BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DATENSCHUTZ- UND IT-RECHT

23./24.9.2022

Peter Burgstaller

Fachhochschulprofessor für IT- und IP-Recht
Rechtsanwalt für IT- und IP-Recht
Gerichtssachverständiger für Urheberfragen und Medienwesen

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Warum Datenschutz und Informationssicherheit – Motivation für Unternehmen und Einrichtungen

Datenschutz

- DSGVO sieht hohe Strafen vor(2 oder 4 % des Jahres- Konzernumsatzes oder 10 bzw 20 Mio)
- Grundrecht – Verletzung führt zu Image- und Vertrauensschaden
- Compliance-Vorgaben

Informationssicherheit

- NISG sieht (auch) Strafen vor aber dzt. nur für einige Unternehmen (KRITIS)
  - NIS 2.0 ab Mitte 2024: Strafen wie DSGVO für „wichtige Unternehmen“
- **Haftung der Unternehmensleitung mit der Sorgfalt eines ordentlichen Unternehmers**, für Schaden des Unternehmens – Informationssicherheit = Funktionsfähigkeit des Unternehmens; Störung kann zu existenzbedrohenden Schäden führen

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

A. DATENSCHUTZ iSd DSGVO

Datenschutz trifft **jeden und jede Einrichtung** die personenbezogene Daten verarbeitet, sofern

- Niederlassung/Sitz im EWR liegt oder
- Waren/DL an Personen im EWR angeboten werden

Datenschutz ist ein Grundrecht mit unmittelbarer Drittwirkung („Horizontalwirkung“) zugunsten der Betroffenen

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Datenschutz betrifft …

- JEDE VERARBEITUNG von personenbezogenen Daten, also das Speichern, Ablegen, Ändern, Weiterleiten, Zusammenführen udgl in elektronischer oder manueller Art und Weise
- Ausg. ist grundsätzlich nur die Verarbeitung
  - von manuell unstrukturierten Daten
  - rein privater Daten zu privaten Zwecken
  - ohne EU/EWR-Anknüpfung
  - anonymen Daten

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Personenbezogene Daten sind…

alle Informationen, die jemand vernünftiger Weise einsetzt, um einen Bezug zu einer natürlichen Person herzustellen, also insb

- Name und Adresse,
- Email-Adresse mit Vor- und Nachnamen
- IP-Adresse, Telefon-Nummer,
- SVNR, KfZ-Kennzeichen
- Persönliches Bildnis

=> Auch **Pseudonyme** sind personenbezogenen => DSGVO-Anwendbarkeit

=> **Anonyme Daten** sind nicht personenbezogen => Keine DSGVO-Anwendbarkeit

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

GRUNDSÄTZE der zulässigen Datenverarbeitung heißt …

Verarbeitung hat

- **rechtmäßig** (Art 6) und
- transparent und klar/verständlich und
- **zweckgebunden** und
- unter Wahrung von **Vertraulichkeit/Integrität/Verfügbarkeit („CIA") („CIA")** durch TOMs und
- unter Wahrung der Betroffenenrechte (auch Info-Pflicht durch Datenschutzerklärung)

zu erfolgen.

Stand der Technik ist technische Maßnahmen zu setzen wo möglich!!

Der Stand der Technik ist mit Blick auf die zu verarbeitenden Daten zu beurteilen!

Stand der Technik ist die am Markt beste, allgemein verfügbare Technologie!

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

CIA - die 3 zentralen Sicherheitsziele

- C – Confidentiality = Vertraulichkeit
  - Verschlüsselung = Geheimahlten
- I – Integrity = Integrität
  - Signaturen (qual. el. Signatur = Sicherstellung der „Echtheit" des Dokuments – keine Änderungen ohne Kenntnis
- A – Availability = Verfügbarkeit
  - Back-up; Redundanzen

⇒Mit techn. Maßnahmen, wo möglich: ZB: Keine organisatorische Passwordpolicy, sondern technisch vorgegeben (zB 10 Zeichen, alle 6 Monate ändern und nach 5 Fehlversuchen Sperre für eine bestimmte Zeitdauer)

⇒Passwordcracker – Bruteforce = 10 Mrd Versuche pro Sekunde!! 10 Stellige Passwörter die auch Symbole und Nummern enthalten ergeben etwa 170 Trillionen Kombinationsmöglichkeiten => 520 Jahre Bruteforce!!

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Rechtmäßigkeit

Die rechtmäßige Verarbeitung ist zentraler Teil der Verarbeitungsgrundsätze und steht in Wechselbeziehung zur Zweckbindung.

Der **Zweck muss durch einen Rechtsgrund gedeckt** sein; Rechtsgründe sind:

- Einwilligung oder Vertrag
- Pflichten aus öffentlich-rechtlichen Vorgaben (Gesetze, VO,…)
- öffentliches Interesse oder lebenswichtige Interessen des Betroffenen/Dritten
- berechtigtes Interesse desjenigen, der die Daten verarbeiten will

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Akteure der DSGVO

- Betroffene = natürliche Person (deren Daten zu schützen sind)
- Verantwortlicher = verarbeitet die Daten des Betroffenen; er ist Verantwortlich für die Einhaltung der DSGVO gegenüber den Betroffenen (jede Rechtsperson)
- Auftragsverarbeiter = verarbeitet Daten **nur** im Auftrag des Verantwortlichen; kein eigener Zweck (jede Rechtsperson; Art 28-Vertrag)
- Sub-Auftragsverarbeiter = verarbeitete Daten als Sub-DL nur für den AV (kein eigener Zweck); Verantwortliche muss den Einsatz des Sub-AV genehmigen (jede Rechtsperson)
- Verantwortlicher darf sich nur „verlässlicher" AV bedienen und hat sich darüber auch zu vergewissern (=**Rechenschaftspflicht**); Auditierung; Zertifizierungen …

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

So funktioniert Datenschutz…

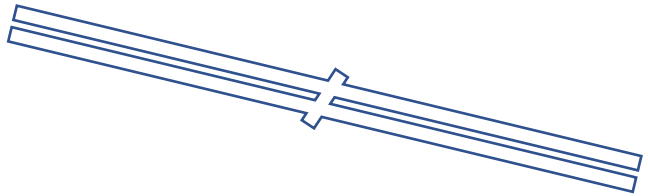
Rechtmäßigkeit: Einwilligung, Vertrag, lebenswichtige Int., berechtigte Int. des V oder Dritter, …

Betroffene (B)

Verarbeitungsgrundsätze insb Zweckbindung

Verantwortliche (V)

Schriftliches Dokument (Ar 28-Vertrag)



Auftragsverarbeiter (AV)

Sub-Auftragsverarbeiter …

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

B. DSGVO-SONDERTHEMEN

I. Datenübermittlung in Drittländer (Art 49):

- ausdrückliche Einwilligung nach Aufklärung über Risken oder (jederzeit widerrufbar)
- zur Vertragserfüllung notwendig (zB HR zentral im Konzern) oder
- öffentliches Interesse oder
- nicht wiederholt (zB Reisebüro für Geschäftsreisen)

Besonderheit für die USA (EuGH C-311/18 vom 16. Juli 2020):

- Standard-Vertragsklauseln (2021) und
- zusätzlich technische Maßnahme, um Zugriff von Behörden in den USA zu verhindern „customer key encryption"
- NEU:
  - Grundsatzeinigung zum „**Trans-Atlantic Data Privacy Framework**" publiziert, 25.3.2022
  - **American Data Privacy and Protection Act** (ADPPA), 3.6.2022 im Kongress

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Klausel für USA

Aufgrund des Urteils des EuGH in der Rechtssache C-311/18 vom 16. Juli 2020 erklären und garantieren wir Folgendes:

(i) Wir sind keine relevante US-Einrichtung (weder ein für die Verarbeitung Verantwortlicher noch ein Auftragsverarbeiter gemäß der DSGVO), die unter die Definitionen des 50 U.S.C. § 1881(b)(4) fällt, die uns direkt unter 50 U.S.C. **§ 1881a (FISA 702)** stellen könnte.

(ii) Wir sind keine relevante US-Einheit (weder ein für die Verarbeitung Verantwortlicher noch ein Auftragsverarbeiter gemäß der GDPR), die in irgendeiner Hinsicht mit US-Behörden kooperiert, die Kommunikationsüberwachungen gemäß **EO 12.333** durchführen.

(iii) Nach unserem besten Wissen sind wir keine relevante US-Einheit, die personenbezogene Daten verarbeitet, die an uns übermittelt werden und die einem anderen Gesetz unterliegen würde, das als Untergrabung des Schutzes personenbezogener Daten gemäß der DSGVO (Art 44) oder der EuGH-Entscheidungen, insbesondere in Bezug auf die Rechtssache C-311/18, angesehen werden könnte.

(iv) Wir beauftragen keinen anderen Auftragsverarbeiter, der die obigen Punkte bejaht und wir fordern dafür auch eine schriftliche Bestätigung von unseren Auftragsverarbeitern.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

II. Datenschutzfolgenabschätzung - KI und neue Technologien; Profiling

- Zweistufig: Risikobewertung einerseits und Konsultation der DSB andererseits
- DSFA nach Art 35 DSGVO – Risikobewertung – Maßnahmen – wenn hohes Risiko bleibt, dann Konsultation der DSB
- § 2 Abs 2 DSFA-V (BGBl 2018/278):
  - Z 1: Profiling
  - Z 3 a – h: Videoüberwachung an öffentlichen Plätzen
  - Z 4: Verarbeitungen von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien … insbesondere durch den Einsatz von künstlicher Intelligenz und die Verarbeitung biometrischer Daten, sofern die Verarbeitung nicht die bloße Echtzeitwiedergabe von Gesichtsbildern betrifft.

  Ausg.: Im **Zusammenhang mit Beschäftigungsverhältnissen gilt dies nicht**, wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

III. TOMs (dazu eingehende der nachfolgende Vortrag)

- **TOMs = Technische Organisatorische Maßnahmen**
- **Stand der Technik sind technische Maßnahmen =** Vorrang der technischen vor organisatorischen Maßnahmen
- Der Verantwortliche / Auftragsverarbeiter haben
  - 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,
  - unter Berücksichtigung der unterschiedlichen Kategorien von personenbezogenen Daten

  geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

§ 54 DSG (analog)

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle**);

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (**Datenträgerkontrolle**);

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**);

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**);

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (**Zugriffskontrolle**);

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**);

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**);

8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**) - zB Bitlocker (Stand d. Technik wäre AES 256 – BSI);

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellung**);

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

IV. Data Breach

- Art 33 – Meldung an DSB, wenn Risiko für die Rechte und Freiheiten des Betroffenen (72 h)
- Art 33 – Meldung auch an Betroffenen, wenn hohes Risiko für die Rechte und Freiheiten des Betroffenen (unverzüglich) = liegt idR bei Vertraulichkeitsverletzung von Gesundheitsdaten vor!
- Kein Data Breach bei „bloßer" Verfügbarkeitsverletzung (Achtung: IT-Sicherheitsvorfall setzt hingegen Verfügbarkeitsverletzung voraus)

TIPP:

- Data Breach alt: „***schwerwiegende und systematische***" Datenschutzverletzung von Vertraulichkeit und/oder Integrität
- https://www.dsb.gv.at/download-links/dokumente.html

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

V. Löschrecht

- Löschen heißt nicht immer physisch vernichten (nur wenn von vornherein rechtswidrig erhoben)
- Löschen heißt auch anonymisieren
- Löschen heißt idR ändern der Zugriffsrechte, um einen notwendigen/zwingenden/
  rechtfertigenden Zugriff auf Daten zu sichern (zB bei ausscheidenden Mitarbeitern – 7 Jahre Aufbewahrung von Geschäfts- und Finanzdaten und darüber hinaus!)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

VI. Datenschutzbeauftragter

- Zwingend nach Art 37 DSGVOI für Verantwortliche oder AV, wenn
  - Behörde/öffentliche Stelle oder
  - Kerntätigkeit in der Verarbeitung sensibler Daten liegt oder
  - Kerntätigkeit regelmäßige, systematische Überwachung
- Kann auch freiwillig errichtet werden
- Rat des DSB ist einzuholen bei DSFA und Data Breach
- Intern- oder Externe Besetzung des DSB
- Nicht kompatibel mit Geschäftsleitung, CISO, Leiter Marketing, Leiter Personal oder Leiter Rechtsabteilung

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

VII. TKG 2020 – Spamming, § 174

Unerbetene Nachrichten zu Werbezwecken (= § 107 alt):

- Vorherige Einwilligung = Opt-in
- Opt-in für Anrufe, Telefax, SMS, Email udgl
- Opt-in B2B und B2C
- Einwilligung kann jederzeit widerrufen werden
- Einwilligungswiderruf darf keinen Einfluss auf das Vertragsverhältnis haben

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

C. AUSGEWÄHLTE ENTSCHEIDUNGEN ZUM DATENSCHUTZ

VfGH 23.10.2017 – Videoaufnahmen am Arbeitsplatz

- Bilddaten sind grundsätzlich personenbezogene Daten
- Kann bei einer objektiven Betrachtungsweise eine Mitarbeitererfassung nicht wirksam ausgeschlossen werden, ist eine Videoüberwachung betriebsvereinbarungspflichtig iSd § 96a Abs 1 Z 1 ArbVG.
- BV-Pflicht auch dann, wenn die Erfassung von Mitarbeiter(-bild)daten nur „beiläufig" erfolgt bzw. ein „Nebeneffekt" der Videoüberwachung ist

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB 17.01.2018 – Permanente Videoüberwachung (Dash-Cam)

- digitale Videoüberwachung zur permanenten Beweissicherung durch Bildaufnahmen u.a. zwecks Erstattung von Verwaltungsstrafanzeigen bzw. zur Gewinnung von Beweismitteln ist datenschutzwidrig.
- Zulässig ist eine anlassbezogene Bildverarbeitung im vertretbaren Ausmaß für den Zweck der Erstattung einer Anzeige.

BGH 15.5.2018 – Dash-Cam / Beweismittel

1. **Videoüberwachung** auch nur teilweise im öffentlichen Raum **verlässt die rein private Sphäre** und kann nicht mehr als ausschließlich persönliche oder familiäre Tätigkeit betrachtet werden.

2. Eine Videoüberwachung mit Aufzeichnungsfunktion kann in das allgemeine Persönlichkeitsrecht der Betroffenen in seiner Ausprägung als Recht auf **informationelle Selbstbestimmung** eingreifen; dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.

3. Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie zur **Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke** erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

4. Die **permanente und anlasslose Aufzeichnung des Verkehrsgeschehens** ist mit den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes nicht vereinbar.

5. **Rechtswidrig geschaffene oder erlangte Beweismittel sind im Zivilprozess aber nicht schlechthin unverwertbar.**

6. Der Einzelne hat keine absolute, uneingeschränkte Herrschaft über "seine" Daten, weil er seine Persönlichkeit innerhalb der sozialen Gemeinschaft entfaltet. Mit der **Teilnahme am öffentlichen Straßenverkehr** setzt sich der Einzelne bspw selbst der Wahrnehmung und Beobachtung durch andere Verkehrsteilnehmer aus.

7. Das in Art. 20 Abs. 3 GG **verankerte Rechtsstaatsprinzip** – ordnet das Streben nach einer materiell richtigen Entscheidung an. Um die Wahrheit zu ermitteln, sind die Gerichte deshalb grundsätzlich gehalten, von den Parteien angebotene Beweismittel zu berücksichtigen, wenn und soweit eine Tatsachenbehauptung erheblich und beweisbedürftig ist.

8. Obgleich die permanenten und anlasslosen Verkehrsgeschehensaufzeichnungen mit den datenschutzrechtlichen Regelungen nicht vereinbar sind, ist die **Verwertung dieser als Beweismittel** im Unfallhaftpflichtprozess **zulässig**.

9. Im **Unterschied zum heimlichen Belauschen von Gesprächen** und den dazu judizierten Beweisverwertungsverboten, wird bei Aufzeichnungen des öffentlichen Verkehrsgeschehens ein Verhalten festgehalten, das ohnehin in der Öffentlichkeit, zB auf öffentlichen Straßen, stattfindet.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB, 27.08.2018 – Löschfrist von Bewerberdaten

- Die Speicherung von Bewerberdaten für die Dauer von sieben Monaten ist gerechtfertigt, angemessen und verhältnismäßig
- Die zulässige Löschfrist von sieben Monaten für die Bewerberdaten ab Bewerbungseingang setzt sich aus der sechsmonatigen Anspruchsfrist des Betroffenen und einem weiteren Monat für den allfälligen Klageweg zusammen

Achtung: Dienstzeugnisse von ausgeschiedenen Mitarbeitern sind 30 Jahre lang aufzubewahren!

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB, 09.04.2019 – SVNR ist per se kein Gesundheitsdatum

- Gesundheitsdaten sind Informationen aus denen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen
- Eine SVNR al bloß zusätzliches Identifizierungsmerkmal ist kein Gesundheitsdatum; das gilt auch im Zusammenhang mit der Inanspruchnahme von Sozialleistungen

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB, 16.04.2019 – Fotos auf Sommerrodelbahn

- Die Koppelung der Einwilligung zur Fotoaufnahme mit einer Actioncam an den Benützungsvertrag einer Sommerrodelbahn ist gemäß Art 7 Abs 4 DSGVO rechtswidrig

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB, 04.07.2019 – Videoüberwachung Tiefgarage

- Die elektronische Erfassung von Zeit, Ort und Kfz-Kennzeichen zur Abwicklung einer Parkraumbewirtschaftung in der Tiefgarage eines Einkaufszentrums ist eine zulässige Datenverarbeitung

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

EuGH, 01.10.2019 – Cookie-Einwilligung

- IP-Adressen sind personenbezogene Daten
- Der Einsatz Cookies, um Websitenutzerverhalten zu protokollieren, bedarf der vorherigen Zustimmung der Websitebesucher (zB Google Analytics, zu Feststellung des Nutzerverhaltens auf der Website)
- Der Einsatz von sog. „technisch bedingter Cookies" kann ohne Zustimmung vorgenommen werden – berechtigtes Interesse (zB zur Bewirtschaftung des „Einkaufswagens" bei Webshops)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

BayLDA 15.03.2021, LDA_1085.1-12159-IDV – US-Newslettertool („Mailchimp“) und EU-US-Datenexport

Die Übermittlung von Email-Adressen an einen US-Newslettertool-Provider (hier: „Mailchimp“) ist nach Art 44ff DSGVO unzulässig, wenn

- nicht die Standardvertragsklauseln („SCC“) abgeschlossen **und**
- zusätzlich (insbesondere technische) Maßnahmen ergriffen wurden, um den Zugang/Zugriff der personenbezogenen Daten (Email-Adressen) vor US-Behörden sicherzustellen.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB Bescheid 16.11.2021 – unverschlüsselter USB Stick

Nach Art 5 DSGVO sind personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung, und zwar durch **geeignete technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit").

Dieser Verarbeitungsgrundsatz wird durch Gebrauch eines unverschlüsselten USB-Sticks verletzt.

Verschlüsselung: AES 256 (BSI-Stand der Technik; Bitlocker hat standardmäßig AES 128)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB – Aufzeichnung von Kundenanrufen

Es gibt für Banken keine gesetzliche Pflicht als Zahlungs- und Wertpapierdienstleister Kundenanrufe aufzuzeichnen.

Im Konkreten erfolgte eine Aufzeichnung des Kundenanrufs ohne Opt-out-Option – dies verletzt den Grundsatz der Datenminimierung.

DSB 22.12.2021 – Google Analytics
(=CNIL 2.3.2022, MED 2022-015, -016)

Google Analytics: Kennnummern sind personenbezogene Daten iSd Art 4 Z 1 DSGVO.

Wer die Entscheidung trifft das Tool „Google Analytics" auf der Website zu implementieren, entscheidet über „Zwecke und Mittel" der mit dem Tool in Verbindung stehenden Datenverarbeitung und ist daher als Verantwortlicher iSd Art. 4 Z 7 DSGVO anzusehen; der Tool-Anbieter ist hingegen Auftragsverarbeiter

Der EU-US Angemessenheitsbeschluss („Privacy Shield") ist ohne Aufrechterhaltung seiner Wirkung ungültig; eine Datenübermittlung in die USA findet daher keine Deckung in Art. 45 DSGVO (Angemessenheitsbeschluss).

Solange ein Datenimporteur in die USA die Möglichkeit hat, auf Daten im Klartext zuzugreifen, sind die technischen Maßnahmen (hier: Verschlüsselung) nicht als effektive geeignete Garantien im Sinne des Art 46 DSGVO anzusehen, wenn der Datenimporteur 50 U.S. Code § 1881a („FISA 702") unterliegt.

Für den Fall das weder ein Angemessenheitsbeschluss (Art 45) noch geeignete Garantien (Art 46) vorgebracht werden können, ist eine Datenübermittlung an ein Drittland/internationale Organisation bspw möglich, wenn nach Art 49 Abs 1 lit a DSGVO die betroffene Person ausdrücklich eingewilligt hat, nachdem die Betroffene Person über Risken und Sicherheitsgarantien aufgeklärt wurde.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Google-Fonts – Abmahnwelle Sommer 2022

- Datenübermittlung in die USA ist datenschutzrechtlich bedenklich, weil die USA als Drittstaat qualifiziert wird.
- Übermittlung nur mit ausdrücklicher Zustimmung und vorheriger Aufklärung über Risken
- Google-Fonts – IP-Adresse an Google = Google unterliegt 50 U.S. Code § 1881a („FISA 702")

Google-Fonts-Abmahnwelle - Was ist zu tun:

=> Einbettung von Google-Fonts beseitigen

=> Kein Schadenersatz

=> Auskunfterteilung nach Art 15 DSGVO, wenn ausreichend identifiziert

=> Keine Anwaltskosten, weil nicht zur zweckenstprechenden Rechtsverfolgung

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB 27.1.2022 – Aufsicht des Arbeitgebers

- Ein wirksames Kontrollsystem setzt nicht voraus, dass Arbeitnehmer ständig durch den Arbeitgeber beaufsichtigt werden – im Gegenteil: Ohne Anhaltspunkte wäre eine laufende Beaufsichtigung eine unverhältnismäßige Überwachung.
- Wenn daher ein an sich „unauffälliger" Mitarbeiter unberechtigte ELGA-Abfragen (hier: zum Impfstatus- und Medikationsdaten) vornimmt, ist dieser Mitarbeiter aus Sicht der DSGVO Verantwortlicher; dem Arbeitgeber ist jedenfalls ohne Anlass keine Verletzung der Kontrollpflicht vorzuwerfen.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

DSB 1.3.2022 – GPS-System im Firmenauto

Ein GPS-Gerät im Firmenfahrzeug kann nicht auf Art. 6 Abs. 1 lit. f DSGVO mit dem Argument gestützt werden, dass das Tracking-System eine administrative Erleichterung und eine ökonomische Entlastung darstellt.

Dies auch dann, wenn zwar das Gerät durch Start der Zündung des Fahrzeugs aktiviert und durch Ausschalten der Zündung deaktiviert wird, allerdings zusätzlich auch für private Fahrten deaktiviert werden kann.

Vielmehr könnte der Zweck auch durch gelindere Mittel, welche eine geringere Datenverarbeitung mit sich bringen, erreicht werden könnte.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

D. Netz- und Informationssicherheit

NIS-RL 2016/1148 vom 6.7.2016

- Rechtsakt zu „Cybersicherheit" in der EU für kritische Infrastrukturen und bestimme kritische Onlinedienste
- NIS-RL legt Maßnahmen fest, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssicherheit in der EU erreicht werden soll.
- NIS-RL ist in nationales Recht umzusetzen – AT: NISG 2018
- Strafen bei Verletzung: bis EUR 100.000

NIS-RL 2.0 (in nationales Recht per Mitte 2024 umzusetzen**)**

- Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
- Ausweitung des Anwendungsbereiches von kritischer Infrastruktur auf wichtige Infrastrukturen
- Strafen bei Verletzung = DSGVO

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

1. Grundlage und Ziel von NIS

Mit diesem **NISG 2018** soll ein **hohes Sicherheitsniveau von Netz- und Informationssystemen** von

- **Betreibern wesentlicher Dienste** in den Sektoren: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur
- **Anbietern digitaler Dienste** im Bereich Cloud-, Suchmaschinen und Online Marktplätzen sowie
- **Einrichtungen der öffentlichen Verwaltung** erreicht werden.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

1.1 Betreiber wesentlicher Dienste

- Anbieter von Diensten aus folgenden Sektoren:
  - Energie,
  - Verkehr,
  - Bankwesen,
  - Finanzmarktinfrastrukturen,
  - **Gesundheitswesen,**
  - Trinkwasserversorgung und
  - Digitale Infrastruktur („Internet-Knoten" (IXP – Internet Exchange Point)

denen eine **wesentliche Bedeutung insbesondere für die Aufrechterhaltung des öffentlichen Lebens, nämlich** Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie hat **und dessen Verfügbarkeit abhängig von Netz- und Informationssystemen ist.**

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

BwD wird mittels Bescheid des BMI nach der NISV („Schwellenwerte“) festgelegt

- Stromerzeugung: Engpassleistung mehr als 340 MW
- Gasspeicheranlagenbetreiber: mehr als 10.000 GWh Arbeitsgasvolumen/Jahr
- Luftverkehr – Flughafen: > 10 Mio Passagiere (Wien: 2021 – 10,5 Mio; 2019 – 30 Mio; Linz: 2021 – 70K; 2019: 450K)
- Trinkwasserversorgung – Gewinnung oder Aufbereitung oder Verteilung: 6,424 Mio m³ Wasser/Jahr

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Gesundheitswesen als KRITIS iSd NISG und NISV

§ 8. (1) Wegen ihrer Bedeutung für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes im Sinne des § 16 Abs. 2 NISG sind im Sektor Gesundheitswesen wesentliche Dienste:

- 1. die medizinische Versorgung in den Bereichen Diagnose, Therapie und Pflege als
- a) akutstationäre Versorgung oder
- b) akutambulante ärztliche Versorgung (§ 2 Z 11) in einer Spitalsambulanz
- durch **Krankenanstalten**, wenn sie insgesamt
  - **drei Betten je 1 000 Einwohner** pro Bundesland in zentral gelegenen Versorgungsregionen mit großem Einzugsgebiet (§ 2 Z 10), oder
  - **zwei Betten je 1 000 Einwohner** pro Bundesland in allen anderen Versorgungsregionen (Bettenrichtwerte) vorhalten;
- 2. das **Betreiben einer Leitstelle**, die die Durchführung von Notfallrettungstransporten unterstützt.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

1.2 Anbieter digitaler Dienste

- **Online-Marktplatz** = einen digitalen Dienst, der es Verbrauchern oder Unternehmern ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen
- **Online-Suchmaschine** = einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können
- **Cloud-Computing-Dienst** = einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht

Sofern sie keine **Kleinst- oder Kleinunternehmen** sind: weniger als 50 Mitarbeiter und max 10 Mio Umsatz/Jahr

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

1.3 Einrichtungen der öffentlichen Verwaltung

Einrichtungen des Bundes sind

- die Bundesministerien,
- die Gerichtshöfe des öffentlichen Rechts,
- den Rechnungshof,
- die Volksanwaltschaft,
- die Präsidentschaftskanzlei und
- die Parlamentsdirektion

Weitere Dienststellen des Bundes können vom zuständigen Bundesminister durch Verordnung bestimmt werden.

NISG gilt **nicht für öffentliche Einrichtungen des Landes** (Hackerangriff in Kärnten oder in der Stadtgemeinde Feldbach odgl)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

2. Was ist zu tun nach dem NISG

- Mind. eine NIS-Behörde/Mitgliedstaat (BKA und BMI in AT)
- Computer-Nofallteams (CERT, CSIRT – Allg. Cert, Gov-Cert und Branchen-Certs)
- ISMS – Informations-Sicherheits-Management System = **Info-Sec ist zu managen (CISO)**
- Meldepflicht bei Sicherheitsvorfall (in AT an CSIRT)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

3. Einrichtung einer NIS-Behörde

BKA:

- Koordination der **Erstellung einer Strategie** und eines jährlichen Berichts zur Sicherheit von Netz- und Informationssystemen
- **Vertretung von Österreich in der Kooperationsgruppe** sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind; die Zuständigkeiten anderer Ressorts bleiben davon unberührt
- **Koordination der öffentlich-privaten Zusammenarbeit** im Bereich der Sicherheit von Netz- und Informationssystemen;
- **Betrieb des GovCERT**
- **Unterrichtung der Öffentlichkeit** über einen Sicherheitsvorfall, der ganze Sektoren betrifft
- **Ermittlung von Betreibern wesentlicher** Dienste und laufende Aktualisierung einer Liste von wesentlichen Diensten
- **Feststellung der Eignung und Ermächtigung von Computer-Notfallteams**
- Veröffentlichung und Aktualisierung einer Liste der Computer-Notfallteams

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

BMI:

- **Betrieb einer zentralen Anlaufstelle** (SPOC) für die Sicherheit von Netz- und Informationssystemen
- **Entgegennahme und Analyse von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle**, regelmäßige Erstellung eines diesbezüglichen Lagebildes und Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter Informationen an inländische Behörden oder Stellen
- Überprüfung der Sicherheitsvorkehrungen und die Einhaltung der Meldepflichten
- **Feststellung und Überprüfung der qualifizierten Stellen (**prüfen KRITIS**)**
- **Unterrichtung der Öffentlichkeit über einzelne Sicherheitsvorfälle**
- Leitung und Koordination des **Cyberkrisenmanagements auf operativer Ebene**
- **Feststellung einer Cyberkrise** = Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

4. Einrichtung einer Zentralen Anlaufstelle – SPOC (**Single Point of Contact**)

Für die Sicherheit von Netz- und Informationssystemen wird eine zuständige zentrale Anlaufstelle (SPOC) beim Bundesminister für Inneres eingerichtet

SPOC dient als operative Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union sowie der Kooperationsgruppe und dem CSIRTs-Netzwerk dient

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

5. Einrichtung einer **Qualifizierte Stelle**

- Einrichtung mit Niederlassung in Österreich die für die **Überprüfung von Sicherheitsvorkehrungen bei Betreibern wesentlicher Dienste** zuständig ist.
- Qualifizierte Stellen werden vom Bundesminister für Inneres festgestellt
- Führen einer Liste von Qualifizierten Stellen beim BMI

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

6. Einrichtung von **Computer-Notfallteams**

- Zur Gewährleistung der Sicherheit von Netz- und Informationssystemen werden Computer-Notfallteams eingerichtet.
- Zu diesem Zweck werden
  - **Nationale Computer-Notfallteams** (zuständig insb für Anbieter digitaler Dienste) und
  - **sektorenspezifische Computer-Notfallteams** (zB MilCert oder Österreichs Energie für Energieversorger) sowie
  - das **Computer-Notfallteam der öffentlichen Verwaltung** (GovCERT) die Einrichtungen der öffentlichen Verwaltung

bei der Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Aufgaben des Computer-Notfallteams

- Entgegennahme von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle;
- Weiterleitung von Meldungen an den Bundesminister für Inneres;
- Ausgabe von Frühwarnungen, Alarmmeldungen und Handlungsempfehlungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken, Vorfälle oder Sicherheitsvorfälle;
- Erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;
- Beobachtung und Analyse von Risiken, Vorfällen oder Sicherheitsvorfällen sowie Lagebeurteilung;
- Beteiligung am CSIRTs-Netzwerk

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

7. **Sicherheitsvorkehrungen** - TOMS

- NISG-relevante Einrichtungen haben **geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen** zu treffen, **insb um Verfügbarkeit der Dienste sicher zu stellen**
- TOMS haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.
- Der **Stand der Technik ist die beste am Markt allgemein verfügbare Technologie**
- Technische Maßnahmen sind Stand der Technik; org. Maßnahmen sind subsidiär zu ergreifen.

⇒ ISMS hat folgendem Rechnung zu tragen:

  - Sicherheit der Systeme und Anlagen
  - Bewältigung von Sicherheitsvorfällen
  - Betriebskontinuitätsmanagement
  - Überwachung, Überprüfung und Erprobung
  - Einhaltung der internationalen Normen

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Sicherheitsvorkehrungen iSd NISV

Sicherheitsvorkehrungen müssen den Stand der Technik berücksichtigen und insb iSd Analge 1 zur NISV folgendes umfassen:

- Sicherheitsmaßnahmen für Governance und Risikomanagement
- Sicherheitsmaßnahmen zum Umgang mit Dienstleistern, Lieferanten und Dritten
- Sicherheitsmaßnahmen zur Sicherheitsarchitektur
- Sicherheitsmaßnahmen zur Systemadministration
- Sicherheitsmaßnahmen zum Identitäts- und Zugriffsmanagement
- Sicherheitsmaßnahmen zur Systemwartung und zum Betrieb
- Sicherheitsmaßnahme zur physischen Sicherheit
- Sicherheitsmaßnahmen zur Erkennung von Vorfällen
- Sicherheitsmaßnahmen zur Bewältigung von Vorfällen
- Sicherheitsmaßnahmen zur Betriebskontinuität
- Sicherheitsmaßnahme zum Krisenmanagement

Die Umsetzung jeder Sicherheitsmaßnahme hat, nach Durchführung einer Risikoanalyse zu erfolgen (siehe dazu auch die Anlage 1 zur NISV)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

8. **Sicherheitsvorfälle und Meldung**

- Sicherheitsvorfall = Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, **die zu einer Einschränkung der Verfügbarkeit** oder zu einem Ausfall des betriebenen Dienstes **mit erheblichen Auswirkungen geführt** hat; bei der Beurteilung der Erheblichkeit sind insbesondere folgende Parameter zu berücksichtigen:
  - Zahl vom Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
  - Dauer des Sicherheitsvorfalls,
  - geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet und
  - Auswirkung auf wirtschaftliche und gesellschaftliche **Tätigkeiten;**

=> Sicherheitsvorfall setzt also zwingend Verfügbarkeitsbeschränkung voraus!

- Ein Sicherheitsvorfall ist unverzüglich an das zuständige Computer-Notfallteam zu melden
- Notfall-Team hat die Meldung unverzüglich an den Bundesminister für Inneres weiterzuleiten
- Details zur **Wesentlichkeit des Sicherheitsvorfalls** NISV, zB Stromerzeugung: 340 MW Erzeugungsleistungsverringerung; Gesundheit: mehr als 3 Stunden Ausfall; Flughafen: binnen 24h mehr als 1/3 von einem Ausfall betroffen sind.

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

9. **NIS 2.0 Sektor Gesundheitswesen**

- Gesundheitsdienstleister iSd Art 3 lit g der RL 2011/24/EU
- EU-Referenzlaboratorien iSd Art 15 der VO XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren
- Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel iSd Art 1 Nr 2 der RL 2001/83/EG
- Einrichtungen, die pharmazeutische Erzeugnisse iSd Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2), herstellen
- Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch iSd Art 20 der VO XXXX22 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

10. ISMS

- Informationssicherheit als zentrales Asset eines Unternehmens
- IT hat zu funktionieren – sonst Stillstand, Fehler udlg = Schaden
- Informationssicherheit ist zu managen durch eine eigens eingerichtete Managementfunktion – „Informationssicherheitsbeauftragter" oder „Chief Information Security Officer"
- CISO ist losgelöst von der operativen Tätigkeit; er plant und prüft die Umsetzung geeigneter Sicherheitsmaßnahmen
- CISO darf nicht CIO oder CTO sein; auch mit DSB inkompatibel
- CISO ist zwingend für NISG-Unternehmen; dringend empfehlenswert für alle

⇒**Je besser qualifiziert Mitarbeiter sind, desto höher ist deren Eigenverantwortung**

⇒**Schulung, um die Eigenverantwortung der Mitarbeiter zu erhöhen!**

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

NIS 2.0 auch für wichtige Einrichtungen

Schwellenwerte für wesentliche/wichtige Einrichtungen

- **Wesentliche Einrichtungen – Anhang I NIS-RL - NISV**
- **Wichtige Einrichtungen**
  - Alle anderen Einrichtungen sofern kein Kleinstunternehmen.
  - ZB Lebensmittel, Post, Abfallwirtschaft, Chemie, Medizinproduktehersteller, Plattformen für soziale Netze, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräten
- Ausnahmen:
  - Sektoren Digitale Infrastruktur und Öffentliche Verwaltung = immer wesentlich, da kritische Einrichtung

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Schwellenwerte Empfehlung 2003/261/EG EU Kommission

Empfehlung 2003/361/EG der EU-Kommission

- **Großunternehmen**: Alle Unternehmen, sofern kein KMU.
- **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
- **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
- **Kleinstunternehmen**: Weniger als 10 Mitarbeiter und weniger als 2 Mio Umsatz

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Gesundheitsdienstleister und NIS 2.0

- Gemäß GTelG sind ELGA-Gesundheitsdienstleister Angehörige des ärztlichen Berufes, des zahnärztlichen Berufes, **Apotheken**, Krankenanstalten und Einrichtungen der Pflege
- Gesundheitswesen nach NISG und NISV:
  - Kritische Infrastrukur = NISV § 8 siehe oben „Bettenrichtwerte“

- Gesundheitswesen nach NIS 2.O
  - Auch Apotheken ausg. Apotheken mit weniger als 2 Mio Umsatz und weniger als 10 Mitarbeitern („Kleinstunternehmen“)

BURGSTALLER
& PARTNER
RECHTSANWÄLTE

Herzlichen Dank für Ihre Aufmerksamkeit

Peter Burgstaller

peter.burgstaller@lawfirm.eu