HÄRTING

DIE NEUSTEN RECHTLICHEN ENTWICKLUNGEN RUND UM CLOUD

RA lic. iur. Nicole Beranek Zanon, Execl. MBA HSG, CIPP/E

Security Roundtable vom 04.05.2023

AGENDA

- Trans-Atlantic Data Privacy Framework
- Datentransfers nach nDSG
- Meldepflichten nach nDSG + ISG
- AI is here, what a surprise!
- Privacy by Design

1. Trans-Atlantic Data Privacy Framework

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK - **INHALT**

- Free and safely data between the EU and participating U.S. companies
- A new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security;
- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- A new two-tier redress system to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a Data Protection Review Court
- Strong obligations for companies processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- Specific monitoring and review mechanisms

https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK - **KRITIK**

- **EU Parlament**
  https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf
  - the indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to confidentiality of communications provided for in Article 7
  - not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47
  - Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the US still does not have a federal data protection law
    → Concludes that the EU-US Data Privacy Framework fails to create actual equivalence in the level of protection

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK - **KRITIK**

- **Max Schrems & NGO «NOYB»** («none of your business»)
  https://noyb.eu/sites/default/files/2022-05/open_letter_EU-US_agreement.pdf
  - it is not the result of material changes to U.S. law in response to the CJEU's judgement
  - the US has rejected any material protections for non-US persons and is continuing to discriminate against non-US persons by refusing baseline protections, such as judicial approval of individual surveillance measures.
  - **claims**:
    - Applying a correct proportionality test on US surveillance law under Article 8 CFR
    - Creating meaningful judicial redress under Article 47 CFR
    - The need to update commercial privacy protections

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK – **TO-DO`S**

Folgendes ist notwendig:

- DPA + TOM
- Weiter bleibt der Cloud Act bestehen

Fällt weg bis Schrems III:

- SCC -> wird ev. Standard für DPA?
- DPIA + TIA

Schweiz folgt der EU d.h. es wird ein äquivalentes Agreement zwischen USA und CH geben

3. Datentransfers nach nDSG

DATENTRANSFERS NACH NDSG

DSG	nDSG
(Bisher) Art. 6 Abs. 1 Grundsätze [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.	**(Neu) Art. 16 nDSG Grundsätze** 1 Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

DSG	nDSG
(Bisher) Art. 6 Abs. 2 DSG [2] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b. die betroffene Person im Einzelfall eingewilligt hat; c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt; d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.	**(Neu) Art. 16 nDSG Grundsätze** 2 Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch: a. einen völkerrechtlichen Vertrag; b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden; c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat; d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden. 3 Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen.

DSG	nDSG
n/a	**(Neu) Art. 17 Ausnahmen** 1 Abweichend von Artikel 16 Absätze 1 und 2 dürfen in den folgenden Fällen Personendaten ins Ausland bekanntgegeben werden: a. Die betroffene Person hat ausdrücklich in die Bekanntgabe eingewilligt. b. Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags: 1. zwischen dem Verantwortlichen und der betroffenen Person; oder 2. zwischen dem Verantwortlichen und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person. c. Die Bekanntgabe ist notwendig für: 1. die Wahrung eines überwiegenden öffentlichen Interesses; oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde. d. Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen. e. Die betroffene Person hat die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt. f. Die Daten stammen aus einem gesetzlich vorgesehenen Register, das öffentlich oder Personen mit einem schutzwürdigen Interesse zugänglich ist, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. 2 Der Verantwortliche oder der Auftragsbearbeiter informiert den EDÖB auf Anfrage über die Bekanntgabe von Personendaten nach Absatz 1 Buchstaben b Ziffer 2, c und d.

3. Meldepflichten nDSG + ISG

MELDEPFLICHTEN NACH NDSG UND DSV

- Verletzungen der Sicherheit der Daten müssen beim EDÖB gemeldet werden
  - *Meldepflicht von Risikoabwägung abhängig*

  Formel: Je mehr Personendaten betroffen sind, je sensibler die Datenkategorien, je leichter der Rückschluss von den Daten auf identifizierbare Personen und je höher die Eintrittswahrscheinlichkeit (insb. beim unbefugten Zugriff durch Dritte), desto höher wird das Risiko für eine Verletzung der Datensicherheit einzustufen sein.
  - *Andere Bewertung als bei DSGVO*

- Keine konkrete Meldefrist
  - *„so rasch als möglich“*
  - *Anders bei DSGVO*
  - *Keine Busse, wenn Frist nicht eingehalten ist (anders DSGVO)*

- U.U. ist die betroffene Person selbst zu informieren
  - *Information ist zum Schutz der betroffenen Person erforderlich*
  - *Information der betroffenen Person wird vom EDÖB verlangt*

MELDEPFLICHTEN NACH ISG

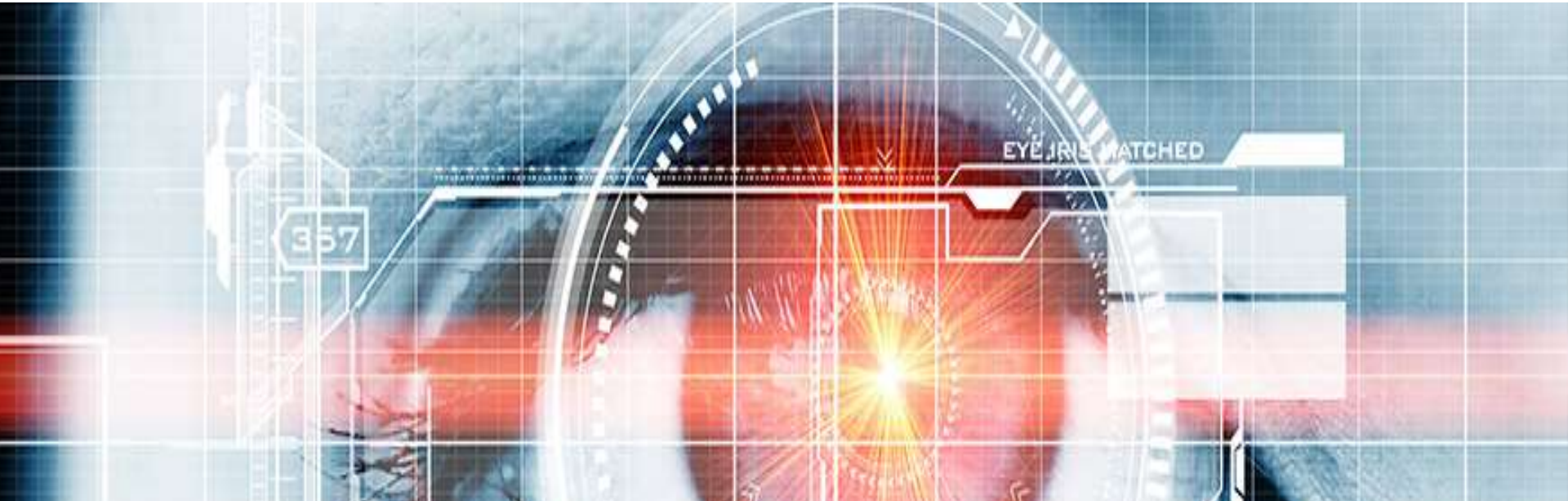
- Meldepflicht bei Cyberangriffen für Betreiber kritischer Infrastrukturen an das Nationale Zentrum für Cybersicherheit (NCSC)
  - *Meldepflicht auf bestimmte Sektoren begrenzt (sehr breit)*
  - *Meldepflicht besteht nur unter gewissen Voraussetzungen*
    - Insb. nur Cyberangriffe, die ein erhebliches Schadenspotenzial aufweisen (namentlich nicht menschliches Fehlverhalten)

- Meldefrist: Innerhalb von 24 h nach Entdeckung des Angriffs
- Durchsetzung:
  - *Positive Anreize:*
    - NCSC bietet „Erste Hilfe“ nach Meldung an
  - *Sanktionen:*
    - Bussen i.H.v. bis zu CHF 100‘000 möglich
    - Persönliche Verantwortlichkeit

MELDEPFLICHTEN – WAS IST ZU TUN?

- **Sicherstellung der internen Kommunikationsprozesse**
  Cyber Incident – Crisis Management Organisation

4. AI IS EVERYWHERE, WHAT A SURPRISE!



AI – REGULIERUNG IN DER EU

In Arbeit: Aritificial Intelligence Act

- Harmonisierung der Vorschriften zu KI-Technologien
- Einteilung von KI-Technologien in Kategorien
  - *Klassifizierung nach bestehendem Risiko*
  - *Verbot von Technologien mit nicht akzeptablen Risiko*

- Richtet sich primär an Anbieter von KI-Technologien
  - *Unter bestimmten Voraussetzungen auch andere Parteien*

- Bussen bei Verstössen gegen auferlegte Pflichten
- Schaffung eines europäischen Ausschusses für KI

- in Kraft jedenfalls nicht vor 2025

AI-SYSTEM

Annex 1 AI Act draft

a) Maschine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide varity of methods including deep learning.

b) Logic- and knowledge-based approaches, including knowledge representaton, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

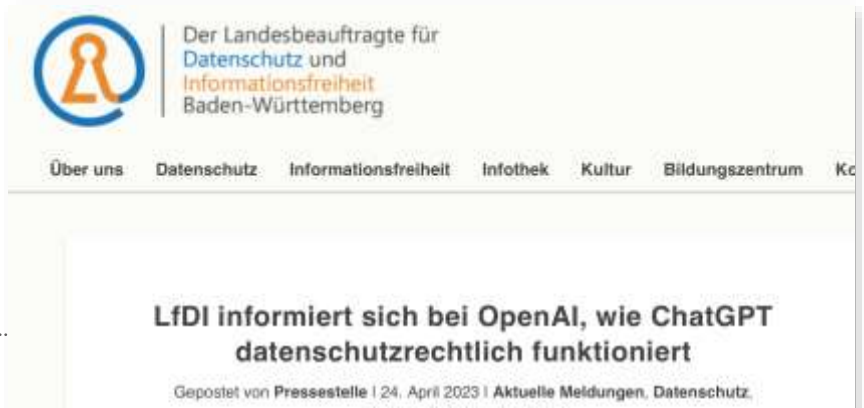
c) Statistical approaches, Bayesian estimation, search and optimization methods

VERBOTENE BEREICHE FÜR AI-SYSTEME

- Biometric Identification and categorisatzion of natural persons
- Management and operation of critical infrastructure
- Education and vocational training institutions
- Employement, workers management access to self-employment
- Access to and enjoyment of essential private services and public services and benefits
- Law enforcement
- Migration, asylum and boarder control management
- Administration of justices and democratic processes

AI IS HERE, WHAT A SURPRISE

- **Chat GTP** in Italien verboten
- EDÖB hat am 4.4.2023 die Prüfung angekündigt https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#238887506
- EDPB bildet Task Force https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en
- Andere Datenschutzbehörde die Zulässigkeit



DATENSCHUTZRECHTLICHE FRAGEN

1. Welche Rollenbeziehung besteht zwischen openAI und dem (Business-)Anwender?
   → openAI: AV! Welche Rolle spielt das Training-Opt-In? (seit 3/2023)
2. Welche Rechtsgrundlage ist eigentlich anwendbar?
   → Wie können Einwilligungserklärungen hinreichend transparent formuliert sein?
   → Was ist mit Drittstaatentransfers?
3. Werden die Grundprinzipien der DSGVO / DSG eingehalten? Erforderlichkeit? Datenminimierung? Etc.
4. Insbesondere: Genügt openAI den Transparenzanforderungen? Und wie informiere ich meine Beschäftigten? Meine Kunden? Dritte?

BEYOND DATENSCHUTZ – VOLLE VERANTWORTLICHKEIT FÜR INHALTE

- Unternehmen ist für KI-generierte Inhalt verantwortlich.
- Haftung für
  - *Urheberrechtsverletzungen*
  - *Wettbewerbsverstöße*
  - *falschen Rat*
  - *Persönlichkeitsrechtsverletzungen*

WENN CHATGPT DENNOCH EINGESETZT WERDEN SOLL …

Nutzungsrichtlinie verabschieden! Mögliche Regelungsinhalte:

- Zulässige Einsatzzwecke klar definieren
- insbesondere Beschränkung auf dienstliche Zwecke (Mitarbeiterexzess?)
- Einbeziehung der Nutzungsbedingungen von openAI
- Inhalts der Prompts definieren; keine pbD, keine Betriebs- u. Geschäftsgeheimnisse, Rechte Dritter?
- Keine Weiterverwendung der Ergebnisse ohne Prüfung
- …

QUELLEN

- https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf
- https://noyb.eu/sites/default/files/2022-05/open_letter_EU-US_agreement.pdf
- https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/
- https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf

TEAM

Monika Abt
Substitutin

Cédric Bamert
Student

Nicole Beranek Zanon
Partnerin | Notarin | Exec. MBA HSG

Olivia Boccali
Juristin

Laetitia Scyboz
Studentin

Christine Grass
Zentrale

Dominic Grunder
Student

Anastasia Käslin
Studentin

Andri Lehmann
Student

Paula Zimmermann
Partnerin | Magister der Sozial- und Wirtschaftswissenschaften (M.A.)

HÄRTING

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1
6300 Zug
Switzerland
Tel. +41 41 710 28 50
www. haerting.ch
beranek@haerting.ch