**Einführung in die rechtlichen Aspekte der IT-Sicherheit – Der Datenschutz**

Wozu brauchen wir Datenschutz?

* Datenskandale wie Abhören durch technische Neuheiten wie Alexa, Siri, etc.
* E-Commerce (Amazon)

Informationelle Selbstbestimmung

* 1983 Volkszählungsurteil: Jeder muss vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten geschützt werden
* Allgemeines Persönlichkeitsrecht: Art. 2 Abs. 1 GG 🡪 Art 1 GG
* §8 Europäische Menschenrechtskonvention: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.“
* Einschränkungen sind nur aufgrund einer gesetzlichen Grundlage und mit überwiegendem Allgemeininteresse zulässig (BVerfGE Art. 2)

Datenschutzgrundverordnung

* Europäische Regelung die seit 25. Mai 2018 gilt
* Subsidiaritätsprinzip 🡪 Zuerst gilt DSGVO dann Bundesdatenschutzgesetz dann Landesdatenschutzgesetz (Spezifizierung der DSGVO)
* Informationsfreiheit und freie Meinungsäußerung mussten bei Einführung mit DSGVO im Einklang sein
* Anwendung (nach Art. 3 DSGVO):
  + Niederlassungsprinzip: Niederlassung oder Tätigkeit einer natürlichen Person des Auftragsverarbeiters innerhalb der Union
  + Marktortprinzip: Sobald sich der Betroffene innerhalb der Union befindet

Verbot mit Erlaubnisvorbehalt

* Eindrückliche Erlaubnis des Betroffenen damit die Handlung der Datenverarbeitung rechtmäßig ist🡪 Aktiv werden des Betroffenen 🡪 Umgehung nur auf Grundlage von Gesetzen
* Einwilligung … (Art. 7 DSGVO) 🡪 Verantwortlicher hat Beweispflicht
  + muss von anderen Sachverhalten abgegrenzt und verständlich geschrieben werden
  + kann jederzeit wiederrufen werden
  + muss freiwillig und zweckgebunden sein
  + ist erst ab 16 Jahren zulässig (Art. 8 DSGVO)

Grundsätze

* Rechtmäßigkeit der Daten
  + Erhebung personenbezogener Daten auf rechtmäßige Weise 🡪 Einwilligung des Betroffenen oder aufgrund eines Gesetzes
  + Verarbeitung nach Treu und Glauben 🡪 Datenverarbeitung nach bestem Wissen und Gewissen
  + Transparenz 🡪 Betroffene weiß, welche Daten wofür und in welcher Form erhoben wurde
* Datensparsamkeit/Datenminimierung
  + Menge der erhobenen Daten sollte so klein wie möglich sein
  + Speicherung nur solange Sie zweckgebunden sind
  + Ausnahme (Art. 89 DSGVO): Datenspeicherung für öffentliche Archivzwecke und wissenschaftliche und historische Forschungszwecke
* Zweckbindung
  + Daten dürfen lediglich für den vorgesehenen **Zweck** verwendet werden.
  + Der Zweck muss bekannt, konkret und dem betroffenen mitgeteilt werden
  + Der Staat und Unternehmen in Ausnahmefällen können die Zweckbindung aufheben
* Datensicherheit
  + Die Schutzziele der Datensicherheit sind Integrität, Belastbarkeit, Verfügbarkeit und Vertraulichkeit
  + Art. 32 DSGVO gibt Anhaltspunkte, die im BDSG und dem Referentenentwurf des Bundesministeriums des Innern für Datenschutz vertieft werden
  + Personenbezogene Daten können in verschiedene Schutzklassen nach dem Standard des BSI 100-2 eingeteilt werden

Betroffenenrechte nach Art. 12-23 DSGVO:



Europäischer Datenschutzausschuss

* Setzt sich zusammen aus den einzelnen **Bundesbeauftragten** der Länder der EU.
* kann Beschlüsse fassen, die für alle EU-Mitgliedsstaaten rechtlich bindend sind
* **Erlässt Leitlinien, Empfehlungen** oder **Verfahren** um die DSGVO einzuhalten

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

* Zuständig für alle öffentlichen Stellen des Bundes und Telekommunikations- oder Postdienstunternehmen
* Ist in Ausschüssen des Bundes aktiv
* Berät, Überwacht und Kontrolliert die Einhaltung der DSGVO

Landesbeauftragte für den Datenschutz und die Informationsfreiheit

* Zuständig für öffentlichen Stellen und nicht-öffentlichen Stellen mit **Ausnahme** von Telekommunikations- und Postdienstunternehmen
* Muss Beschwerden von Bürgern über Behörden oder Unternehmen nachgehen
* Berät, Überwacht und Kontrolliert die Einhaltung der DSGVO im jeweiligen Bundesland

Rechtsdurchsetzung

* Bei schweren Verstößen, **20** Mio Euro oder **4%** des Jahresumsatzes des vorherigen Geschäftsjahres (maximal)
* Bei sonstigen Verstößen, **10 Mio** Euro oder **2%** des Jahresumsatzes des vorherigen Geschäftsjahres (maximal)