xtention
IT with care.

DSGVO und der richtige Umgang mit personenbezogenen Daten in meinem Arbeitsbereich

Datenschutz

Webex, März 2022, Montanuniversität Leoben

MONTAN UNIVERSITÄT LEOBEN

UNTERNEHMENSGRUPPE

xtention IT with care. | soffico | icw | xD | it for industries

Vorstellung

Mag. iur. Martina Wenghofer MA

Datenschutzjuristin

bei x-tention Informationstechnologie GmbH

Ausbildung

Studium der Rechtswissenschaften

Studium IT-Recht und Management

Zertifizierungen

Datenschutzbeauftragter (WIFI - Wirtschaftsförderungsinstitut)

Mag. iur. Tina Nagler

Datenschutzjuristin

bei x-tention Informationstechnologie in Graz

Ausbildung

Studium der Rechtswissenschaften

Zertifizierungen

Datenschutzbeauftragte (Bitkom Akademie)

Agenda

01 Datenschutz – Kurze Einführung

02 DSGVO - Geltungsbereich

03 DSGVO - Definitionen

04 DSGVO - Prinzipien und Grundsätze

05 DSGVO - Betroffenenrechte

06 DSGVO - Datenschutzvorfall

07 Datengeheimnis

08 Lessons Learned

01

Datenschutz

Kurze Einführung

Datenschutz

Was ist Datenschutz?

- Schutz der Privatsphäre
- Freiheit der Menschen, ihre Daten selbst zu bestimmen (informationelle Selbstbestimmung)

Warum brauchen wir Datenschutz?

Ich hab doch nichts zu verbergen!?

- Privatsphäre
- Ob man etwas zu verbergen hat, liegt im Auge des Betrachters
- Private Daten haben einen Wert
- Datensparsamkeit (Data Minimization) ist Risikominimierung
- Gelegenheit macht Datendiebe
- Was heute harmlos ist, ist es morgen vielleicht nicht mehr

Wie viel verdienen Sie?

Darf ich Ihr E-Mail-Passwort haben?

Wozu sollen Sie Ihre Haustüre absperren?

Was haben Sie diese Woche eingekauft?

Wenn Sie jemanden 24h beobachten würde, würden Sie etwas an Ihrem verhalten ändern?

Traditioneller Datenschutz

Artikel 8 der Europäischen Grundrechtecharta

Recht auf Achtung des Privat- und Familienlebens

Jeder hat das Recht auf Achtung seiner Privatsphäre und Familie Leben, sein Zuhause und seine Korrespondenz.

DSGVO

Datenschutz-Grundverordnung der EU

- Gilt seit 25. Mai 2018
- Einheitliche Regeln zum Datenschutz für alle Mitgliedstaaten der EU
- Große Anzahl an Öffnungsklauseln
  - Dadurch sind auch unterschiedliche Regelungen je Mitgliedstaat möglich
  - Siehe z. B. Österreich: DSG
- Ziel: Schutz personenbezogener Daten und Befähigung des Einzelnen
- Betroffenenrechte im Fokus
  - In der DSGVO gibt es einen eigenen Abschnitt zu Betroffenenrechten

02

DSGVO

Geltungsbereich

DSGVO

Welche Arten von Daten gibt es?

Personenbezogene Daten

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Adresse, Telefonnummer).

Besondere Kategorien personenbezogener Daten („sensible Daten“)

- Rassische oder ethnische Herkunft
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse oder weltanschauliche Überzeugungen
- Genetische oder biometrische Daten
- Gesundheit
- Sexualleben oder sexuelle Orientierung

Materieller/inhaltlicher Anwendungsbereich

Wann gilt sie?

z.B. Internet, E-mail, `Computer

“Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.".”

z.B. handgeschriebene Notiz, Papierdokument

strukturierte Sammlung von Daten, auf die nach bestimmten Kriterien zugegriffen werden kann

Nicht umfasst

- Papierakte, die nicht nach bestimmten Kriterien sortiert ist
- Ausnahme für rein persönliche oder haushaltsmäßige Tätigkeiten

Räumlicher Anwendungsbereich

Wo gilt die DSGVO?

- Der räumliche Geltungsbereich ist weit gefasst
- Es gibt 3 Hauptanwendungsfälle
  1. Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der EU (Unerheblich, ob die Verarbeitung in der EU stattfindet oder nicht)
  2. Verantwortlicher oder Auftragsverarbeiter sind nicht in der EU niedergelassen, bieten aber Betroffenen in der EU Waren oder Dienstleistungen an
  3. Auch wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter nicht in der EU, sondern an einem Ort niedergelassen ist, an dem das Recht der Mitgliedstaaten gilt

03

DSGVO

Definitionen

Definitionen

Personenbezogene Daten

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

Name

Telefonnummer

IP-Address

E-Mail-Addresse

Geburtsdatum

Krankenstand

Nummernschild

Gesundheitsdaten

Haut-,Haar-, Augenfarbe

Urlaubsplanung

Job

Familienstand

Addresse

Einkommen

Kleidergröße

Vermögenssituation

Ausbildung

Solzialversicherungsnummer

Steurnummer

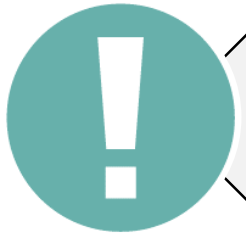
Religionsbekenntnis

Bankverbindung

Definitionen

Personenbezogene Daten

- Besondere Kategorien von Daten
  - Rasse oder ethnische Herkunft
  - Politische Meinungen
  - Religiöser oder philosophischer Glaube
  - Gewerkschaftsmitgliedschaft
  - Genetische Daten
  - Biometrische Daten
  - Sexuelle Orientierung
  - Gesundheitsdaten



Die Verarbeitung dieser Art von Daten ist verboten und nur unter bestimmten Umständen erlaubt und muss mit besonderer Sorgfalt behandelt werden.

Defintionen

Pseudonymisierung und Anonymisierung

- Pseudonymisierung
  - Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können
  - zusätzliche Informationen müssen gesondert aufbewahrt werden und unterliegen technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden
- Anonymisierung
  - Verarbeitung der Entfernung aller persönlichen Identifikatoren, die zu einer Person führen könnten

Pseudonyme Daten sind ebenfalls personenbezogene Daten und fallen in den Anwendungsbereich der DSGVO!

Definitionen

Rollen/Beteiligte

- Betroffener
  - natürliche oder natürliche Person, die Gegenstand personenbezogener Daten ist
- Verantwortlicher
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten bestimmt, so können der Verantwortliche oder die spezifischen Kriterien für seine Benennung im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehen werden
- Auftragsverarbeiter
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet

Definitionen

Rollen/Beteiligte

- Empfänger
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, gegenüber der die personenbezogenen Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen einer bestimmten Untersuchung im Einklang mit dem Unionsrecht oder dem Recht der Mitgliedstaaten personenbezogene Daten erhalten können, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch diese Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften entsprechend den Zwecken der Verarbeitung
- Dritter
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten

04

DSGVO

Prinzipien und Grundsätze

DSGVO

Grundsätze der DSGVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

- Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Zweckbindung

- Die Verarbeitung von Daten ist immer auf einen bestimmten Zweck festgelegt. Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden.

Datenminimierung

- Daten dürfen nur in dem Ausmaß erhoben und verarbeitet werden, in dem sie benötigt werden.

Speicherbegrenzung

- Der Personenbezug darf nur solange gegeben sein, wie es für den bestimmten Zweck erforderlich ist.

DSGVO

Grundsätze der DSGVO

Richtigkeit

- Es sind alle angemessenen Maßnahmen zu treffen, damit die Daten sachlich richtig sind.

Integrität und Vertraulichkeit

- Die Sicherheit der verarbeiteten Daten ist sicherzustellen, v.a. Vertraulichkeit, Integrität und Verfügbarkeit.

Rechenschaftsplicht

- Die Einhaltung der angeführten Grundsätze (Konformität zur DSGVO) muss nachgewiesen werden können.

05

DSGVO

Betroffenenrechte

DSGVO

Betroffenenrechte

Recht auf Auskunft (Art. 15)

- Der Betroffene kann Auskunft über die personenbezogenen Daten verlangen, die über ihn verarbeitet werden.

Recht auf Berichtigung (Art. 16)

- Falls Informationen fehlerhaft sind, kann der Betroffene die Richtigstellung verlangen.

Recht auf Löschung (Art. 17)

- Der Betroffene kann verlangen, dass Daten, die ihn betreffen, unverzüglich gelöscht werden.
- Dies gilt nur, wenn dem keine gesetzlichen Verpflichtungen entgegenstehen wie z.B. die gesetzliche Aufbewahrungspflicht von Vertragsdaten von 7 Jahren oder von Gesundheitsdaten von 30 Jahren.

DSGVO

Betroffenenrechte

Recht auf Einschränkung der Verarbeitung (Art. 18)

- Die betroffene Person hat das Recht unter bestimmten Umständen die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen.

Recht auf Datenübertragbarkeit (Art. 20)

- Der Betroffene hat das Recht, seine personenbezogenen Daten in einer strukturierten, gängigen und maschinenlesbaren Form zu erhalten oder diese an einen anderen Verantwortlichen übermitteln zu lassen.

Recht auf Widerspruch (Art. 21)

- Die betroffene Person hat das Recht, unter bestimmten Umständen gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen.

06

DSGVO

Datenschutzvorfall

DSGVO

Data Breach / Datenschutzverletzung

Definition

- Datenschutzverletzung: Verletzung des Schutzes personenbezogener Daten.
- Identifizierte Datenschutzverletzungen sind unverzüglich weiterzuleiten!
- Meldung innerhalb von 72 Stunden an die Datenschutzbehörde, wenn ein Risiko für betroffene Person besteht.

Beispiele für Datenschutzverletzungen

- Ungewünschte Veröffentlichung von personenbezogenen Daten im Internet
- Versehentliches Versenden von personenbezogenen Daten an falsche Empfänger
- Verlust oder Diebstahl von Datenträgern
- Weitergabe personenbezogener Daten an unbefugte Dritte

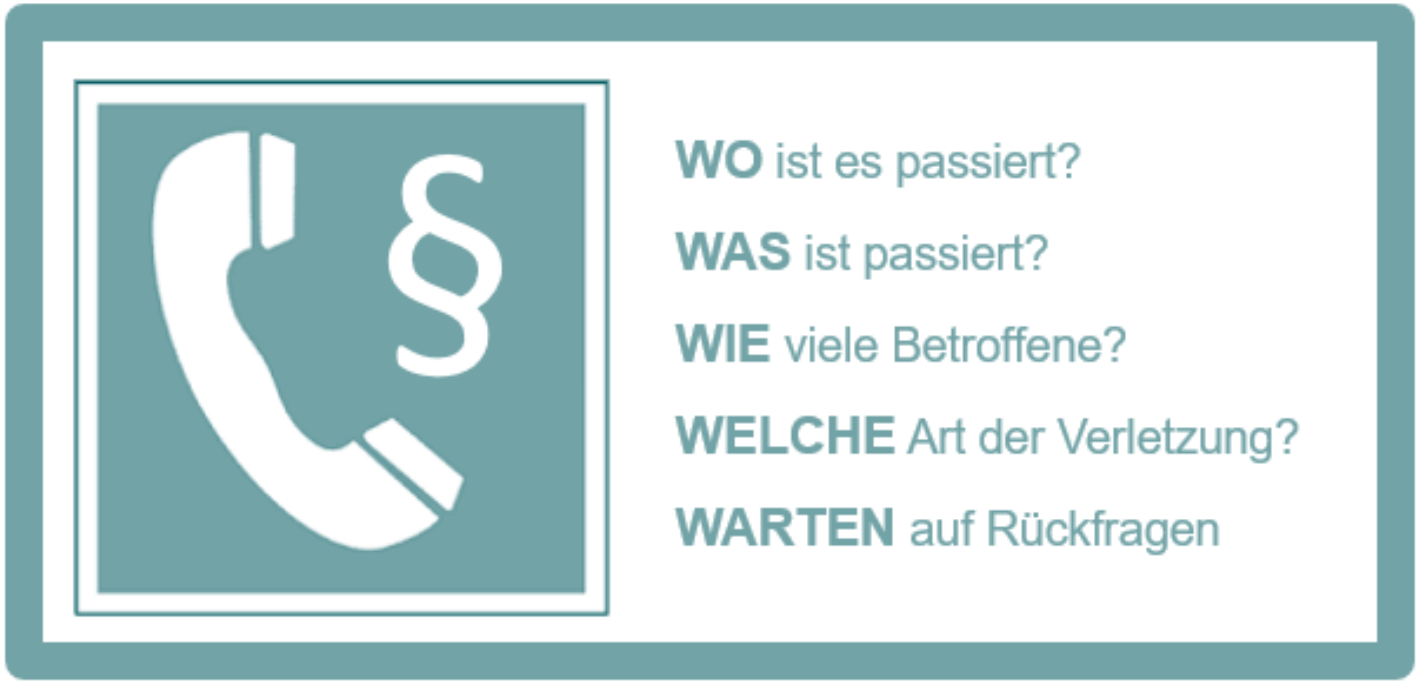
DSGVO

Data Breach – Nützliche Links

- https://haveibeenpwned.com/ - waren meine Daten Teil eines Data Breaches
- https://www.watchlist-internet.at/ - Auflistung der Jüngsten Fishing Attacken

Datenschutzvorfälle

Welche Informationen sind zu melden?



DSGVO

Ansprechpartner bei Datenschutzangelegenheiten

Datenschutz-Koordinator

- Interne Ansprechperson für Datenschutz
- Anlaufstelle für Betroffenenrechte und Datenpannen
- Regelmäßige Aktualisierung und Verbesserung des Datenschutz-Managementsystems


Dr. Klaus Sapetschnig


+43 3842/402-7002


dsb@unileoben.ac.at

Datenschutzbeauftragter

- Unterrichtet und berät zum Thema Datenschutz
- Überwachung der Einhaltung Datenschutzvorschriften
- Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter
- Zentrale Anlaufstelle für die Datenschutzbehörde


Fa. x-tention Informationstrechnologie GmbH


Service.Datenschutz@x-tention.at

07

Datengeheimnis

Datengeheimnis

§ 6 DSG

DSG definiert das Datengeheimnis in § 6

- Alle Arbeitnehmer sind dazu verpflichtet, sämtliche personenbezogenen Daten, die ihnen auf Grund ihrer berufsmäßigen Beschäftigung zugänglich geworden sind, geheim zu halten.
- Datengeheimnis endet nicht mit dem Dienstverhältnis, sondern gilt darüber hinaus.

08

Lessons Learned

Was gibt’s zu merken?

1. Datenschutz ist wichtig
2. Daten haben einen Wert
3. Datenschutzvorfälle melden
4. Datenschutz schützt mich und dich vor schlimmen Folgen
5. Nützliche Links:
   - https://haveibeenpwned.com/
   - https://www.watchlist-internet.at/
6. Nächster Schulungstermin am 26.04.2022 09:30-10:30

Zeit für Fragen ☺

Vielen Dank

x-tention Informationstechnologie GmbH
Römerstraße 80a, 4600 Wels, Austria
Service.Datenschutz@x-tention.com

IT with care.