quintessenz
Datenschutz ist Menschenrecht

Einführung in den Datenschutz

EU-DSGVO ab 25.Mai 2018

Mag. Georg Markus Kainz

quintessenz
Datenschutz ist Menschenrecht

Prinzipien der Datenverarbeitung

- **Rechtmäßigkeit**
  nach dem Grundsatz von Treu und Glauben
- **Transparenz**
  für die betroffene Person nachvollziehbar
- **Zweckbindung**
  nur für den Zweck zu dem sie generiert wurden
- **Datenminimierung**
  dem Zwecke angemessen
- **Richtigkeit**
  und auf dem neuesten Stand
- **Speicherbegrenzung**
  nur solange gespeichert wie notwendig
- **Integrität und Vertraulichkeit**

quintessenz
Datenschutz ist Menschenrecht

Wie sicher ist die Infrastruktur

- spanische Telefónica
- britischer National Health Service (NHS)
- US-Logistikunternehmen FedEx
- französische Automobilkonzern Renault
- japanische Automobilhersteller Nissan
- Deutsche Bahn mit der Logistiktochter Schenker
- spanische Banco Bilbao Vizcaya Argentaria
- brasilianische Telekommunikationsunternehmen Vivo
- schwedische Unternehmen Sanduk
- chinesische Ölkonzern PetroChina
- rumänische Außenministerium
- russisches Innenministeriums (MWD)
- russisches Katastrophenschutzministerium
- russisches Telekommunikationsunternehmen MegaFon

quintessenz
Datenschutz ist Menschenrecht

Wie sicher ist die Infrastruktur

- ☐ War das Unternehmen vor **WannaCry** geschützt?
  - ☐ gab es einen Maßnahmen-Plan
  - ☐ eine Fallbackvariante
  - ☐ Information der Mitarbeiter

quintessenz
Datenschutz ist Menschenrecht

Compliance-Anforderungen

- ☐ Welche Anwendungen fallen unter die DSGVO und was ist zu tun?
- ☐ Werden personenbezogene Daten verarbeitet?
- ☐ Werden sensible, personenbezogene Daten verarbeitet?
- ☐ Werden die Daten zum Profiling genutzt?
- ☐ Werden Daten compliancemäßig an Dritte/ Empfängern weitergegeben?
- ☐ Sind die Mitarbeiter compliancemäßig instruiert und geschult?
- ☐ Muss ein Verfahrensregister geführt werden?
- ☐ Ist die Speicherdauer der verschiedenen Datenkategorien überprüft worden?
- ☐ Sind die technischen und organisatorischen Sicherheitsmaßnahmen dokumentiert?
- ☐ Muss eine Datenschutzfolgeabschätzung gemacht werden?
- ☐ Haben die Kunden wirksam eingewilligt und wurden sie über die Datenverarbeitung belehrt.
- ☐ Ist ein Verfahren aufgesetzt wie Datenauskünfte erteilt werden?
- ☐ Wie wird mit Löschanträgen verfahren?
- ☐ Sind Verträge, AGBs compliancemäßig angepasst worden?
- ☐ Muss die Datenschutzbehörde verpflichtend konsultieren werden?

quintessenz
Datenschutz ist Menschenrecht

EU-Datenschutz-Grundverordnung

- ☐ Verarbeitung der Daten nur nach ausdrücklicher Einwilligung der betroffenen Person;
- ☐ Recht der Betroffenen, bei Verletzung des Schutzes der eigenen Daten darüber informiert zu werden;
- ☐ Datenschutzbestimmungen müssen in klarer und verständlicher Sprache erläutert werden
- ☐ bei Verstößen wird härter durchgegriffen; im Fall eines Unternehmens werden Strafen von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt.

quintessenz
Datenschutz ist Menschenrecht

EU-Datenschutz-Grundverordnung

- ☐ Recht auf Vergessenwerden
- ☐ Recht auf Datenportabilität
- ☐ Privacy by Design
- ☐ Privacy by Default
  - ☐ Opt-Out
  - ☐ Opt-In
- ☐ Datenschutzbeauftragte
- ☐ Dokumentationspflichten

quintessenz
Datenschutz ist Menschenrecht

Wirksame Einwilligung

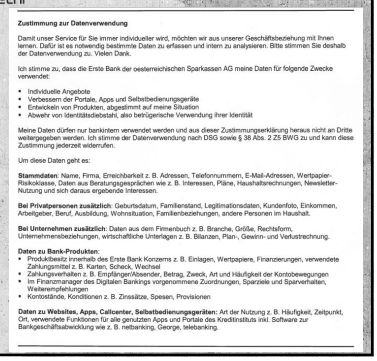
- ☐ Einwilligung muss freiwillig erfolgen
- ☐ Zustimmung in informierter Weise

- ☐ Verträge, Allgemeinen Geschäftsbedingungen und die Website müssen angepasst werden
- ☐ Formulare, egal ob analog oder digital, müssen auf ihre Datenschutzhinweise, Belehrungen und Widerrufsmöglichkeiten hin überprüft werden

- ☐ allgemeine Klauseln in den AGBs reichen nicht

quintessenz
Datenschutz ist Menschenrecht

AGBs



Zustimmung zur Datenverwendung

Damit unser Service für Sie immer individueller wird, möchten wir aus unserer Geschäftsbeziehung mit Ihnen lernen. Dafür ist es notwendig bestimmte Daten zu erfassen und intern zu analysieren. Bitte stimmen Sie deshalb der Datenverwendung zu. Vielen Dank.

Ich stimme zu, dass die Erste Bank der oesterreichischen Sparkassen AG meine Daten für folgende Zwecke verwendet:

- Individuelle Angebote
- Verbessern der Portale, Apps und Selbstbedienungsgeräte
- Entwickeln von Produkten, abgestimmt auf meine Situation
- Abwehr von Identitätsdiebstahl, also betrügerische Verwendung ihrer Identität

Meine Daten dürfen nur bankintern verwendet werden und aus dieser Zustimmungserklärung heraus nicht an Dritte weitergegeben werden. Ich stimme der Datenverwendung nach DSG sowie § 38 Abs. 2 Z5 BWG zu und kann diese Zustimmung jederzeit widerrufen.

Um diese Daten geht es:

Stammdaten: Name, Firma, Erreichbarkeit z. B. Adressen, Telefonnummern, E-Mail-Adressen, Wertpapier-Risikoklasse, Daten aus Beratungsgesprächen wie z. B. Interessen, Pläne, Haushaltsrechnungen, Newsletter-Nutzung und sich daraus ergebende Interessen.

Bei Privatpersonen zusätzlich: Geburtsdatum, Familienstand, Legitimationsdaten, Kundenfoto, Einkommen, Arbeitgeber, Beruf, Ausbildung, Wohnsituation, Familienbeziehungen, andere Personen im Haushalt.

Bei Unternehmen zusätzlich: Daten aus dem Firmenbuch z. B. Branche, Größe, Rechtsform, Unternehmensbeziehungen, wirtschaftliche Unterlagen z. B. Bilanzen, Plan-, Gewinn- und Verlustrechnung.

Daten zu Bank-Produkten:

- Produktbesitz innerhalb des Erste Bank Konzerns z. B. Einlagen, Wertpapiere, Finanzierungen, verwendete Zahlungsmittel z. B. Karten, Scheck, Wechsel
- Zahlungsverhalten z. B. Empfänger/Absender, Betrag, Zweck, Art und Häufigkeit der Kontobewegungen
- Im Finanzmanager des Digitalen Bankings vorgenommene Zuordnungen, Sparziele und Sparverhalten, Weiterempfehlungen
- Konditionen z. B. Zinssätze, Spesen, Provisionen

Daten zu Websites, Apps, Callcenter, Selbstbedienungsgeräten: Art der Nutzung z. B. Häufigkeit, Zeitpunkt, Ort, verwendete Funktionen für alle genutzten Apps und Portale des Kreditinstituts inkl. Software zur Bankgeschäftsabwicklung wie z. B. netbanking, George, telebanking.

quintessenz
Datenschutz ist Menschenrecht

Recht auf Vergessenwerden

- Art. 17 - Wann müssen Daten gelöscht werden
  - Wenn die Speicherung der Daten nicht mehr notwendig ist
  - Wenn der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat
  - Wenn die Daten unrechtmäßig verarbeitet wurden
  - Wenn eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht

quintessenz
Datenschutz ist Menschenrecht

Recht auf Vergessenwerden

- Wann findet das Recht auf Vergessenwerden **keine** Anwendung?
  - Wenn das Recht auf freie Meinungsäußerung bzw. die Informationsfreiheit überwiegen
  - Wenn die Datenspeicherung der Erfüllung einer rechtlichen Verpflichtung dient
  - Wenn das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt
  - Wenn Archivzwecke oder wissenschaftliche und historische Forschungszwecke entgegenstehen
  - Wenn die Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist

quintessenz
Datenschutz ist Menschenrecht

Recht auf Datenportabilität

- **Art. 20**
  - Der Betroffene soll befugt sein, die von ihm zur Verfügung gestellten Daten von einer automatisierten Anwendung, etwa einem sozialen Netzwerk, auf eine andere Anwendung zu übertragen.
  - Betroffene sollen dadurch leichter von einem Anbieter zu einem anderen wechseln können, ohne den Verlust ihrer Daten befürchten zu müssen.

quintessenz
Datenschutz ist Menschenrecht

Betroffenenrechte

- ☐ Art. 12 bis 22
  - ☐ Informationsrecht
    - ☐ Art. 13 - **sofort** bei Erhebung der Daten
  - ☐ Auskunfts- und Widerspruchsrecht
  - ☐ Recht auf Berichtigung, Löschung und Einschränkung
  - ☐ Recht auf Datenübertragbarkeit

quintessenz
Datenschutz ist Menschenrecht

Informationsrecht

- ☐ Name und Kontaktdaten des Verantwortlichen (ggf. auch des Vertreters)
- ☐ Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- ☐ Zweck und Rechtgrundlage der Verarbeitung
- ☐ Berechtigte Interessen (bei Verarbeitung nach Art. 6 DSGVO)
- ☐ Empfänger bzw. Kategorien von Empfängern
- ☐ Übermittlung in Drittland oder an internationale Organisation
- ☐ Dauer der Speicherung
- ☐ Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit
- ☐ Bestehen eines Rechts auf Widerspruch der Einwilligung
- ☐ Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ☐ Information, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und mögliche Folgen der Nichtbereitstellung
- ☐ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- ☐ Information über eine mögliche Zweckänderung der Datenverarbeitung

quintessenz
Datenschutz ist Menschenrecht

Auskunftsrecht

- ☐ Zwecke der Datenverarbeitung
- ☐ Kategorien der Daten
- ☐ Empfänger oder Kategorien von Empfängern
- ☐ Dauer der Speicherung
- ☐ Recht auf Berichtigung, Löschung und Widerspruch
- ☐ Beschwerderecht bei einer Aufsichtsbehörde
- ☐ Herkunft der Daten (wenn nicht bei Betroffenen erhoben)
- ☐ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- ☐ Übermittlung in Drittland oder an internationale Organisation

quintessenz
Datenschutz ist Menschenrecht

Datenschutzmanagementsystem

- ☐ **Art. 5 –** Grundsätze für die Verarbeitung personenbezogener Daten
- ☐ **Art. 30 –** Verzeichnis aller Verarbeitungstätigkeiten
- ☐ **Art. 32 –** technische und organisatorische Maßnahmen umzusetzen haben, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung von personenbezogenen Daten gemäß DSGVO erfolgt
- ☐ **Art. 35 –** verpflichtet bei Verarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, vorab eine Abschätzung der Folgen durchzuführen

quintessenz
Datenschutz ist Menschenrecht

Nachweispflichten („accountability").

- ☐ Art. 5 Abs. 2 - Unternehmen müssen beweisen können, dass sie geeignete Datenschutzrichtlinien und geeignete Datenschutzvorkehrungen umsetzen

quintessenz
Datenschutz ist Menschenrecht

Meldung von Datenschutzverstößen

- ☐ Unternehmen muss einen Prozess implementieren
  - ☐ Verletzung wird erkannt
  - ☐ Datenschutzbeauftragter erhält Meldung
  - ☐ Bewertet ob kein oder normales oder hohes Risiko für die Rechte und Freiheiten von Betroffenen vorliegt
- ☐ Art. 33 Abs. 1
  - ☐ im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich (binnen 72 Stunden) die Verletzung bei der zuständigen Aufsichtsbehörde melden
- ☐ Art. 34
  - ☐ bei einem hohen Risiko für die persönlichen Rechte und Freiheiten zusätzlich die Betroffenen zu informieren

quintessenz
Datenschutz ist Menschenrecht

Nachweis der Datensicherheit

- ☐ Pseudonymisierung
- ☐ Verschlüsselung
- ☐ Ansonsten keine konkreten Vorschriften
  - ☐ in DE gab es§ 9 BDSG mit genauen Regeln
    - ☐ Zutrittskontrolle
    - ☐ Zugangskontrolle
    - ☐ Zugriffskontrolle
    - ☐ Weitergabekontrolle
    - ☐ Eingabekontrolle
    - ☐ Auftragskontrolle
    - ☐ Verfügbarkeitskontrolle

quintessenz
Datenschutz ist Menschenrecht

Datensicherheit

- ☐ Wer hat Zugriff auf die Daten
- ☐ An wen wurden die Daten weitergegeben
- ☐ Wie werden die Daten gesichert
- ☐ Wie wird die Infrastruktur abgesichert
  - ☐ Fernzugriff
  - ☐ LapTop
  - ☐ SmartPhones
  - ☐ Kopierer
  - ☐ IoT

quintessenz
Datenschutz ist Menschenrecht

Allgemeinen Erklärung
der Menschenrechte
Artikel 12

Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Georg Markus Kainz
kainz@quintessenz.at
+43 676 – 74 83 676