Jahre (Verlängerung möglich)

Rechtsvergleich – Grundlage der Beauftragung

Bindung des Auftragsverarbeiters

- Regelung im DSG (§§ 10 und 11)
  - die hierfür notwendigen Vereinbarungen treffen
  - Empfehlung Schriftlichkeit zur Beweissicherung, sofern über § 11 hinausgehende Pflichten überbunden werden sollen

- Neues Regime der DSGVO (Art 28)
  - schriftlicher Vertrag oder vergleichbares Rechtsinstrument,
  - der/das Auftragnehmer bindet.

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Rechtsvergleich – Inhalt der Beauftragung

Regelungsinhalt nach DSG

- keine inhaltlichen Vorgaben
  - Bestehendes Muster der Datenschutzbehörde

- Pflichten des Dienstleisters in § 11 DSG festgelegt
  - Geltung unabhängig von vertraglicher Vereinbarung
  - Muster der Datenschutzbehörde geht kaum darüber hinaus
    - ua Data Breach Notification nicht abgedeckt
  - Zusätzliche Regelungen in der Praxis erforderlich und sinnvoll

Rechtsvergleich – Inhalt der Beauftragung

Regelungsinhalt nach DSGVO

- Mindestinhalt für schriftlichen Vertrag (Art 28 Abs 3)
  - Verarbeitung nur auf dokumentierte Weisung
  - Verpflichtung Mitarbeiter zur Vertraulichkeit und Verschwiegenheit
  - Einhaltung Datensicherheitsmaßnahmen nach Art 32
  - Einhaltung Zustimmungserfordernis/Widerspruchsrecht bei Subs
  - Unterstützung bei Wahrung der Betroffenenrechte
  - Unterstützung bei Datensicherheit und PIA
  - Löschung/Rückgabe nach Beendigung
  - Zurverfügungstellung aller erforderlichen Informationen
  - Ermöglichung von Überprüfungen/Inspektionen

Hinzuziehung von Subverarbeitern

Auftragsverarbeiter kann weitere Subverarbeiter hinzuziehen

- Verantwortlicher muss schriftlich zustimmen (Art 28 Abs 2)
  - vorherige gesonderte Genehmigung eines konkreten Sub; oder
  - allgemeine schriftliche Genehmigung mit
    - Vorab-Informationspflicht des Auftragsverarbeiters, sodass
    - Verantwortlicher gegen Sub Einspruch erheben kann

- Überbindung aller Pflichten an Sub (Art 28 Abs 4 DSGVO)
  - in schriftlichem Vertrag
  - Auftragsverarbeiter haftet gegenüber Verantwortlichen, sofern Sub seinen Datenschutzpflichten nicht nachkommt

Hinzuziehung von Subverarbeitern

Grenzüberschreitender Datenverkehr

- Auftragsverarbeiter und/oder Sub mit Niederlassung in einem Drittland

- Datentransfer auf Basis Angemessenheitsbeschluss
  - Genehmigungsfrei sofern Kommissionsbeschluss vorliegt
  - Kommission muss Entscheidungen alle vier Jahre überprüfen
  - vgl EU-US Privacy Shield

- ohne Angemessenheitsbeschluss nur wenn
  - geeignete Garantien ergriffen und
  - Gewährung durchsetzbare Rechte / wirksame Rechtsbehelfe für Betroffenen

Hinzuziehung von Subverarbeitern

Grenzüberschreitender Datenverkehr

- Datentransfer vorbehaltlich geeigneter Garantien
  - genehmigungsfrei, wenn
    - bindendes/durchsetzbares Dokument zwischen Behörden
    - verbindliche interne Datenschutzvorschriften nach Art 47
    - Standarddatenschutzklauseln
    - genehmigte Verhaltensregeln iZm rechtsverbindlichen/durchsetzbaren Verpflichtungen
    - genehmigte Zertifizierung iZm rechtsverbindlichen/durchsetzbaren Verpflichtungen
  - genehmigungspflichtig, wenn
    - Vertragsklauseln zwischen Verantwortlichen und Empfänger
    - Bestimmungen in Verwaltungsvereinbarungen zwischen Behörden

Hinzuziehung von Subverarbeitern

Grenzüberschreitender Datenverkehr

- Fazit: Steigende Bedeutung von BCR / EU SCC
  - keine separate Genehmigung mehr in Österreich
- umfangreicher Katalog verpflichtender Angaben:
  - Anwendung allgemeiner Datenschutzgrundsätze
  - Rechte der Betroffenen und deren Wahrnehmung
  - Haftung für etwaige Verstöße
  - Aufgaben und Tätigkeit des Datenschutzbeauftragten
  - Verfahren zur regelmäßigen Überprüfung
  - Verfahren für Änderungen und Meldung an Aufsichtsbehörde
  - Verfahrung zur Meldung von nachteiligen Bestimmungen in Drittländern
  - geeignete Datenschutzschulungen
  - ...

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Hinzuziehung von Subverarbeitern

Grenzüberschreitender Datenverkehr

- weiterhin keine Genehmigung notwendig, wenn
  - Einwilligung der Betroffenen
  - Übermittlung für Vertragserfüllung erforderlich
  - wichtige Gründe des öffentlichen Interesses
  - Geltendmachung, Ausübung, Verteidigung von Rechtsansprüchen
  - Schutz lebenswichtiger Interessen
  - Daten aus öffentlichen Registern
  - sonst nur wenn
    - keine wiederholte Übermittlung
    - nur begrenzte Zahl Betroffener
    - Wahrung zwingender überwiegend berechtigter Interessen
    - alle Umstände beurteilt und angemessene Garantien getroffen
    - Information an Aufsichtsbehörde

Erweiterte Pflichten / Haftung

Zusätzliche Pflichten für Auftragsverarbeiter

- gesonderte Dokumentationspflicht (Art 30 Abs 2)
  - Name und Kontaktdaten des Auftragsdatenverarbeiters und aller Verantwortlichen
  - Kategorien der Verarbeitungen je Verantwortlichen
  - Beschreibung der geeigneten Garantien bei Übermittlungen in Drittländer
  - allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
- Verzeichnis ist
  - schriftlich / elektronisch zu führen
  - auf Anfrage der Aufsichtsbehörde zur Verfügung stellen

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Erweiterte Pflichten / Haftung

Zusätzliche Pflichten für Auftragsverarbeiter

- Unterstützung des Verantwortlichen bei der Einhaltung von Auflagen (ErwG 95)
  - Datenschutz-Folgenabschätzung und
  - zur Konsultation
- Unverzügliche Meldung etwaiger Verletzungen an den Verantwortlichen (Art 33 Abs 2)
- Benennung Datenschutzbeauftragter (Art 35)

Erweiterte Pflichten / Haftung

Haftung des Auftragsverarbeiters

- Auftragsverarbeiter haftet dem Betroffenen für verursachten Schaden (Art 82 Abs 2)
  - wenn speziell auferlegten Pflichten nicht nachgekommen oder
  - Nichtbeachtung/Zuwiderhandlung rechtmäßig erteilter Anweisungen des Verantwortlichen
- Solidarische Haftung mit Verantwortlichem (Art 82 Abs 4)
  - Regressanspruch (Art 82 Abs 5)
- Potentielle Geldstrafen nach Art 83

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Erweiterte Pflichten / Haftung

Haftung des Verantwortlichen für den Auftragsverarbeiter

- Verantwortlicher haftet dem Betroffenen für verursachten Schaden (Art 82 Abs 2)
  - auch wenn Schaden durch Auftragsverarbeiter verursacht!
  - Regressanspruch (Art 82 Abs 5)
- Potentielle Geldstrafen nach Art 83
  - Verletzung von Prüfung- und Weisungspflichten
  - nicht sorgfältige Auswahl / nicht ausreichende Überwachung des Auftragsverarbeiters (Auswahl-/Überwachungsverschulden)
- Praktisch meist wahrscheinlicher, dass Verantwortlicher direkt in Anspruch genommen

Praktischer Handlungsbedarf

Prüfpflicht

- Strengere Prüfung bei der Auswahl der Auftragsverarbeiter
  - Sicherstellung Compliance mit strengeren Kriterien DSGVO
  - Sicherstellung geeigneter Garantien
- Laufende Kontrolle der Auftragsverarbeiter
  - Umfang und Ausmaß der Kontrolle insb abhängig von den verarbeiteten Datenkategorien und den Risiken für die Betroffenen

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Praktischer Handlungsbedarf

Berücksichtigung bei Vertragsgestaltung

- Überarbeitung bestehender Verträge
  - Dienstleistervereinbarung → Auftragsverarbeitungsvertrag
  - Überbindung neuer Verpflichtungen zur umfangreichen Unterstützung (etwa bei Folgenabschätzung)
- Berücksichtigung bei Erstellung neuer Verträge
  - Neue Verträge bis Mai 2018 doppelgleisig (DSG und DSGVO) ausgestalten
  - Vermeidung von Lücken oder Nachverhandlungsbedarf

Praktischer Handlungsbedarf

Hinzuziehen zur Erfüllung sonstiger Pflichten

- Berücksichtigung von Auftragsverarbeitern bei Erstellung der Dokumentation (Verzeichnis von Verarbeitungsvorgängen nach Art30 DSGVO)

- Rechtzeitige Einbindung der Auftragsverarbeiter bei Datenschutz-Folgenabschätzung
  - unverzichtbarer, meist technischer Input
  - erforderlich für belastbare Risikoanalyse

Ansprechpartner

Dr Axel Anderl, LL.M.

- Partner bei DORDA
- Absolvent der Universität Wien (Dr iur 2005) und des Universitätslehrgangs für Informationsrecht und Rechtsinformation der Universität Wien (LL.M. 2001)
- Fachliche Schwerpunkte: IT-Recht, insb E-Commerce, Datenschutzrecht, Urheber-, Medien- und Wettbewerbsrecht
- ILO Clients Choice Award für E-Commerce 2012 und 2013
- ILO Clients Choice Award für Information Technology 2014, 2015, 2016 und 2017
- Empfohlen als führender Anwalt in IT-Recht im renommierten internationalen Handbuch “Chambers Europe”, "Legal 500“ und "International Law Office"
- Autor zahlreicher Fachpublikationen in den Bereichen IT-, Urheber- und Medienrecht
- Mitglied des Österreichischen Juristenverbandes und der Interessensgemeinschaft „www.it-law.at“

Ansprechpartner

MMag Dr Felix Hörlsberger

- Partner bei DORDA
- Universität Wien (Dr iur 2003; Ranking Top 1%) und der Wirtschaftsuniversität Wien (Mag rer soc oec 2003)
- Fachliche Schwerpunkte: Restrukturierungen, Versicherungsrecht, Datenschutzrecht, Zivilprozessrecht, Compliance
- Empfohlen von den renommierten internationalen Handbüchern „Chambers Global“ und „Legal 500“ für seine Expertise in Restrukturierungen und für seine Expertise in Dispute Resolution
- Autor zahlreicher Fachpublikationen in den Bereichen Versicherungsrecht, Datenschutz, Gesellschafts- und Bankrecht
- Regelmäßig Vortragender bei Fachseminaren
- Mitglied der IBA (Insurance, Litigation)
- Gründungsmitglied und Vizepräsident der YACLA (Young Austrian Commercial Litigation Association)

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Ansprechpartner

Mag Nino Tlapak, LL.M.

- Rechtsanwaltsanwärter bei DORDA
- Universität Wien, Mag iur 2012
- Universität Wien, Universitätslehrgang Medien- und Informationsrecht, LL.M. (IT-Law) 2013
- Fachliche Schwerpunkte: Datenschutzrecht, IT-Recht, E-Commerce, Outsourcing, Urheber- und Medienrecht
- Autor von Fachpublikationen im Bereich Datenschutz und E-Commerce
- Vortragender für "E-Commerce Recht" bei der Werbe Akademie
- Vortragender innerhalb des "Social Media" Lehrgangs an der Werbeakademie
- Mitglied der Interessensgemeinschaft "www.it-law.at"
- Mitglied der Interessensgemeinschaft "Privacyofficers.at"

Kontakt

Dr Axel Anderl, LLM
T: +43 1 533 47 95 – 23
E: axel.anderl@dorda.at

MMag Dr Felix Hörlsberger
T: +43 1 533 47 95 – 17
E: felix.hoerlsberger@dorda.at

Mag Nino Tlapak, LLM
T: +43 1 533 47 95 – 23
E: nino.tlapak@dorda.at

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien