DSGVO-konforme Software-Entwicklung

Pflichten und Haftungsrisiken für Entwickler

Höhne
In der Maur
& Partner

Rechtsanwälte

Mag. Markus Dörfler
Rechtsanwalt
27.2.2019

Markus Dörfler

1999 - 2005	Synaptic Networks
2006	Mag. iur. Universität Linz
2006 - 2007	Universitätslehrgang für Informationsrecht und Rechtsinformation, Universität Wien
2007	Master of Laws (LL.M.)
2012 - 2016	selbstständiger Rechtsanwalt - in Kooperation mit Höhne, In der Maur & Partner
2016	Partner bei Höhne, In der Maur & Partner Rechtsanwälte

Das „Warum“: die DSGVO

Die Datenschutzgrundverordnung:

Besteht Sorge?

Nein*

Rechtsgrundlage

- Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- In Kraft seit 24.5.2016 (anzuwenden seit 25.5.2018)
- Nationale Gesetze (DSG, …)

DSGVO

- Sanktion:
  - „wirksam, verhältnismäßig und abschreckend“
- Geldbuße:
  - bis zu EUR 10 Mio (oder 2% des weltweiten Jahresumsatzes)
  - bis zu EUR 20 Mio (oder 4% des weltweiten Jahresumsatzes)
  - zuständig: Aufsichtsbehörde

Das „Was“: Personenbezogene Daten

- „personenbezogene Daten“ (Art 4 Z 1 DSGVO) alle Informationen, die sich
  - direkt oder indirekt
  - auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;
- Keine juristischen Personen
- Keine Daten von verstorbenen Personen
  - Achtung: Öffnungsklausel

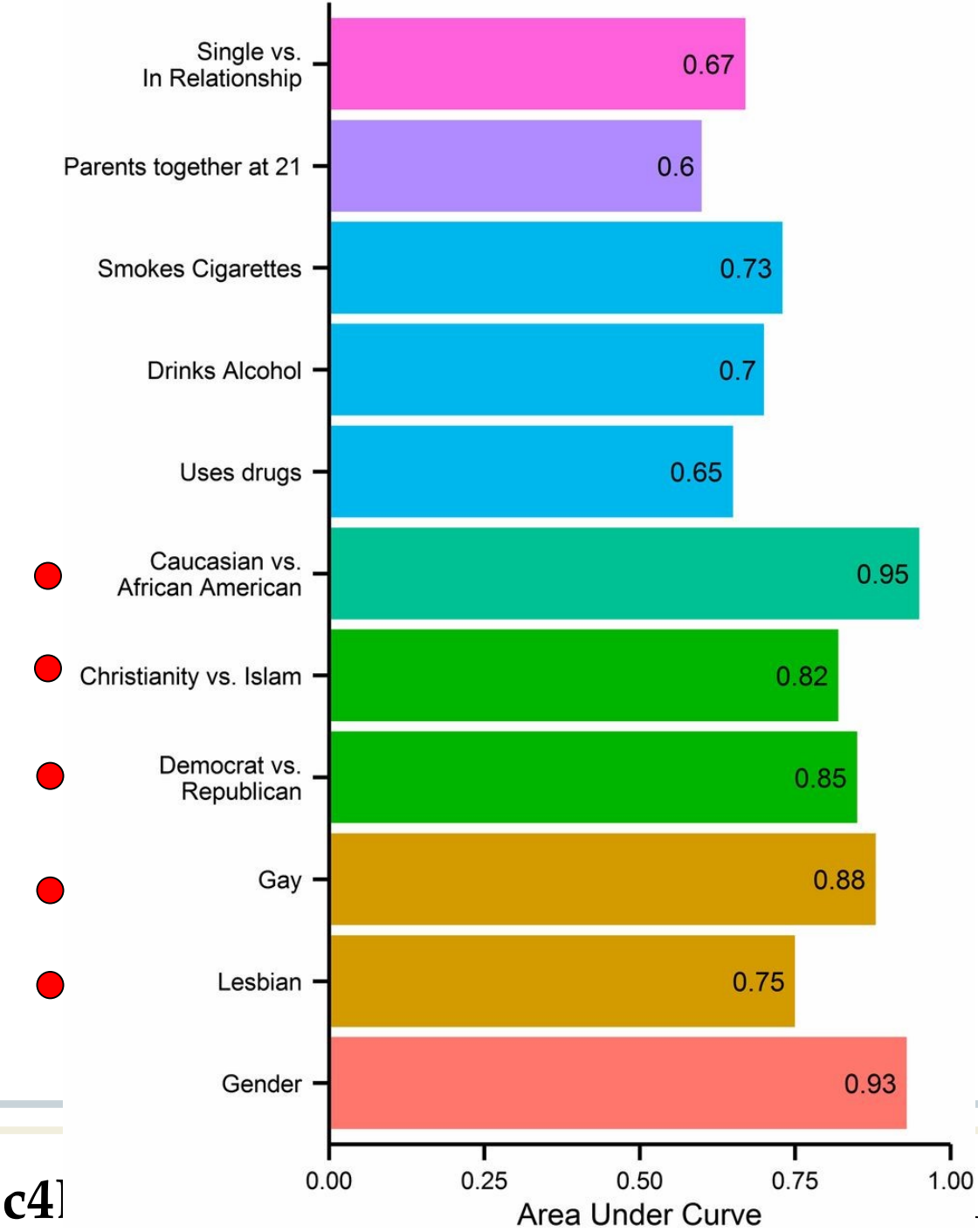
Personenbezogene Daten

- Als identifizierbar wird eine natürliche Person angesehen, die insbesondere mittels Zuordnung
  - zu einer Kennung wie einem Namen,
  - zu einer Kennnummer,
  - zu Standortdaten,
  - zu einer Online-Kennung oder
  - zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind…. identifiziert werden kann

Personenbezogene Daten

- Die Unterscheidung „identifizierbar vs indentifiziert“ ist irrelevant
- Wann ist eine Person identifizierbar:
  - Berücksichtigung aller Mittel
  - Außer: eine Identifizierung ist praktisch nicht durchführbar (EuGH vom 12.5.2016 – C-582/14)

- Studie:
  - “Private traits and attributes
  - are predictable from digital records of human behavior” (PNAS 2013 April, 110 (15) 5802-5805)
  - 58,466 Freiwillige
  - ~170 „Likes“



Das „Wie“: Sicherheit der Verarbeitung

– Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein (Art 32 DSGVO):

Sicherheit der Verarbeitung

- Pseudonymisierung und Verschlüsselung
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherstellen
- Widerherstellbarkeit
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Softwareentwicklung

- Dürfen Daten aus dem Produktivsystem für Testzwecke verwendet werden?
- Betroffenenrechte technisch Umsetzen – Auskunft, Richtigstellung, Datenportabilität, Löschung und Einschränkung der Verarbeitung
- Wie sieht DSGVO-konformes Logging aus?

Softwareentwicklung

- Wie sind Backups zu schützen?
- Was bedeutet Privacy by Design & by Default?
- Passwortauthentifizierung – DOs & DON‘Ts
- Haftung des Entwicklers nach der DSGVO?

Danke für die Aufmerksamkeit

Höhne
In der Maur
& Partner

Rechtsanwälte

Markus Dörfler
E: markus.doerfler@h-i-p.at
T: 01/521 75-41
www.h-i-p.at
datenschutz-recht.at