NÄGELE
Rechtsanwälte

28. September 2017 – Kommod Ruggell | RA Mag. iur. Thomas Nägele

Die Datenschutz-Grundverordnung (DSGVO, GDPR)

Rechtlicher Überblick über die EU-Datenschutzgrundverordnung. Welche Firmen sind davon betroffen, was ist zu beachten?

Disclaimer

- Alle Angaben des Vortrages und dieser Präsentation erfolgen ohne Gewähr für die inhaltliche Richtigkeit und Vollständigkeit. Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers.
- Der Vortrag und die Präsentation stellen keine Rechtsberatung dar. Diese muss individuell unter Berücksichtigung der Umstände des Einzelfalls erfolgen.

Thomas Nägele

- Lehrbeauftragter IT-Recht der Universität Liechtenstein
- Gründungsmitglied und Präsident der CRYPTO COUNTRY ASSOCIATION (CCA) e.V., Vaduz
- Gründungspartner der NÄGELE Rechtsanwälte GmbH, Vaduz
- Doktorarbeit (in Arbeit) "Distributed Ledgers and Smart Contracts", Private Universität Liechtenstein
- Studium der Rechtswissenschaften, Universität Wien, Österreich
- Gründer und Verwaltungsrat der ekey biometric systems Est., Vaduz
- 10 Jahre Erfahrung als Softwareprogrammierer

Agenda

- Teil I – Übersicht über die wichtigsten Regelungen
- Teil II – Data Breach Notification Duty
- Teil III – Stand der Umsetzung

NÄGELE
Rechtsanwälte

28. September 2017 | RA Mag. iur. Thomas Nägele

DSGVO 2017

Teil I – Übersicht über die wichtigsten Regelungen

Ziele der Neuordnung

- Vereinheitlichung des EU-Rechts zur Sicherstellung
  - des Schutzes von personenbezogenen Daten als Grundrecht,
  - des freien Datenverkehrs innerhalb des Europäischen Binnenmarktes

Die wichtigsten Änderungen im Überblick

- "Recht auf Vergessen“
- «Opt in» statt «Opt out»
- Recht auf Transparenz
- Weniger «Behördenchaos»
- Grenzübergreifend
- Erweiterter Geltungsbereich
- Hohe Bussgelder
- Stärkung der nationalen Aufsichtsbehörden
- Data Breach Notification Duty

Was regelt die DSGVO?

› Die Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Art. 2 – Anwendungsbereich

- DSGVO 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.
- gilt nicht für die Verarbeitung durch natürliche Personen zur Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten

- → betrifft jeden Unternehmer, der in irgendeiner Art und Weise personenbezogenen Daten erfasst oder verarbeitet.

Erweiterter Geltungsbereich

› Die EU-DSGVO gilt auch für aussereuropäische Unternehmen, die keinen Sitz in der EU haben, sobald sie

- Waren oder Dienstleistungen in der EU anbieten
- oder auch nur Online-Marktforschung unter EU-Bürgern betreiben.

Art. 4 – Begriffsbestimmungen

- Verarbeitung
  - «jeden mit oder ohne Hilfe automatisierter Verfahren angeführten 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, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.»

Art. 4 – Begriffsbestimmungen

- Personenbezogene Daten
  - «alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person («betroffene Person») beziehen;
  - als identifizierbar wird eine natürliche Person angesehen, die … insbesondere mittels Zuordnung zu einer Kennung wie Namen, Kennnummer, Standortdaten, Online-Kennung oder besonderen Merkmalen, die Ausdruck der physischen, psychosozialen, genetischen, psychischen, wirtschaftlichen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;»

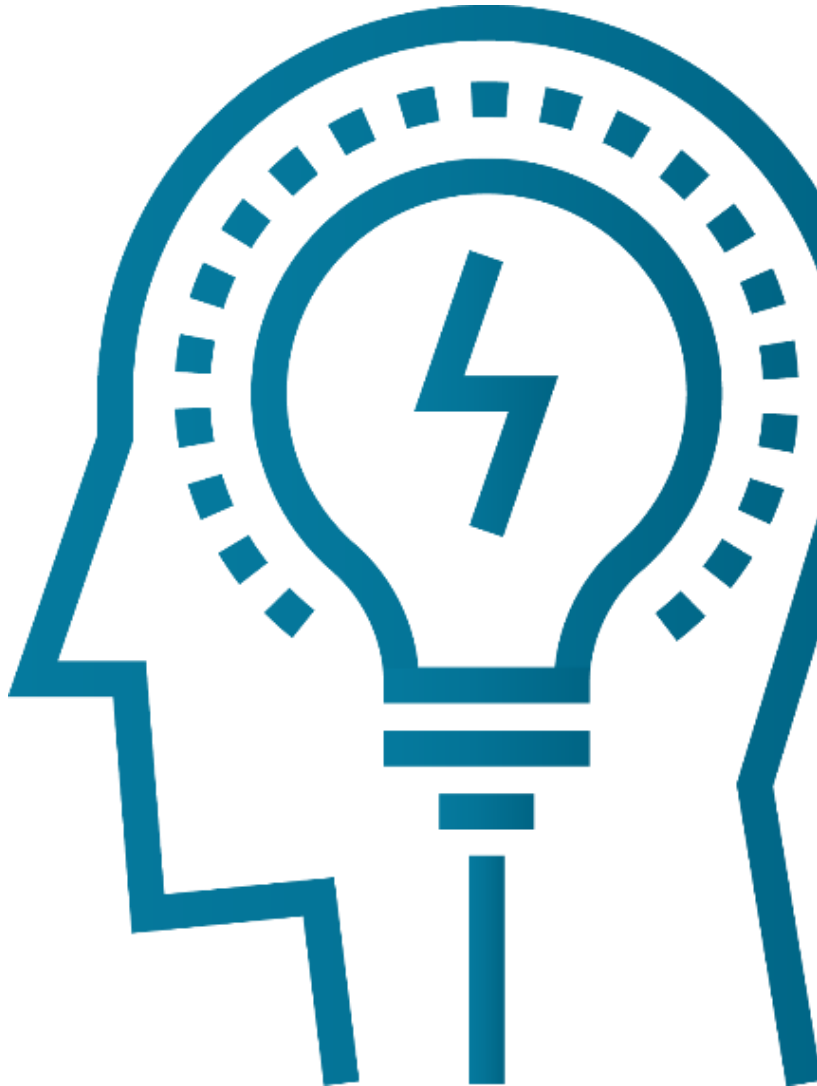
Art. 6 – Rechtmässigkeit der Verarbeitung

› Die Verarbeitung ist nur rechtmässig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Einwilligung der betroffenen Person
- Verarbeitung ist für Erfüllung eines Vertrages, der auf Anfrage der betroffenen Person erfolgt, erforderlich
- Erfüllung rechtlicher Verpflichtungen des Verantwortlichen
- Schutz lebenswichtiger Interessen natürlicher Personen
- Wahrnehmung öffentlicher Aufgabe, die dem Verantwortlichen übertragen wurde
- Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten

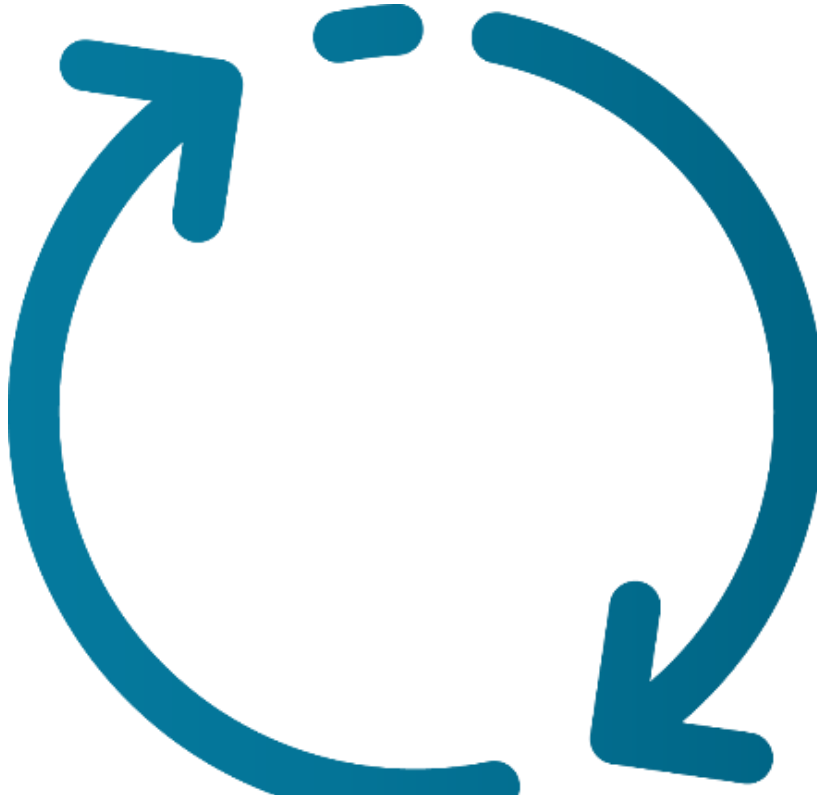
Recht auf Vergessen

- Wollen Nutzer ihre Daten nicht weiter verarbeitet sehen, müssen diese gelöscht werden - vorausgesetzt, es spricht aus juristischer Sicht nichts dagegen (Strafverfolgung, öffentliche Ämter,...).



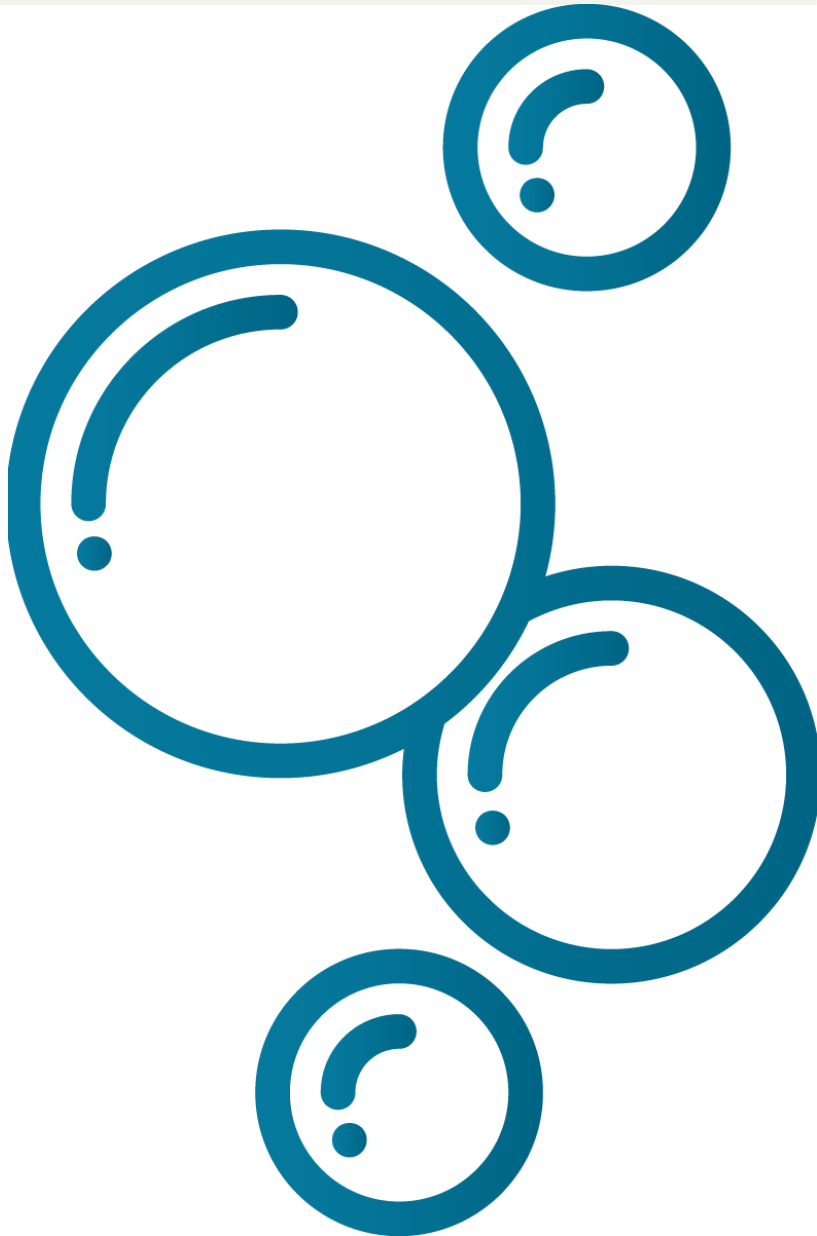
«Opt in» statt «Opt out»

- Sollen persönliche Daten verarbeitet werden, müssen Nutzer aktiv zustimmen
  - bisher ging man automatisch vom Einverständnis aus, wenn der Verarbeitung nicht aktiv widersprochen wurde



Recht auf Transparenz

- Nutzer haben ein Recht auf Transparenz - sie dürfen erfahren, welche Daten über sie gesammelt und wie diese verarbeitet werden.



Neue Zuständigkeit: Weniger Behördenchaos?

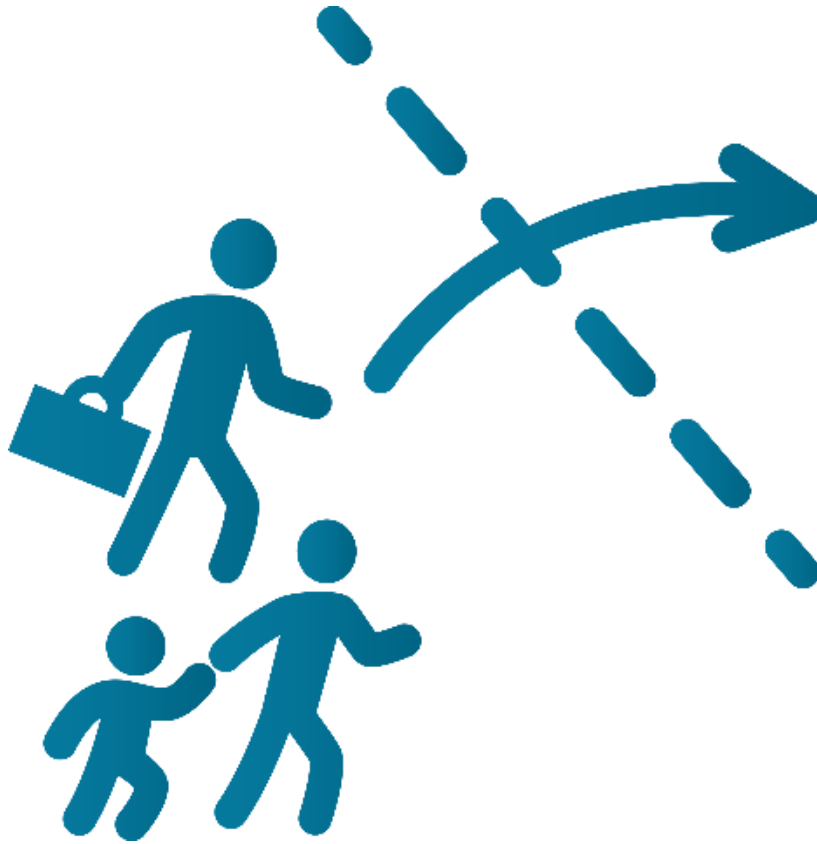
› Unternehmen müssen sich nur noch mit einer einzigen Aufsichtsbehörde auseinandersetzen – und zwar dort, wo sie ihren Hauptsitz haben.

Stärkung der nationalen Aufsichtsbehörden

- Nationale Datenschutzbehörden werden in ihren Kompetenzen gestärkt, so dass sie die neuen EU-Regeln besser umsetzen können.
  - Unter anderem dürfen sie einzelnen Unternehmen verbieten, Daten zu verarbeiten, und Bussgelder verhängen.
- Darüber hinaus dürfen sie Gerichtsverfahren in Datenschutzfragen anstrengen.

Grenzübergreifend

- Privatanwender dürfen jeden Fall von Datenmissbrauch an ihre nationale Aufsichtsbehörde melden - selbst dann, wenn die betroffenen Daten im Ausland verarbeitet wurden.



Art. 5 – Grundsätze Verarbeitung pers. Daten

- Personenbezogene Daten müssen nach folgenden Grundsätzen verarbeitet werden:
  - «Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz»
  - «Zweckbindung»
  - «Datenminimierung» ⟶ nicht mehr Daten, als notwendig!
  - «Richtigkeit»
  - «Speicherbegrenzung»
  - «Integrität und Vertraulichkeit

Art. 5 - Grundsätze für die Datenbearbeitung

› Rechenschaftspflicht:

- Der Verantwortliche ist für die Einhaltung der vorgenannten Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können!

Anforderungen an technischen/personellen Massnahmen (Art. 25 und 32)?

- Stand der Technik
- Datenverschlüsselung/Pseudonymisierung
- Risikoabwägung Eintrittswahrscheinlichkeit Risiko – Ausmass der Sicherungsmassnahme
- Bestellpflicht Datenschutzbeauftragter (Diese ist bindend sofern ein Unternehmen einer Tätigkeit nachgeht, die aus datenschutzrechtlicher Sicht einer besonderen Kontrolle bedarf. Darüber hinaus kann jedes Unternehmen einen Datenschutzbeauftragten freiwillig bestellen.)

Art. 25 - Datenschutz durch Technikgestaltung

- (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten ... sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der ... Risiken ... trifft der Verantwortliche ... geeignete technische ... Massnahmen
  - wie z. B. Pseudonymisierung - ..., die dafür ausgelegt sind, die
  - Datenschutzgrundsätze ... wirksam umzusetzen ...
  - ... und die Rechte der betroffenen Personen zu schützen

Art. 32 - Sicherheit der Verarbeitung

› (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und ... der ... Eintrittswahrscheinlichkeit und Schwere des Risikos ... treffen die Verantwortlichen ... **geeignete technische und organisatorische Massnahmen**, ... ; diese Massnahmen schliessen unter anderem Folgendes ein:

- a) die **Pseudonymisierung und Verschlüsselung**;
- b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme ... auf Dauer sicherzustellen; ...

› (2) Bei der Beurteilung des angemessenen Schutzniveaus sind ... **Risiken zu berücksichtigen**, die mit der Verarbeitung verbunden sind, insbesondere durch ... **unbefugten Zugang, Veränderung, Verlust** ... von Daten, ...

Art. 37 – Benennung eines Datenschutzbeauftragten

I. Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

b) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, **welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder**

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

Art. 37 – Benennung eines Datenschutzbeauftragten

› 2. Eine Unternehmensgruppe darf einen **gemeinsamen Datenschutzbeauftragten** ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

Art. 37 – Wer kann Datenschutzbeauftragter sein?

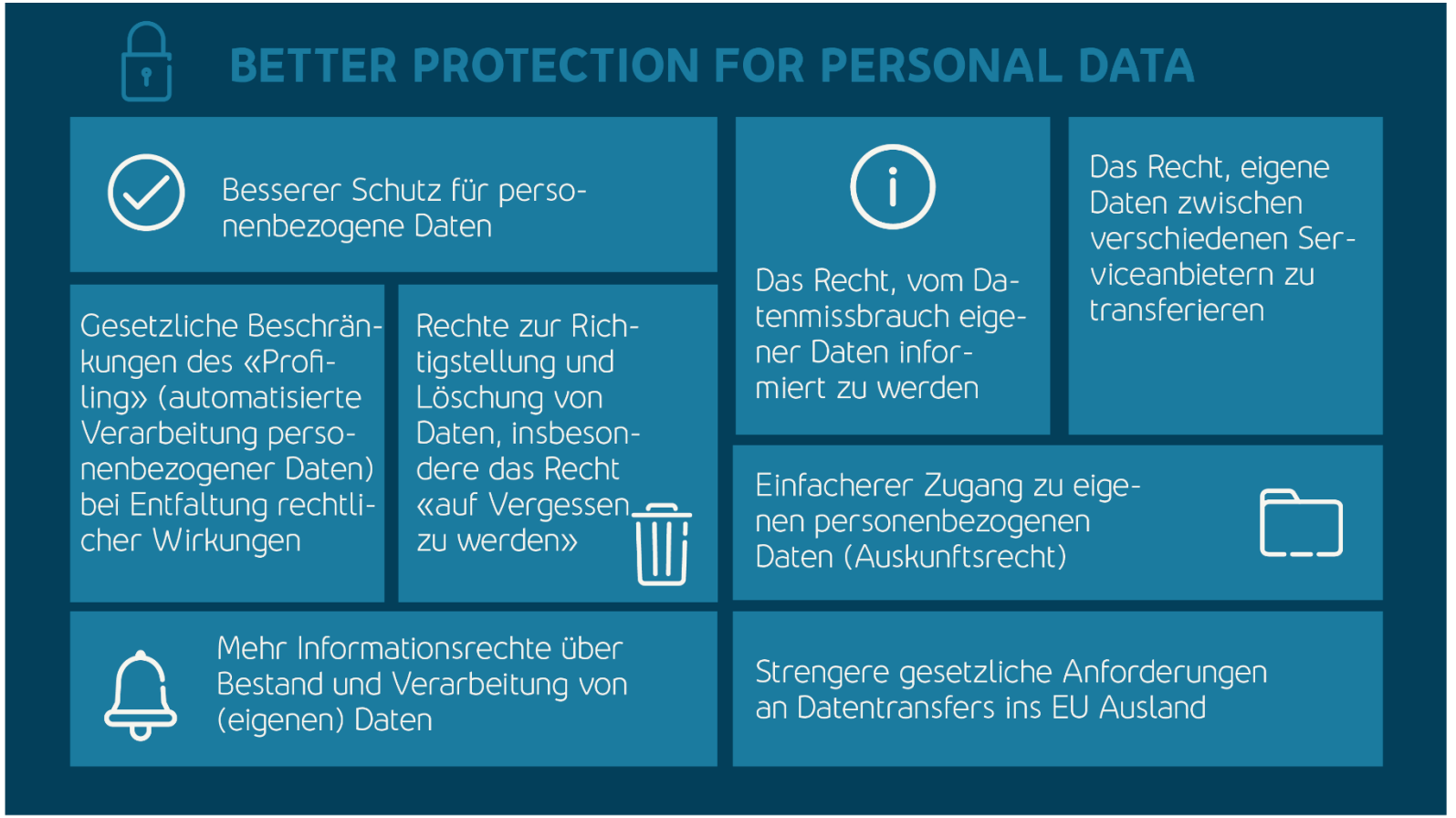
- Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und **insbesondere des Fachwissens benannt**, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
- 6. Der Datenschutzbeauftragte **kann Beschäftigter** des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines **Dienstleistungsvertrags** erfüllen.
- 7. Der Verantwortliche oder der Auftragsverarbeiter **veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.**

Verstoss gegen die DSGVO

- Wie hoch sind die Bussgelder?
- Trifft es auch den Bäckereibetrieb im Dorf?

Art. 83 - Verhängung von Geldbussen

- (1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbussen ... in jedem Einzelfall wirksam, verhältnismässig und abschreckend ist.
- (5) Bei Verstössen gegen die folgenden Bestimmungen ... werden ... Geldbussen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu **4 % seines gesamten weltweit erzielten Jahresumsatzes** ... verhängt, je nachdem, welcher der Beträge höher ist:
  - a) die Grundsätze für die Verarbeitung, ...
  - b) die Rechte der betroffenen Person gemäss den Artikeln 12 bis 22


BETTER PROTECTION FOR PERSONAL DATA
Besserer Schutz für personenbezogene Daten
Gesetzliche Beschränkungen des «Profiling» (automatisierte Verarbeitung personenbezogener Daten) bei Entfaltung rechtlicher Wirkungen
Rechte zur Richtigstellung und Löschung von Daten, insbesondere das Recht «auf Vergessen zu werden»
Das Recht, vom Datenmissbrauch eigener Daten informiert zu werden
Das Recht, eigene Daten zwischen verschiedenen Serviceanbietern zu transferieren
Einfacherer Zugang zu eigenen personenbezogenen Daten (Auskunftsrecht)
Mehr Informationsrechte über Bestand und Verarbeitung von (eigenen) Daten
Strengere gesetzliche Anforderungen an Datentransfers ins EU Ausland
Strafen
bis zu Euro 20 Millionen
oder
4 % des Jahresumsatzes

NÄGELE
Rechtsanwälte

28. September 2017 | RA Mag. iur. Thomas Nägele

Die Datenschutz-Grundverordnung (DSGVO, GDPR)

Teil II – Data Breach Notification Duty

Neuerung: Schnellere Meldung bei Datenverlust

- Tritt ein Datenverlust auf, müssen Unternehmen und Organisationen unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden ihre Behörde benachrichtigen.
- Die betroffenen Personen sind bei hohem Risiko unverzüglich zu informieren.

Data Breach Notification Duty

- Data Breaches sind Verstösse gegen die Datensicherheit und den Datenschutz, bei denen personenbezogene Daten Unberechtigten vermutlich oder erwiesenermassen bekannt werden.
- Ursachen dafür sind vielfältig und können z.B. in einem Hackerangriff, dem Verlust eines USB-Sticks, dem Diebstahl eines Smartphones oder in einem unbefugten Weitergeben durch Mitarbeiter – gleichgültig ob bewusst oder unbewusst – liegen.
- Folgen: Rufschädigung/Kreditkartenmissbrauch/Identitätsdiebstahl/

Art. 33 und 44 - Meldung von Verletzungen

- 33 (I) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der … Aufsichtsbehörde …
- ⟶ In Liechtenstein Datenschutzstelle
- 34 (I) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen …, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich …
- 34 (3) Die Benachrichtigung … ist nicht erforderlich, wenn …
  - a)… Daten …, unzugänglich gemacht werden, etwa durch Verschlüsselung; …

Dokumentationspflicht

- Dem Verantwortlichen nach Art. 33 Abs. 5 DSGVO werden in Bezug auf die Data Breach Notification Dokumentationspflichten hinsichtlich
  - aller Verletzungen des Schutzes personenbezogener Daten einschliesslich
  - aller damit im Zusammenhang stehenden Fakten,
  - deren Auswirkungen und
  - der ergriffenen Abhilfemassnahmen auferlegt.

Ablauf Data Breach Notification

- Unternehmen gibt Data Breach/Datenpanne der Behörde und dem Individuum bekannt
- Aufsichtsbehörde veröffentlicht eine Bekanntmachung und leitet eine Untersuchung ein
- Aufsichtsbehörden anderer EU Mitgliedstaaten leiten ebenfalls Untersuchungen ein
- Sammelklagen werden erhoben
- Veröffentlichung bzw. Veröffentlichung durch Medien

NÄGELE
Rechtsanwälte

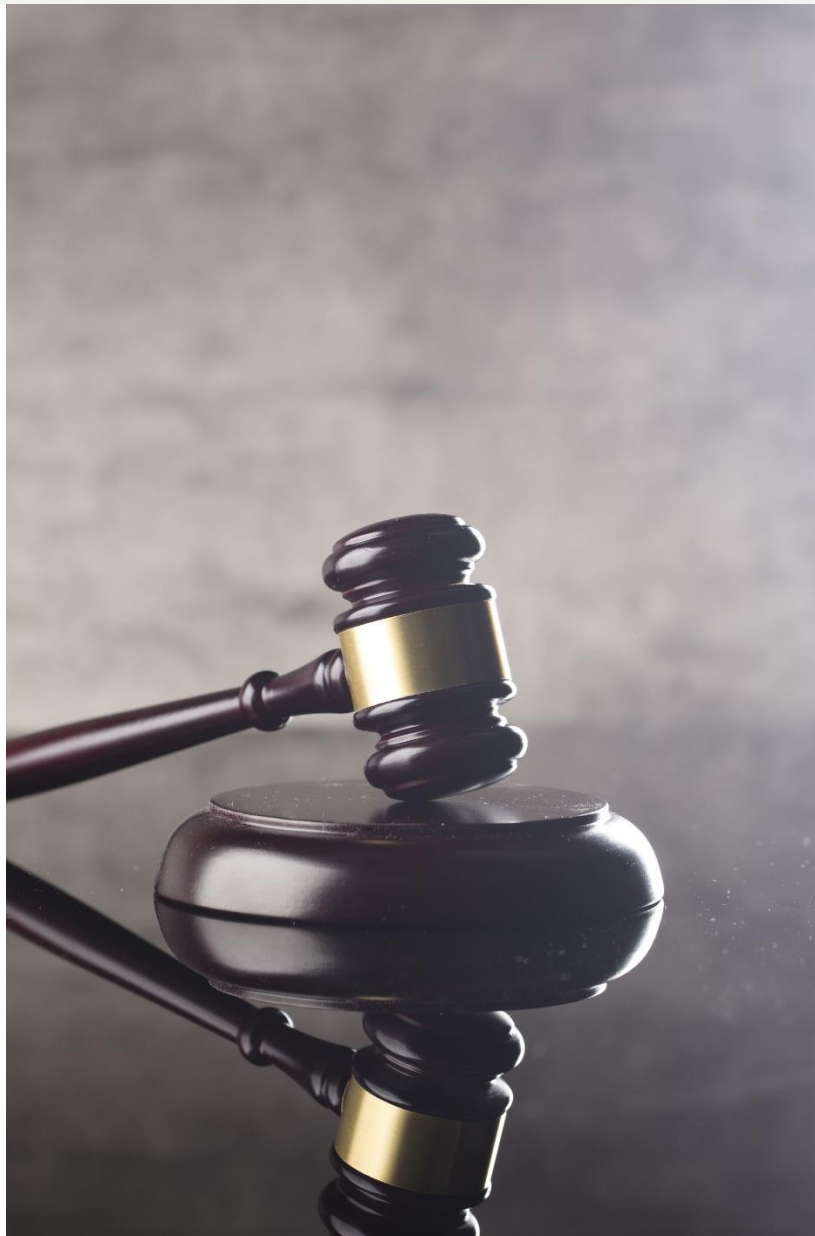
28. September 2017 | RA Mag. iur. Thomas Nägele

Die Datenschutz-Grundverordnung (DSGVO, GDPR)

Teil III – Stand der Umsetzung

Kurzübersicht DSGVO

- Titel: Verordnung (EU) 2016/679
- Kurztitel: Datenschutz-Grundverordnung
- Rechtsnatur: Verordnung
- Geltungsbereich: Europäische Union
- Rechtsmaterie: Datenschutzrecht
- Veröffentlichung: 4. Mai 2016
- Inkrafttreten: 25. Mai 2016
- Wirksam ab: 25. Mai 2018



Verordnung vs. Richtlinie

- Verordnungen haben allgemeine Geltung (in der EU). Sie sind in allen Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat.
- Richtlinien werden an Mitgliedstaaten gerichtet und sind für diese hinsichtlich des zu erreichenden Ziels verbindlich.
- ⇒ Bei der DSGVO handelt es sich um eine Verordnung, welche ab 25.Mai 2018 in allen (EU) Mitgliedstaaten unmittelbar anwendbar und wirksam ist!

Liechtenstein?

- Datenschutz-Grundverordnung (DSGVO) ersetzt DS-RL und damit Grundlage für DSG-Anwendbarkeit in der EU ab 25. Mai 2018
- Übernahmebeschluss durch gemeinsamen EWR-Ausschuss,
- Kundmachung durch liechtensteinischen Gesetzgeber

Innerstaatliches Verfahren

- Ausarbeitung eines Vernehmlassungsberichtes für ein Umsetzungsgesetz DSGVO (Amt für Justiz, AJU)
- Aufhebung / Anpassung des DSG
- Umgang mit Öffnungsklauseln?

Stand der Umsetzung

- Die DSGVO gilt ab 25. Mai 2018 in allen (EU) Mitgliedstaaten, ist unmittelbar anwendbar und wirksam
- In Liechtenstein: wirksam ab 25. Mai 2018, wenn bis dahin
  - die zentralen Fragen geklärt sind;
  - ein entsprechender EWR Übernahmebeschluss vorliegt und;
  - innerstaatlich eine Durchführungsverordnung kundgemacht wird.

Weitere Informationen

- Webseite der Datenschutzstelle:
  - http://www.llv.li/#/117567/informationen
- Gesetzgebungsakt EU-DSGVO
  - http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

Fragen?

- Kontaktieren Sie mich per E-Mail: tn@naegele.law
- Besuchen Sie auch unseren Rechts-Blog unter www.naegele.law/blog

NÄGELE
Rechtsanwälte

28. September 2017 | RA Mag. iur. Thomas Nägele

Vielen Dank für die Aufmerksamkeit

NÄGELE Rechtsanwälte GmbH | Landstrasse 60, 9490 Vaduz | T 237 60 70 | tn@naegele.law