LexisNexis®

Datenschutzrechtliche Fragen in der COVID-Krise

Vom Umgang mit sensiblen Erkrankungsdaten bis zu datenschutzrechtlichen Themen im Home Office

2.4.2020

Axel Anderl, Nino Tlapak

DORDA

WIR SCHAFFEN KLARHEIT.

Ansprechpartner

Dr Axel Anderl, LL.M.

- Managing Partner bei DORDA
- Leiter der IT/IP und Datenschutz sowie der Digital Industries Group
- Absolvent der Universität Wien (Dr iur 2005) und des Universitätslehrgangs für Informationsrecht und Rechtsinformation der Universität Wien(IT-Law) (LL.M. 2001)
- Fachliche Schwerpunkte: IT-Recht, insb E-Commerce, Outsourcing, IT-Projektverträge, Datenschutzrecht, Urheberrecht
- ILO Clients Choice Award für E-Commerce 2012 und 2013
- ILO Clients Choice Award für Information Technology 2014, 2015, 2016, 2017, 2018 und 2019
- Seit Jahren als führender Anwalt in IT-Recht in "Chambers Europe" und "Legal 500"empfohlen
- Legal500 Hall of Fame TMT
- Autor zahlreicher Fachpublikationen in den Bereichen IT-, IP-Urheber- und Wettbewerbsrecht
- Vortragender an diversen Hochschulen und Fachhochschulen
- Co-Chair Technology Sourcing Committee von ITechLaw

Ansprechpartner

Mag Nino Tlapak, LL.M.

- Rechtsanwalt 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
- Next Generation Lawyer im Bereich TMT "Legal 500" (2018, 2019); Up and Coming im Bereich TMT "Chambers" (2020)
- Autor von Fachpublikationen im Bereich Datenschutz und E-Commerce
- Vortragender für Datenschutzrecht bei den Master-Lehrgängen "Digital Business" an der FH Technikum Wien sowie "Technisches Management" an der FH Campus Wien, Donau Universität Krems ("Datenschutz und Privacy")
- Mitglied der Interessensgemeinschaften "www.it-law.at" und "Privacyofficers.at"

Agenda

I. Rechtsgrundlagen zur Verarbeitung von COVID-19 Daten

II. Weitergabe von sensiblen Daten – intern und extern

III. Etablierung von angemessenen Sicherheitsmaßnahmen

IV. Weitere datenschutzrechtliche Dos and Don'ts

V. Exkurs: Home Office und Datenschutz/-sicherheit

Verarbeitung von Daten über eine (potentielle) Infektion
Rechtsgrundlagen

Datenschutzrechtliche Grundlagen

Verarbeitung von Daten über (potentielle) Infizierungen

- Information über Verdachtsfall ist bereits Gesundheitsdatum (besondere Kategorie personenbezogener Daten)

- Bestätigung der Infizierung selbstverständlich ebenfalls

- Rechtsgrundlage daher anhand Art 9 DSGVO zu beurteilen
  - konkrete gesetzliche Grundlage für Datenverarbeitung?
  - ausdrückliche Einwilligung des Betroffenen?
  - Einhaltung arbeits- und sozialrechtlicher Pflichten
    - Fürsorgepflicht des Arbeitgebers – Schutz der restlichen Arbeitnehmer
  - in Ausnahmefällen: Notwendigkeit zum Schutz lebenswichtiger Interessen der Betroffenen oder anderer Personen (Einzelfallprüfung)

Datenschutzrechtliche Grundlagen

Zulässigkeit von Einlasskontrollen mit Fiebermessungen

- Fiebermessungen am Eingang / Zugangskontrolle
  - Werden Daten dokumentiert? Oder nur "live"?
  - Ist der Bereich uU videoüberwacht?

- bloße Momentaufnahmen ohne Speicherung → außerhalb DSGVO
  - DSGVO gilt für "*ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte, strukturierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen*"

- Rechtsgrundlage bei Anwendbarkeit der DSGVO (Ausreißerfall)
  - Einhaltung arbeits- und sozialrechtlicher Pflichten
    - Informationspflicht beachten (Art 13/14 – Datenschutzhinweise)

Datenschutzrechtliche Grundlagen

Exkurs: Stopp-Corona-App – ein Datenschutzproblem?

- Kontakt Tagebuch vom Österreichischen Roten Kreuz
  - digitaler Handshake mit Personen möglich, zu denen Kontakt besteht
  - Bestätigung durch beide Teilnehmer erforderlich
- Datenminimierung sichergestellt
  - Pseudonymisierung durch ID
  - bei Infizierung zusätzlich Telefonnummer und Zeitpunkt der Meldung
    - mit Einwilligung
  - Statistische Auswertungen über Anzahl der Infizierungen und Downloads
    - anonymisiert
- pseudonymisierte Warnung an Kontakte
  - Kontakte erhalten nur die Information, dass sie Kontakt mit einem Infizierten hatten
- Update mit automatisierter Kontakterfassung angekündigt
  - kann uE ebenfalls nur auf Einwilligung gestützt werden

Verarbeitung von Daten über eine (potentielle) Infektion
Weitergabe / Übermittlung

Datenübermittlung in Zusammenhang mit COVID-19

Interne Übermittlung von Daten über (potentielle) Infektionen

- interne Weitergabe im Unternehmen
  - an andere Abteilungen wie zB HR oder einzelne AN
  - strenges need-to-know Prinzip beachten!

- Grundsatz der Datenminimierung in der Krise
  - Praxisfrage: Wer muss wann was wissen?

- Praktische Handlungsempfehlungen
  - Information über Verdachtsfälle/Erkrankungen grundsätzlich anonym
    - zB nur über betroffenes Stockwerk, Abteilung oder Standort
  - namentliche Offenlegung nur wo notwendig
    - zB rückmeldende AN mit Kontakt zu Stockwerk, Abteilung oder Standort

Datenübermittlung in Zusammenhang mit COVID-19

Externe Übermittlung von Daten über (potentielle) Infektionen

- streng(st)e Datenminimierung
  - Rechtsgrundlage der Fürsorgepflicht greift nicht bei Dritten
  - Weitergabe an Dritte (Kunden, Lieferanten) immer **pseudonymisiert**

- Übermittlung auf Anfrage der zuständigen Behörde
  - gesetzliche Rechtsgrundlage für Verarbeitung durch Behörde
  - § 4 ff EpidemieG iVm Art 9 Abs 2 lit i DSGVO aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit

- Übermittlung iZm Förderungsanträgen für Härtefälle
  - gesetzliche Rechtsgrundlage für Verarbeitung durch WKÖ
    - idR aber ohne Offenlegung von Gesundheitsdaten
  - § 2 ff Härtefallfondsgesetz

Datenübermittlung in Zusammenhang mit COVID-19

Exkurs: neue Pflichten für Mobilfunkanbieter

- neuer § 98a TKG – Öffentliches Warnsystem
  - Verpflichtung der Mobilfunkanbieter zur Zusendung von SMS
  - formlose "Weisung" durch Bundesregierung
  - Durchsetzung mit Bescheid bei Nichtbefolgung

- Warnung vor drohenden oder sich ausbreitenden größeren Notfällen und Katastrophen
  - Rechtsgrundlage zur Verarbeitung der erforderlichen Stammdaten

- zielgerichtete Information in Einzelfällen
  - zB bei Suche nach Kontaktpersonen eines Infizierten
  - Rechtsgrundlage zur Verarbeitung der erforderlichen Standortdaten

Verarbeitung von Daten über eine (potentielle) Infektion
Angemessene Sicherheitsmaßnahmen

Datenschutzrechtliche Grundlagen

Angemessene Sicherheitsmaßnahmen (Art 32 DSGVO)

- **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

- Berücksichtigung
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zwecke der Verarbeitung
  - unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos

Datenverarbeitung in Zusammenhang mit COVID-19

Besondere Sicherheitsmaßnahmen

- Gesundheitsdaten → per se höhere Sicherheitsstandards
- Fokus auf "need-to-know Prinzip"
- technische Umsetzung
  - zB durch Verschlüsselung, Berechtigungskonzepte, Zugriffsbeschränkungen, sichere Kommunikationskanäle
  - auch im Home Office sicherstellen
- vorläufige Erleichterung für Gesundheitsdiensteanbieter
  - aktuelle Anpassung des GTelG (bis Ende 2020)
  - Übermittlung von Gesundheitsdaten und genetischen Daten per Fax und E-Mail zulässig
  - Name und SVN als Identifikationsmaßnahmen ausreichend (um Arztbesuche für Arzneimittelbeschaffung zu vermeiden)

Aktuelle COVID-Situation

Weitere datenschutzrechtliche Implikationen

Aktuelle To Dos in Zusammenhang mit COVID-19

Datenschutzrechtliche Implikationen

- Information der Betroffenen?
  - Anpassung der bestehenden Datenschutzhinweise
  - Verlinkung zB in allgemeinem Informationsschreiben

- Ergänzung des Verarbeitungsverzeichnisses

- Evaluierung und ggf Anpassung der internen Prozesse iZm der Ausübung von Betroffenenrechten
  - Vorbereitung auf erhöhte Anzahl an Auskunfts- und Löschbegehren nach Abklingen der Krise

Aktuelle To Dos in Zusammenhang mit COVID-19

Datenschutz-Folgenabschätzung (Art 35 DSGVO)

- Jedenfalls erforderlich, wenn
  - Bewertung auf Basis automatisierter Entscheidungen (Profiling)
  - umfangreiche Verarbeitung sensibler/strafrechtlicher Daten
  - systematische Überwachung öffentlich zugänglicher Bereiche
- Abgrenzung in der Praxis schwierig
  - Europäischer Datenschutzausschuss gibt erste Auslegungshilfen (sehr abstrakt)
  - Black/White Lists der Datenschutzbehörde
- bei ähnlichen Verarbeitungen genügt eine PIA
- laufende Überprüfung erforderlich
- nicht vom Datenschutzbeauftragten zu erstellen ("*Rat*" einholen)

Aktuelle To Dos in Zusammenhang mit COVID-19

Datenschutz-Folgenabschätzung (Art 35 DSGVO)

Black List

Bei Erfüllung eines der folgenden Kriterien, zB	Bei Erfüllung von zumindest zwei der nachfolgenden Kriterien
Bewertung oder Einstufung (einschließlich des Erstellens von Profilen und Prognosen) sofern potentiell nachteilig	Besondere Kategorien von personenbezogenen Daten
Profiling und automatisierte Entscheidungsfindungen	Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten
Beobachtung, Überwachung oder Kontrolle von Betroffenen (insbesondere im öffentlichen Raum)	Erfassung von Standortdaten iSd TKG
Zusammenführen und/oder Abgleich von Datensätzen aus mehreren Verarbeitungen	Daten zu schutzbedürftigen Betroffenen (unmündige Minderjährige, Arbeitnehmer, Patienten, psychisch Kranke, Asylwerber)
Datenverarbeitung im höchstpersönlichen Bereich (auch mit Einwilligung)	

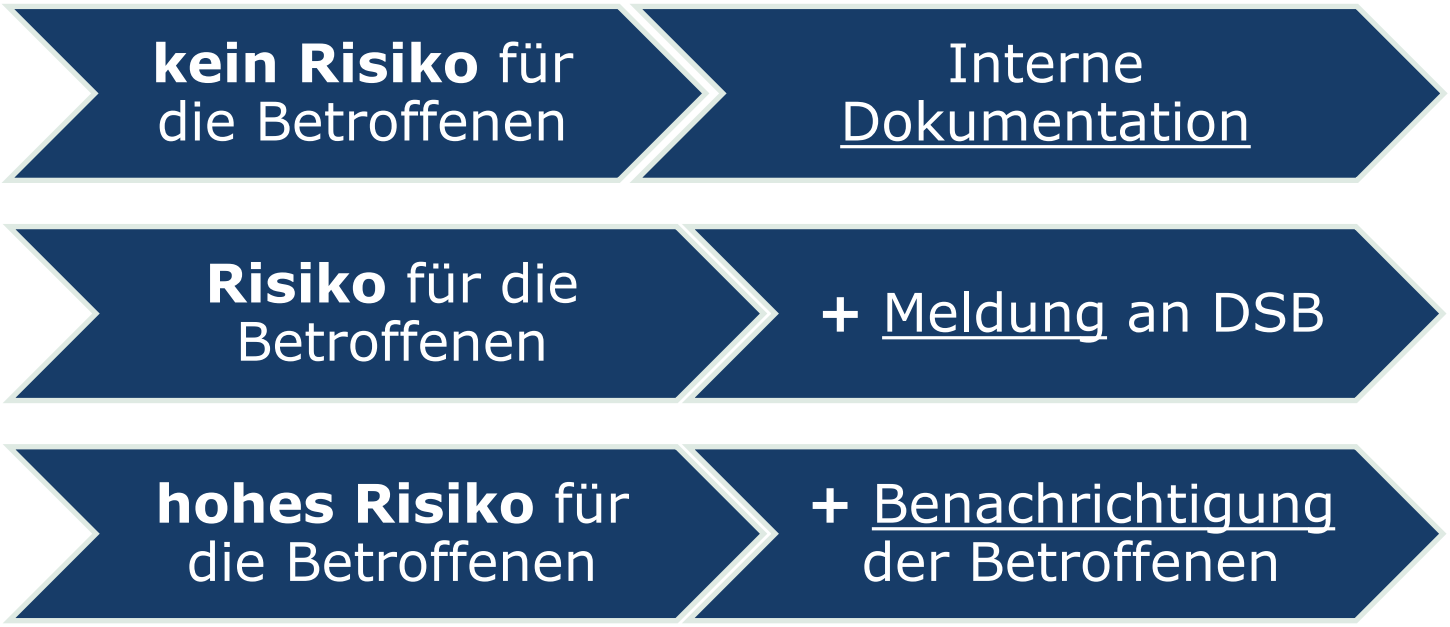
Aktuelle COVID-Situation

Datenschutzverstoß: Was nun?

Datenschutzrechtliche Grundlagen

Datenschutzverstöße: To Dos

- **Evaluierung des Risikos innerhalb von maximal 72 Stunden ab Kenntnis vom Data Breach!**
- Umfassende interne Dokumentation aller Datenvorfälle!



Datenverarbeitung in Zusammenhang mit COVID-19

Datenschutzverstöße: To Dos

- unverzügliche (möglichst binnen 72 Stunden) **Meldung** an die Datenschutzbehörde
  - **KEINE** Hemmung/Unterbrechung während COVID-19 Krise
  - Beschreibung der Art der Verletzung
  - Angabe von Kategorien und Zahl der Betroffenen und Daten
  - Namen und Kontaktdaten des Datenschutzbeauftragten
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der ergriffenen oder vorgeschlagenen Gegenmaßnahmen
- bei hohem Risiko zusätzliche, unverzügliche **Benachrichtigung** der Betroffenen
  - öffentliche Bekanntmachung, wenn sonst unverhältnismäßiger Aufwand
- Praxistipp: im Zweifel eher melden
  - Benachrichtigung der Betroffenen kann von DSB aufgetragen werden

Weitere Auswirkungen der aktuellen Situation

Datenschutz im Home Office

Aktuelle To Dos in Zusammenhang mit COVID-19

Datenschutz im Home Office

- **Mitarbeiter-Awareness schaffen**
- Risikoerhöhung durch Fernzugriff berücksichtigen
  - verschlüsselte VPN-Verbindung erforderlich
  - sensibler Umgang mit Daten/Betriebsgeheimnisses durch AN
  - besondere Vorsicht beim Einsatz privater Geräte
- Vorbereitung der IT-Systeme
  - Kapazitäten, Verfügbarkeit, Updates
  - Ausstattung mit Firmengeräten (Laptops, Smartphones)
- Neubewertung und ggf Anpassung der TOMs
  - regelmäßige Backups
  - Sicherstellung Berichtswege (zB auch für Data Breaches)
  - besondere Vorsicht bei Spam, Malware und Phishing

Aktuelle To Dos in Zusammenhang mit COVID-19

Datenschutz im Home Office

- Sicherstellung der Wahrung des Datengeheimnisses und von Betriebs- und Geschäftsgeheimnissen
  - Leitfaden für TelCos und Videokonferenzen im Home Office
  - Geheimhaltung von Passwörtern
  - Umgang mit ausgedruckten Unterlagen
    - Clean Desk auch im Home Office
    - Aufbewahrung und Zusammenführung nach der Krise
    - Vernichtung während/nach der Krise
- Überprüfung der genutzten Kommunikationsmittel für Austausch von beruflichen Informationen
  - Vorsicht bei kostenlosen, Internet-basierten Anbietern
  - kein Software-Download am Dienstlaptop ohne Freigabe
  - klare Weisungen und Vorgaben

Ansprechpartner

Dr Axel Anderl, LLM

T: +43 1 533 47 95 – 23

E: axel.anderl@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

International Law Office - Information Technology Award for Austria 2014, 2015, 2016, 2017, 2018 & 2019
International Law Office - E-Commerce Award for Austria 2012 & 2013
Managing IP Awards – Austrian Firm of the Year for Copyright & Design 2020