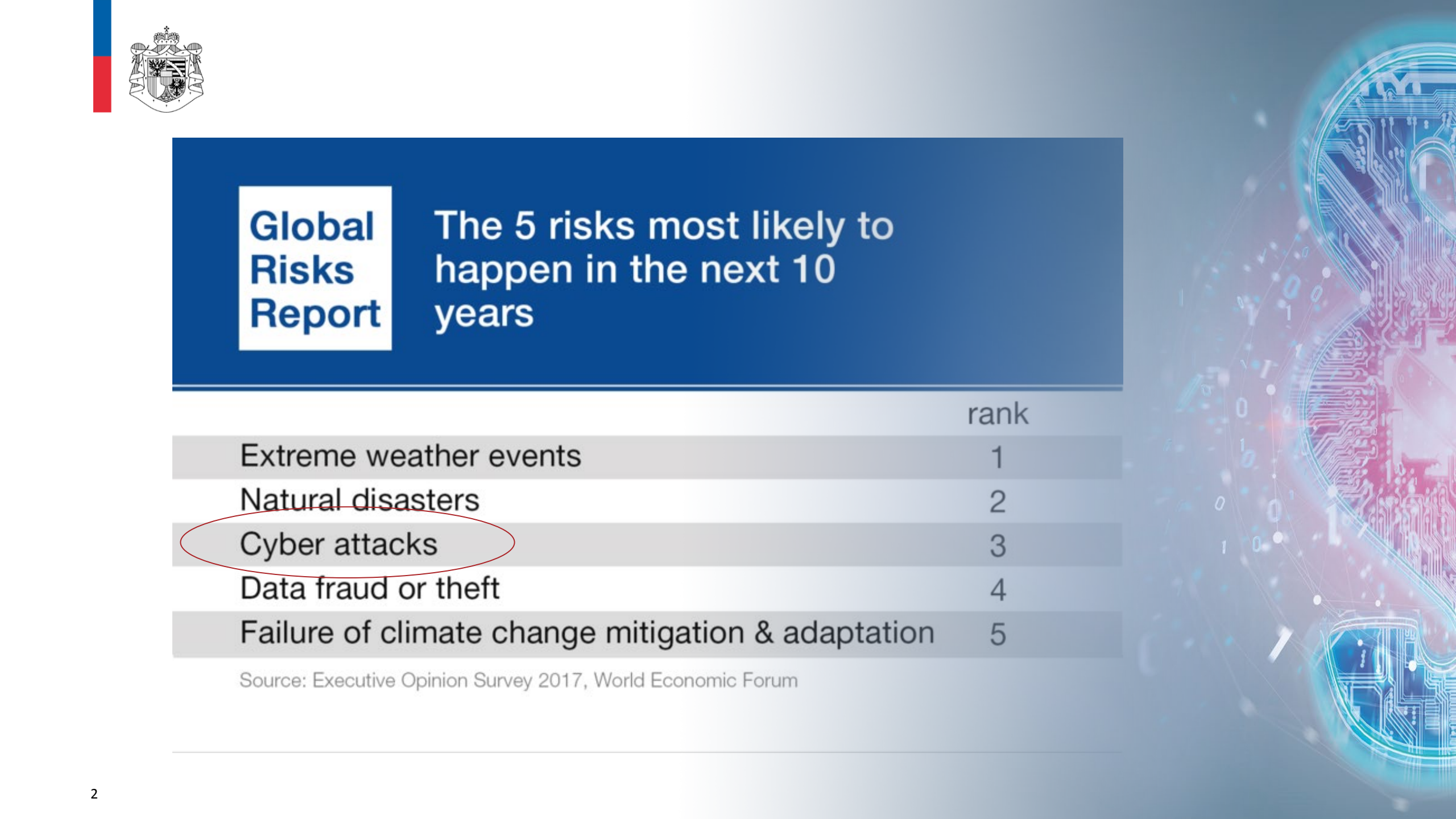
Cybersecurity und Datenschutz

«Cyber Security»

Bedrohung und Risiken im Unternehmen

Vortragsveranstaltung am 24.9.2019

Dr. Marie-Louise Gächter
Leiterin Datenschutzstelle



	rank
Extreme weather events	1
Natural disasters	2
Cyber attacks	3
Data fraud or theft	4
Failure of climate change mitigation & adaptation	5

Source: Executive Opinion Survey 2017, World Economic Forum

Cybersecurity in Zahlen

- alle 39 Sekunden findet ein Cyberangriff statt
- seit 2013 wurden jeden Tag 3,8 Millionen Datensätze gestohlen
- die durchschnittlichen Kosten eines Datenverstosses werden bis 2020 auf über 150 Millionen US-Dollar geschätzt
- die Wahrscheinlichkeit eines Cyberangriffs liegt bei 1 zu 4, bei einem Wohnungseinbruch bei 1 zu 345

Cybersecurity in den Medien

COMPUTERWELT & transform! IDG

THEMEN | TOP 1001 – IT ANBIETER | EVENTS | SOFTWARE | IT-JOBS | PRINTA

NEWS TICKER [19. September 2019] Health Hub Vienna geht in die vierte Runde ▸ NEWS

28. August 2019 pte

Cybercrime kostet britische KMUs 8,8 Mrd. Pfund

Allein in diesem Jahr könnten aktuellen Schätzungen nach rund 57.000 Unternehmen eingehen.

IT&Production ONLINE
Das Industrie 4.0-Magazin für erfolgreiche Produktion

Downloadbereich

NEWS | FACHBEITRÄGE | ANBIETER & PRODUKTE | E

Security

Kosten von Cyberattacken liegen im Schnitt bei 13Mio.US$

Mehr Angriffe und höhere Kosten: Wie die Unternehmensberatung Accenture im Rahmen einer aktuellen Studie ermittelt hat, sind die Kosten im Zusammenhang mit Cyberattacken allein in Deutschland im Vergleich zum Vorjahr um 18% gestiegen.

Cyber–Attacken kosten deutsche Industrie viele Milliarden Euro

der bitkom-Studie sind in den vergangenen zwei Jahren sieben von zehn deutschen nehmen Opfer von Cyberattacken oder Industriespionage geworden.

Gehackt: Cyberangriffe auf die Wirtschaft
ZEIT ONLINE - 09.01.2019
Auch **Unternehmen** fürchten um ihre vertraulichen Dokumente, Ideen und Patente. In vielen Betrieben gibt es heute kaum noch Computer oder ...

Cybersecurity und Datenschutz

heise online

Datenschutzpanne: British Airways soll etwa 204 Millionen Euro Strafe zahlen

Die britische Datenschutzbehörde fordert ein Millionenbußgeld von der Fluggesellschaft British Airways wegen der Datenschutzpanne bei Online-Buchungen von 2018.

Cybersecurity und Datenschutz

heise online

DSGVO-Verstoß: 110 Millionen Euro Bußgeld für Hotelkette Marriott

Britische Datenschützer legen erneut vor: Nach der Airline British Airways soll nun auch die Hotelkette Marriott eine satte Strafe aufgebrummt bekommen.

Cybersecurity und Datenschutz

Cybersecurity und Datenschutz

"Persönliche Daten von Menschen sind genau das – persönlich. Wenn eine Organisation sie nicht vor Verlust, Schaden oder Diebstahl schützen kann, ist das mehr als eine Unannehmlichkeit. Deshalb ist das Gesetz eindeutig – wenn Sie mit personenbezogenen Daten betraut sind, müssen Sie sich darum auch kümmern. Diejenigen, die das nicht tun, werden von meiner Behörde überprüft. "

Elizabeth Denham, ICO

DSGVO und DSG (V)

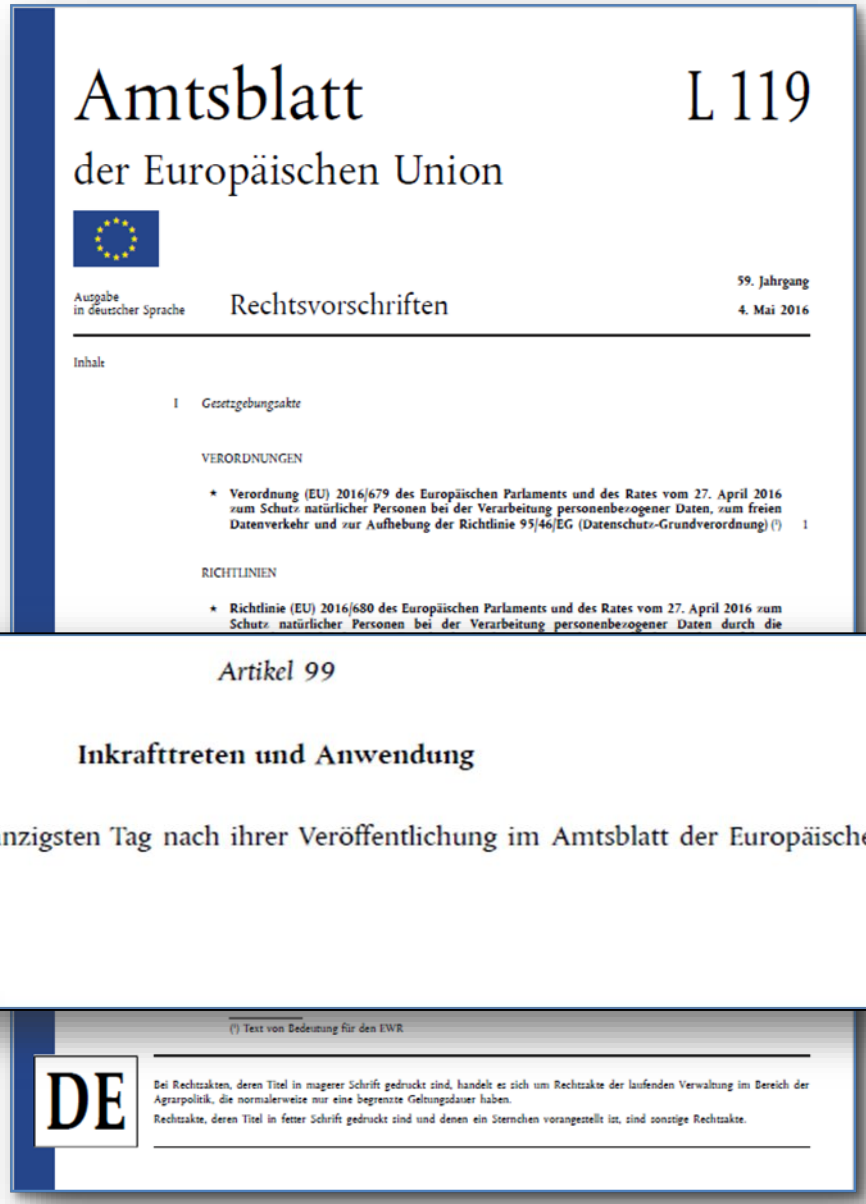
Liechtensteinisches Landesgesetzblatt

Jahrgang 2018 Nr. 272 ausgegeben am 7. Dezember 2018

Datenschutzgesetz (DSG)

vom 4. Oktober 2018

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:[1]



Amtsblatt L 119

der Europäischen Union

Ausgabe in deutscher Sprache Rechtsvorschriften 59. Jahrgang 4. Mai 2016

Inhalt

I *Gesetzgebungsakte*

VERORDNUNGEN

* **Verordnung (EU) 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)** (1) 1

RICHTLINIEN

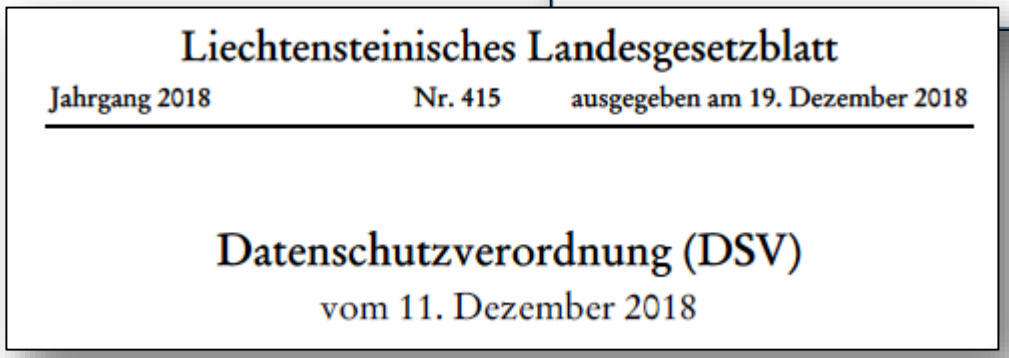
* **Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die**

Artikel 99

Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.



Liechtensteinisches Landesgesetzblatt

Jahrgang 2018 Nr. 415 ausgegeben am 19. Dezember 2018

Datenschutzverordnung (DSV)

vom 11. Dezember 2018

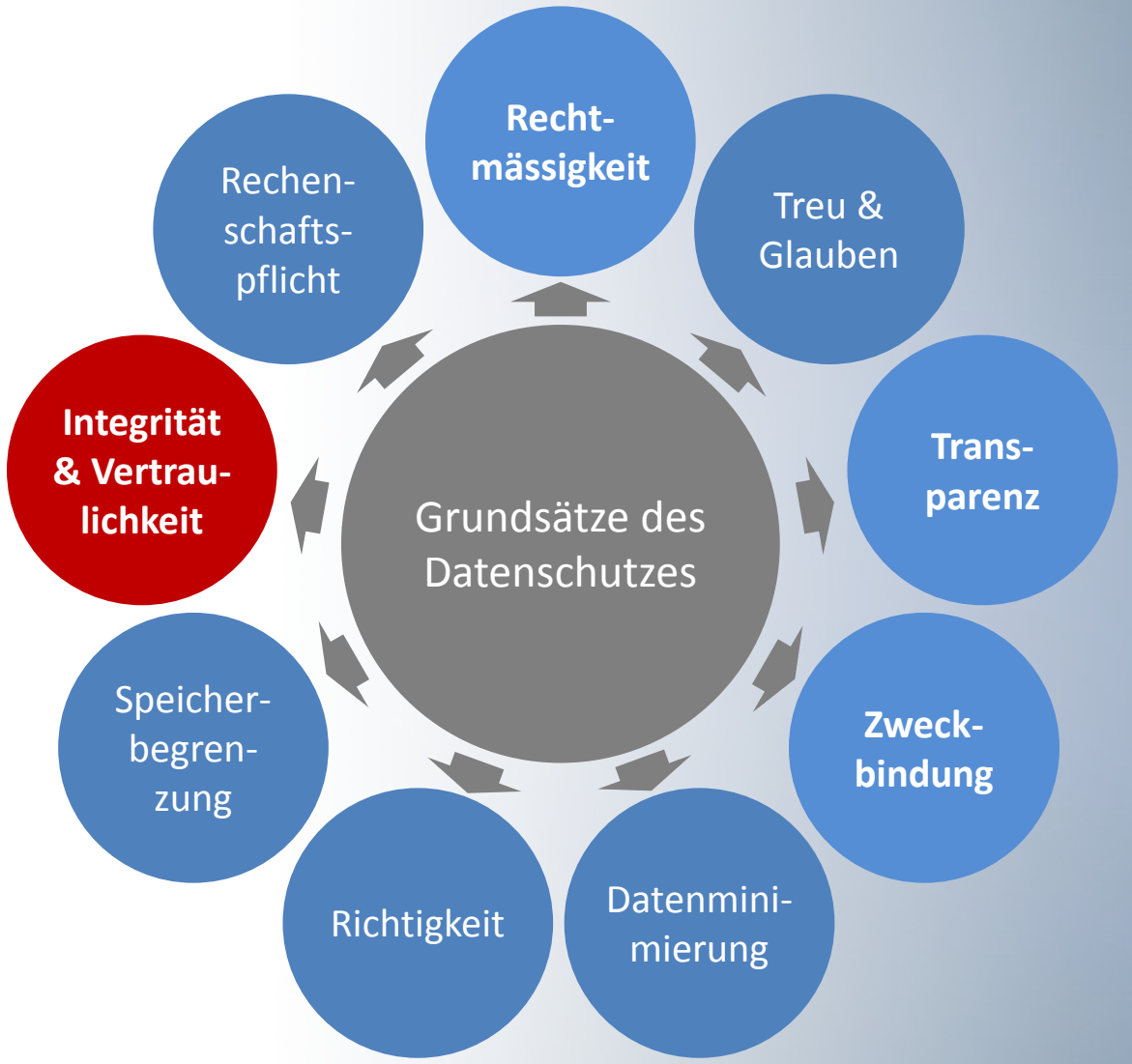
(1) Text von Bedeutung für den EWR

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

Grundsätze für die Datenverarbeitung



Grundsätze für die Datenverarbeitung

Integrität & Vertrau-lichkeit

Um eine angemessene Sicherheit zu gewährleisten, muss der Verantwortliche die personenbezogenen Daten schützen vor:

- unrechtmässiger Verarbeitung durch Unbefugte,
- unbeabsichtigter Schädigung und
- Verlust.

Dies stellt er durch geeignete technische und organisatorische Massnahmen sicher.

Grundsätze für die Datenverarbeitung

Rechen-schafts-pflicht

Hiernach ist der Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO aufgezählten Grundsätze (Rechtmässigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) **verantwortlich** und muss deren Einhaltung nachweisen können.

⇨ **Datenschutzmanagementsystem**

Rollenverteilung im Datenschutz

Art. 5 Abs. 1 Bst. f DSGVO

Personenbezogene Daten müssen

(f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Art. 32 DSGVO – Sicherheit der Verarbeitung

1. 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 gegebenenfalls unter anderem Folgendes ein:
    a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
    b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
    c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
    d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
2. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
3. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 33 DSGVO Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. 2Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Art. 34 DSGVO Benachrichtigung der von einer Verletzung des Schutzes personen-bezogener Daten betroffenen Person

1. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Empfehlungen.
3. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a. […]

Rechtsschutz

Betroffene Person kann Beschwerde einreichen/klagen,

- wo sie ihren Wohnsitz oder Arbeitsort hat;
- wo der Verantwortliche eine Niederlassung hat

Mögliche Ansprüche:

- Betroffenenrechte (Auskunft, Löschung, ...)
- Materieller und immaterieller Schadenersatz (bei Gericht)

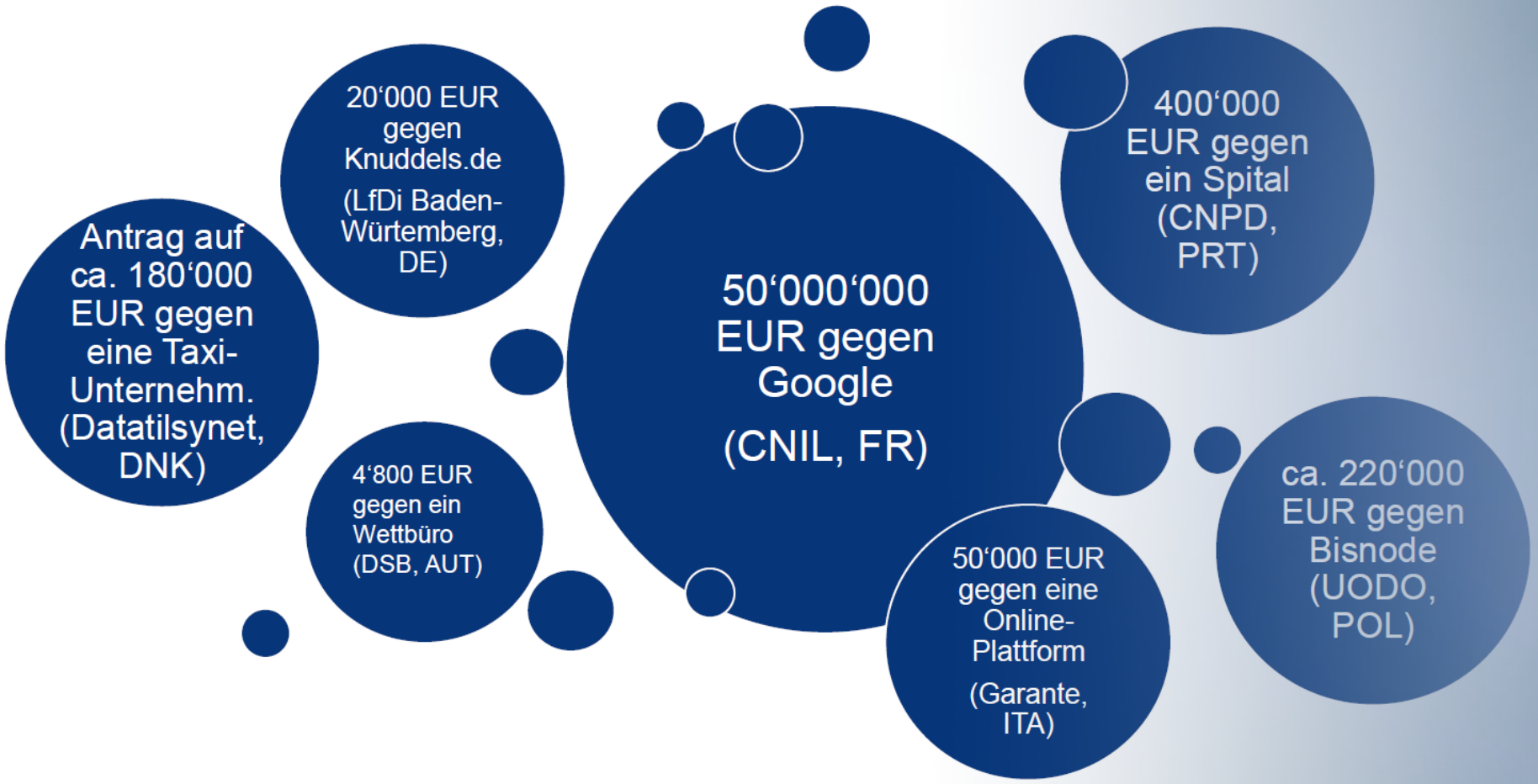
Rechtsdurchsetzung durch NGOs:

- NGOs können im Namen von Betroffenen klagen

Sanktionen

- Art. 83 DSGVO: Je nach Verstoss bis zu 20 000 000 Euro oder im Fall eines Unternehmens 4% des gesamten weltweit erzieltes Jahresumsatzes des vorangegangenen Geschäftsjahres
- Abstrakt bussgeldbewährt (unabhängig vom Eintritt eines Schadens)
- Aber: **Verhältnismässigkeitsprinzip relativiert Höhe**!

Sanktionen


20‘000 EUR gegen Knuddels.de
(LfDi Baden-Würtemberg, DE)
Antrag auf ca. 180‘000 EUR gegen eine Taxi-Unternehm. (Datatilsynet, DNK)
50‘000‘000 EUR gegen Google
(CNIL, FR)
400‘000 EUR gegen ein Spital (CNPD, PRT)
4‘800 EUR gegen ein Wettbüro (DSB, AUT)
50‘000 EUR gegen eine Online-Plattform
(Garante, ITA)
ca. 220‘000 EUR gegen Bisnode (UODO, POL)

MTBF

Personal Firewall

Phishing

OSI-Schichtenmodell

Darknet

Verantwortlicher

WhatsApp

Byte

Megabyte

Cache

Netzwerk

TSR

Operating System

Administrator

Cookie

ePrivacy

Spam

Makro

Fast Ethernet

File-System

Gateway

Hoax

Q-Bus

Proxy

Digitale Signatur

ROM

Datenträger

RAID

Makrovirus

Firmware Upgrade

Notfallkonzept

Spyware

Pseudonymisierung

TOM

FTP

Authentifizierung

Direktwerbung

Anonymisierung

BIOS

Boot-Viren

Auftragsverarbeitung

IPSec

IP-Adresse

Keylogger

Router

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

DATENSCHUTZ SERVICES ÜBER UNS RECHTSGRUNDLAGEN INTERNATIONALES

Datenschutzstelle

Für Bürgerinnen und Bürger

Beschwerde einreichen

Für Unternehmen

Datenschutzbeauftragten melden

Für Vereine

Aktuelles

Veranstaltungen

Datenschutzstelle
Städtle 38
Postfach 684
9490 Vaduz
Liechtenstein

T +423 236 60 90
info.dss@llv.li
www.datenschutzstelle.li