



Daten sind das neue Gold vs Daten(schutz)recht

ncp.ip

29. November 2023



Wie Sie dennoch zum Goldschürfer
werden.

ncp.ip

29. November 2023



Worum geht es denn
rechtlich eigentlich?!



Was macht Ihr den ganzen Tag...

...mit personenbezogenen Daten?

= Datenschutz-Grundverordnung (DSGVO) ...

... aber es kommt auch noch „EU-Buchstabensuppe“



Jede juristische Präsentation beginnt
(i) mit einem Witz, oder
(ii) mit Angst

(Witze sind leider aus)



Warum DSGVO-Compliance?

- Bisher „stiefmütterlich“ ... nunmehr Sanktionen:
 - Geldbußen bis EUR 20 Mio oder 4% Welt-Jahres-Konzern-Umsatzes (je was höher)
 - Persönliche Haftung der Täter & Management? (§ 9 VStG bzw § 30 Abs 3 DSG vs § 11 DSG?)
 - Strafbemessungsgründe in DSGVO



Warum DSGVO-Compliance?

- TikTok 345 Millionen Euro (irische DPC)
- Meta: 1,2 Milliarden Euro



Warum DSGVO-Compliance?

- Schadenersatz (bzw Amtshaftung):
 - materieller oder immaterieller Schadenersatz mit Beweislastumkehr
 - „Datenschutz-Schutzverbände“ → NOYB
 - Immaterieller Schadenersatz als „dogmatischer Fremdkörper im ö Recht?!“
 - keine “Erheblichkeitsschwelle“ (vs „Schmerztage“), aber auch nicht „automatisch“ (EuGH C-300/21)
 - Persönliche Haftung der Täter & Management?!



Worum geht es denn eigentlich
inhaltlich?



Datenverarbeitungsverbot mit Erlaubnisvorbehalt

Verbot *personenbezogene Daten* zu
verarbeiten, außer ein gesetzlich normierter
Erlaubnisgrund „*rechtfertigt*“ die
Datenverarbeitung.

→ Viele Erlaubnisgründe ...



Personenbezogene Daten ...

... sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. [...]



Personenbezogene Daten

Identifizierbar ist eine Person, die direkt oder indirekt, insb mittels Zuordnung zu einer Kennung wie Namen, (Online-)Kennnummer, Standortdaten, 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.



Pseudonyme vs Anonyme Daten

Personenbezogene Daten

Pseudonyme Daten

Anonyme Daten



Verarbeitung

jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten ...

→ Nichtautomatisiert in Dateisystem
(strukturierte Sammlung: zB Karteikartensystem)



Verarbeitung

... 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 oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.



Datenverarbeitungsverbot mit Erlaubnisvorbehalt

Was machst Du Datenschutzrelevantes?

Gegenfragen:

- wer? (nicht Mitarbeiter sondern „Entität“)
- welche Daten?
- aus welchem (Rechts)Grund?
- wie lange?
- wo bzw von wem und wie sicher?



Worum geht es denn eigentlich
im Datenschutz(recht)?!



„Zehn Gebote“

- Rechtmäßigkeit
- Treu und Glauben
- Transparenz (= „Informationspflicht“)
- Zweckbindung (mit möglichen Ausnahmen)
- Datenminimierung (= „Notwendigkeitsbegrenzung“)
- Richtigkeit (und Aktualität)
- Speicher(dauer)begrenzung
- Integrität (= „IT-Sicherheit“)
- Vertraulichkeit (= „Daten-Sicherheit“)
- Rechenschaftspflicht = („Verfahrensverzeichnis“)



Rechtmäßigkeit

- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung *erforderlich*, der der Verantwortliche unterliegt.

z.B. Personal-, Buchhaltungs-, ...-verwaltung



Rechtmäßigkeit

- Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

z.B. Nutzer-, Lieferanten-, ...-verwaltung



Rechtmäßigkeit

- Betroffener hat Einwilligung zu Zweck und Daten gegeben.
- ...

→ „Machen Sie sich keine Sorgen. Wir werden (zu fast Allem) einen rechtmäßigen Verarbeitungsgrund finden.“

ABER ZU UNTERSCHIEDEN: ...



Rechtmäßigkeit durch Einwilligung

- Bei Einwilligungen bei einem Angebot von Diensten der Informationsgesellschaft (verallgemeinerungsfähig?)
 - das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das 14te [in Österreich! sonst 16te, oder national 13te bis 16te] Lebensjahr vollendet hat.
 - Hat das Kind noch nicht das obige Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.



Rechtmäßigkeit durch Einwilligung

- Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.
- Dies lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.



Rechtmäßigkeit durch Einwilligung

- Verantwortliche muss nachweisen können, dass Betroffener in die Verarbeitung eingewilligt hat.
- Bei schriftlicher Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann **nicht verbindlich**, wenn sie einen Verstoß gegen diese Verordnung darstellen.



Rechtmäßigkeit durch Einwilligung

- Recht, die Einwilligung jederzeit zu widerrufen, wodurch aber die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird.
- Informationspflicht über Widerrufsrecht. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.



„Zehn Gebote“

- Rechtmäßigkeit (uE „datenschutzrechtliche iwS“)
- Treu und Glauben (uE „Fairness“)
- Transparenz 



Informationspflichten

- Namen und die Kontaktdaten des Verantwortlichen;
- Kontaktdaten (!) des Datenschutzbeauftragten;
- Zwecke, für welche die Daten verarbeitet werden;
 - explizit wenn, Details über Profiling;
- die Rechtsgrundlage für die Verarbeitung (→ Art 6);
 - explizit wenn, welche berechtigten Interessen;
- [die Kategorien personenbezogener Daten];
- [die (öffentliche) Quellen der Daten];
- Empfänger oder Kategorien von Empfängern;
- Garantien für Internationalen Datentransfer und Zugang;



Informationspflichten

- Speicherdauer oder - falls nicht möglich - Kriterien für die Festlegung der Speicherdauer;
- über Betroffenenrechte (Detailgrad?);
 - Sonderinfo über Widerspruch bei berechtigten Interessen;
- über Widerrufsrecht der Einwilligung;
- Beschwerderecht bei einer (?) Aufsichtsbehörde.

→ „Form“ und Zeitpunkt der Information?!



„Zehn Gebote“

- Rechtmäßigkeit (uE „datenschutzrechtliche iwS“)
- Treu und Glauben (uE „Fairness“)
- Transparenz 
- Zweckbindung (uE „Zweckvereinbarkeit“)
- Datenminimierung 
- Richtigkeit
- Speicherbegrenzung (uE „Speicherdauerbegrenzung“) 



Die „Kapperl-Frage“



Wem ist es verboten? Rollen!

- „Haushaltsausnahme“: Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten
- Rollenverteilung:
 - Verantwortlicher
 - Auftragsverarbeiter
 - Betroffener
 - Empfänger
 - Dritter



**„für Verarbeitung
Verantwortlicher“**

der allein oder gemeinsam mit
anderen über die
Zwecke und Mittel der
Verarbeitung von
personenbezogenen Daten
entscheidet

„Auftragsverarbeiter“

die personenbezogene Daten im
Auftrag des für die Verarbeitung
Verantwortlichen verarbeitet

„Betroffene Person“

Person, deren Daten verwendet werden



Auftragsverarbeiter

Verantwortlicher

„Kleines“ Verz der Verarb (Art 30/2)

TOMs
(bei sich)

Rechtmäßigkeit
(auch Info und BetroffenR)

AV- bzw JC-Verträge
(Art 28 bzw Art 26)

Verz der Verarb
(Art 30/1)

TOMs
(ganze Kette)



Internationaler Datentransfer



DSB am 22.12.2021:

„Da für die gegenständliche Datenübermittlung [des Websitebetreibers] an [Google] (in den USA) kein angemessenes Schutzniveau durch ein Instrument [der DSGVO] gewährleistet wurde, liegt eine Verletzung [der] DSGVO vor.“ [Seite 39]



Zugriff staatlicher Behörden

- US (aber auch Indien, China, ...) Gesetze ermöglichen im Verhältnis zur EU leichteren Zugriff auf Daten beim „IT-Providern“
- US Cloud Act verpflichtet „IT-Provider“, Zugriff auch auf Daten außerhalb der US zu gewähren
- Verhinderung durch „(technical) supplementary measures“!



... seit 10.07.2023



**DATA PRIVACY
FRAMEWORK
PROGRAM**

Search

Home Self-Certify Data Privacy Framework List Audiences About

ACTIVE INACTIVE

Search

Advanced Search

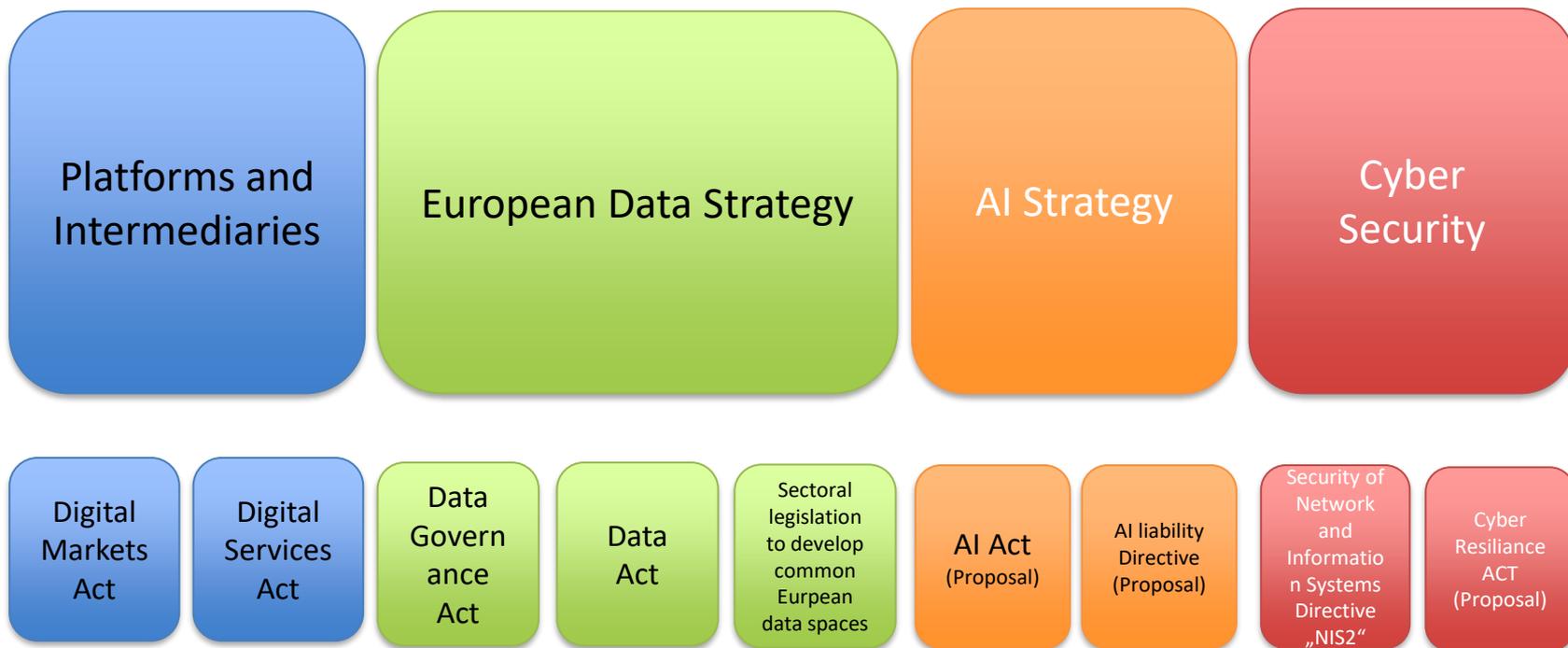
23andMe, Inc. South San Francisco, California Active	Framework EU-U.S. Data Privacy Framework Swiss-U.S. Data Privacy Framework UK Extension to the EU-U.S. Data Privacy Framework	Covered Data Non-HR Questions or Complaints
247Digitize LLC Chicago, Illinois Active Covered Entities (1)	Framework EU-U.S. Data Privacy Framework Swiss-U.S. Data Privacy Framework UK Extension to the EU-U.S. Data Privacy Framework	Covered Data Non-HR Questions or Complaints



Daten(schutz)recht



Ausgewählte Gesetzes-Vorhaben auf EU-Ebene





Vertragsmuster

Home | Vertragsmuster (IPAG) | Vertragsmuster | Software Entwicklung und Datennutzung

Software Entwicklung und Datennutzung



Geheimhaltungsvereinbarungen



FH und Uni-Ausgründungen



Material Transfer Agreements



Software Entwicklung und Datennutzung



IP-Transfer



Forschung und Entwicklung

Vertragsmuster Software Entwicklung und Datennutzung

< Zurück zu Vertragsmuster

Bitte beachten Sie die [Nutzungsbestimmungen](#), vor dem Herunterladen von hier angebotenen Inhalten.

Software-Entwicklung und Datennutzung

- > Software-/IT-Forschungs- und Entwicklungsauftrag
- > Software-Evaluierungs-Lizenzvertrag
- > Lange Klausel zur Streitbeilegung
- > Datennutzung Kopfdokument
- > Vereinbarung Nutzung Anonymer Daten
- > Vereinbarung Nutzung Daten
- > Vereinbarung Nutzung sensibler Daten

> Zum Seitenanfang



GEISTWERT
RECHTSANWÄLTE LAWYERS AVVOCATI

MMag.

JULIANE MESSNER
Partner

tel +43 1 585 03 03-20
fax +43 1 585 03 03-99

Linke Wienzeile 4
1060 Wien · Vienna · Austria

juliane.messner@geistwert.at
www.geistwert.at