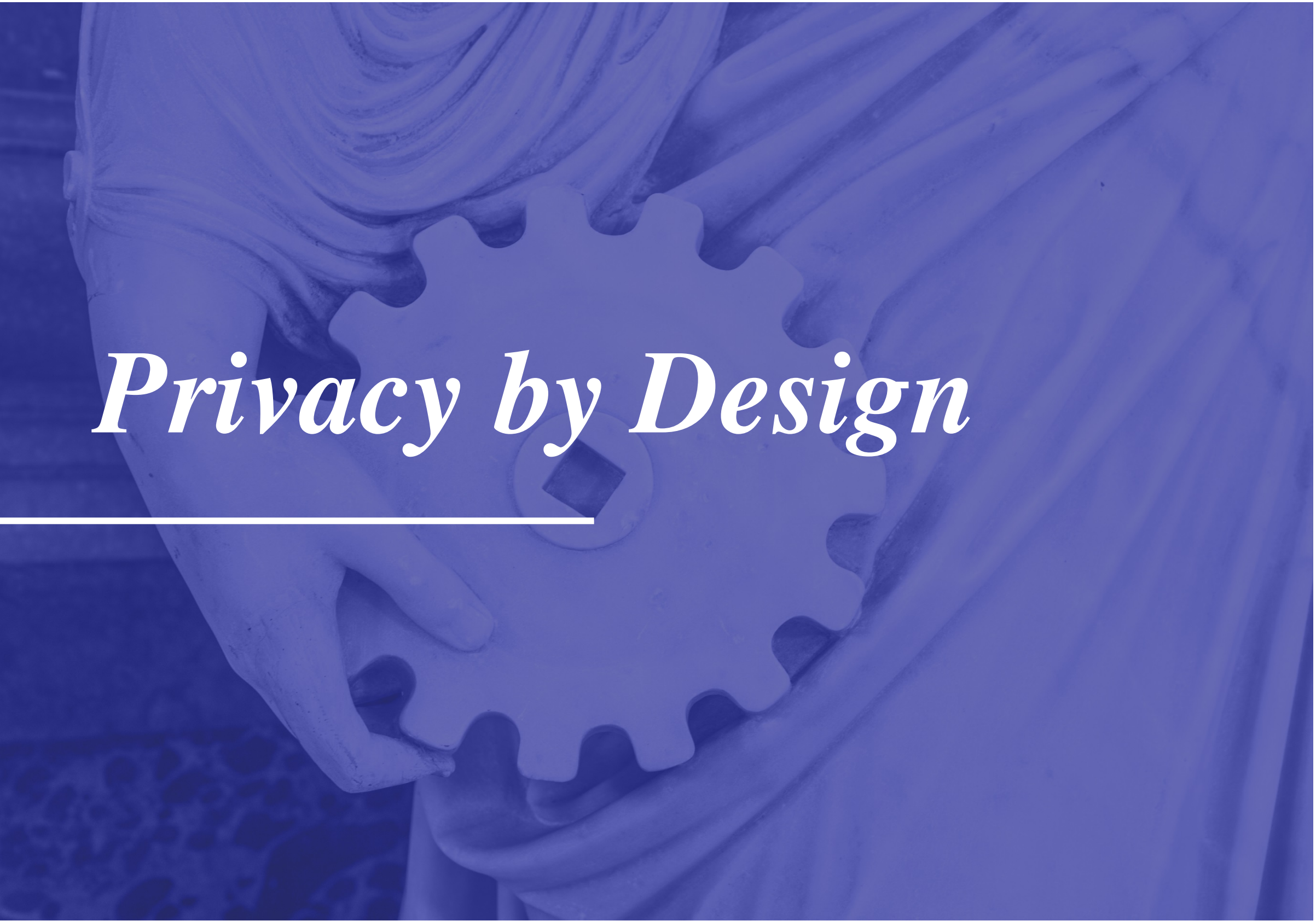
CERHA HEMPEL

Privacy by Design, Privacy by Default und vertragliche Umsetzungsmöglichkeiten

Dr. Kristoferitsch, LL.M. (Harvard)

INHALT

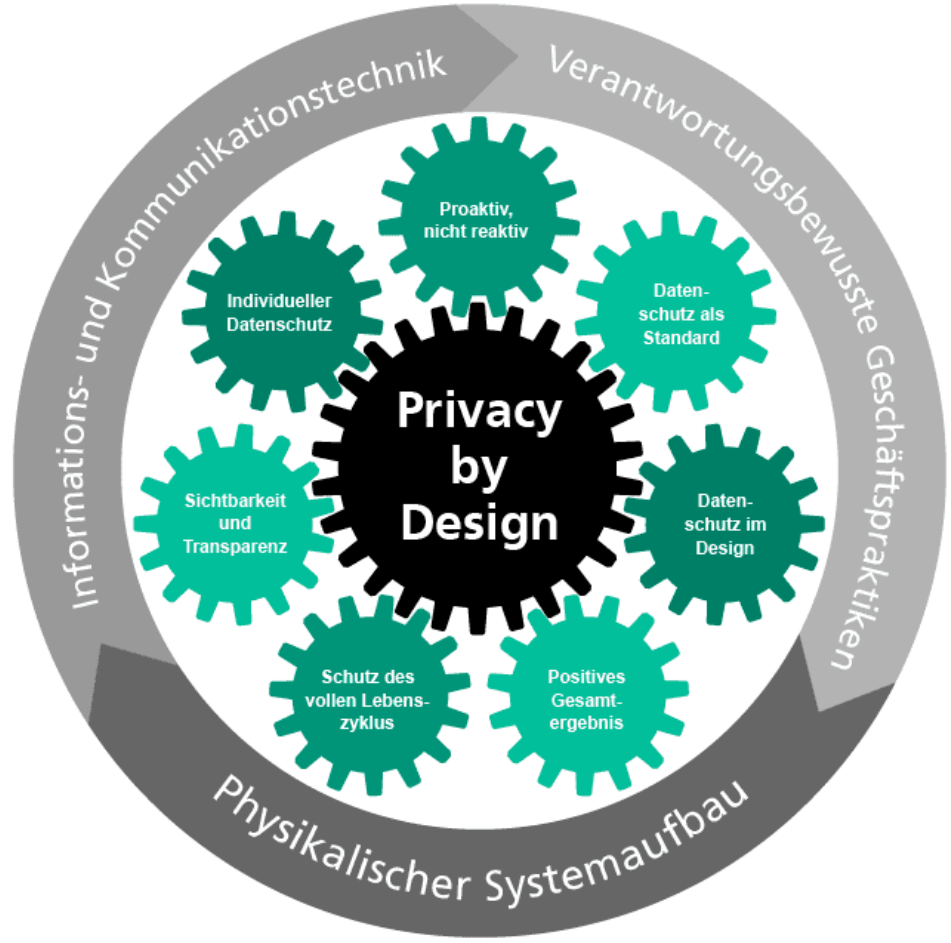
CERHA HEMPEL



Privacy by Design

Privacy by Design
Einleitung

- Geschichtlicher Hintergrund
  - Technologie wurde bis in die 1970iger nur als Ursache für zunehmenden Eingriff in die Privatsphäre verstanden.
  - Trendumkehr in den 1970igern
    - ➢ Technologie könnte auch Privatsphäre wiederherstellen.
    - ➢ Kodifizierung von Grundsätzen und Best Practices (Ende der 1970iger)
- Privatsphäre durch Technikgestaltung
  - Konzept von Ann Cavoukian (DSB, Ontario, Kanada), 1990iger Jahre



Privacy by Design
Einleitung

- 7 Grundsätze von Ann Cavoukian
  - (1) Proaktive, nicht reaktive Maßnahmen
  - (2) Schutz der Privatsphäre als Standardvoreinstellung
  - (3) In das Design eingebetteter Datenschutz
  - (4) Volle Funktionalität
  - (5) Ende-zu-Ende-Sicherheit
  - (6) Sichtbarkeit und Transparenz
  - (7) Achtung der Privatsphäre des Nutzers

Appendix A: *The 7 Foundational Principles*

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default Setting***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – ***Positive-Sum***, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.

5. End-to-End Security – ***Full Lifecycle Protection***

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency*** – Keep it ***Open***

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. ***Respect*** for User Privacy – Keep it ***User-Centric***

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy by Design
Einleitung

- Rechtsgut
  - Die Unerfahrenheit und Unwissenheit der Betroffenen soll nicht ausgenutzt werden
- „Privacy by Design“
  - Technische und organisatorische Mittel sollen ein hohes Datenschutzniveau gewährleisten und hierdurch die Datensammlung minimieren
- Umsetzung in der DSGVO
  - Grundsatz der Datenminimierung und Zweckbindung (Art 5)
  - Datenschutz durch Technikgestaltung (Art 25)
  - Sicherheit der Verarbeitung (Art 32)

Privacy by Design
Technikgestaltung – Art 25 Abs 1 DSGVO

- Umsetzung
  - geeigneter technischer und organisatorischer Maßnahmen, sowie
  - notwendiger Garantien
- Ziel
  - Umsetzung der Datenschutzgrundsätze sowie der sonstigen Anforderungen der DSGVO, sowie
  - Schutz der personenbezogenen Daten
- Berücksichtigung von
  - Risiken (ermittelt in der Risiko-Folgenabschätzung)
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände, Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Privacy by Design
Technikgestaltung – Art 25 Abs 1 DSGVO

- Zeitpunkt
  - Planungsphase des Projekts und
  - Operationelle Phase des Projekts
- Adressat
  - Verantwortlicher
    - Entscheidung über Zwecke und Mittel der Verarbeitung personenbezogener Daten (Art 4 Z 7 DSGVO)
  - Auftragsverarbeiter nur indirekt (über die Auswahl)
    - Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen (Art 4 Z 8 DSGVO)
  - Hersteller und Entwickler der Produkte nur indirekt (über die Auswahl)
    - Ausnahme: Sie sind Verantwortliche

Privacy by Design

Rechtsgrundlagen – Art 32 DSGVO

- Datensicherheit als Grundlage für einen effektiven Datenschutz und damit Privacy by Design
- Sicherheit der Datenverarbeitung
  - Treffen von geeigneten technischen und organisatorischen Maßnahmen
    - Pseudonymisierung und Verschlüsselung
    - Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen.
    - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
    - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
  - Ziel
    - Gewährleistung von einem dem Risiko angemessenen Schutzniveau

Privacy by Design

Rechtsgrundlagen – Art 32 DSGVO

- Berücksichtigung von
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zwecke der Verarbeitung
  - Der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen
- Trifft Verantwortlichen und Auftragsverarbeiter

Privacy by Design
Rechtsgrundlagen

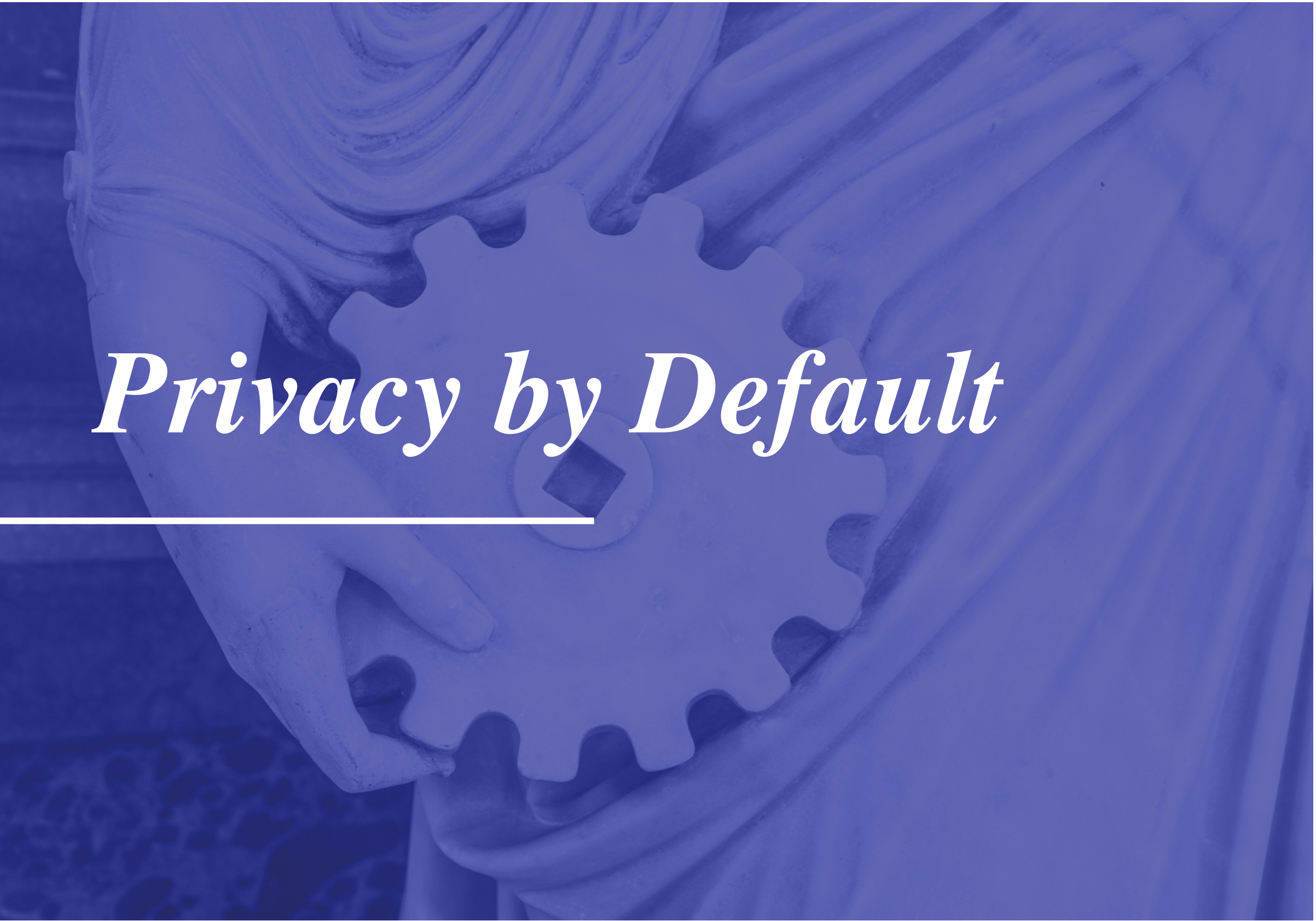
- Die rechtliche Verpflichtung nach der DSGVO
  - **Trifft** den/die datenschutzrechtlich Verantwortlichen, bzw Auftragsverarbeiter (idR nicht den Hersteller oder Entwickler) und
  - **Gilt** nur für die Verarbeitung personenbezogener (nicht auch anonymisierter/pseudonymiserter) Daten.
- Rechenschaftspflicht
- Die Nichteinhaltung kann beträchtliche Strafen zur Folge haben, und zwar je nach dem welcher Betrag höher ist (Art 83 Abs 4 lit a DSGVO):
  - Geldbußen von bis zu EUR 10 Mio oder
  - 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres

Privacy by Design

Praxistipps

- Anonymisieren und pseudonymisieren Sie die Daten (wenn und soweit möglich).
- Verschlüsseln Sie die Daten (wenn und soweit möglich).
- Behalten Sie den Überblick und die Kontrolle über die Daten (Herkunft, Art, Übermittlung, Zugriff).
- Kontrollieren Sie, wo Sie die Daten speichern (Vorsicht bei einer Speicherung in Drittstaaten).
- Arbeiten Sie nur mit Unternehmen zusammen, die der DSGVO oder einem vergleichbaren Datenschutzniveau unterliegen.
- Verarbeiten Sie die Daten nur auf Basis und nach Maßgabe der Rechtsgrundlage (Art 6 DSGVO).
- Holen Sie sich, soweit notwendig, eine wirksame Einwilligung der Betroffenen ein.
- Informieren Sie die Betroffenen von der Erhebung, Verarbeitung und Übermittlung ihrer personenbezogenen Daten.
- Stellen Sie sicher, dass die Anfragen von Betroffenen fristgerecht beantwortet werden.
- Speichern Sie Daten nur solange Sie sie brauchen und es Ihnen (per Gesetz, Einwilligung etc) erlaubt ist.
- Richten Sie andere angemessene technische und organisatorische Datenschutzmaßnahmen ein.

CERHA HEMPEL



Privacy by Default

Privacy by Default
Einleitung

- „Privacy by Default“
  - Nutzer tendieren nicht dazu, ihre Voreinstellungen zu ändern, obwohl sie Datenschutz schätzen (Privacy Paradox)
  - Voreinstellungen sollen daher ein hohes Datenschutzniveau gewährleisten und hierdurch die Datensammlung minimieren.
  - Zwang zu Opt-in Lösungen
- Zählt im weiteren Sinne zu Privacy by Design.

Privacy by Default

Rechtsgrundlagen – Art 25 Abs 2 DSGVO

- Treffen geeigneter technischer und organisatorischer Maßnahmen, die sicherstellen, dass
  - durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind
- Diese Verpflichtung gilt für
  - die Menge der erhobenen personenbezogenen Daten,
  - den Umfang ihrer Verarbeitung,
  - ihre Speicherfrist und
  - Zugänglichkeit
- Insbesondere ist sicherzustellen, dass
  - personenbezogene Daten nicht per Voreinstellung einer unbestimmten Zahl von Personen zugänglich gemacht werden

Privacy by Default

Rechtsgrundlagen – Art 25 Abs 2 DSGVO

- Die rechtliche Verpflichtung nach der DSGVO
  - **Trifft** den/die datenschutzrechtlich Verantwortlichen (vs Hersteller oder Entwickler) und
  - **Gilt** nur für die Verarbeitung personenbezogener (nicht auch anonymisierter/pseudonymiserter) Daten.
- Rechenschaftspflicht
- Die Nichteinhaltung kann beträchtliche Strafen zur Folge haben, und zwar je nach dem welcher Betrag höher ist:
  - Geldbußen von bis zu EUR 10 Mio oder
  - 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres

Privacy by Default

Praxistipps

- Stellen Sie auf Ihren Endgeräten die Vorab-Einstellungen auf das höchst-mögliche Datenschutzniveau zB social media, Diensthandy der Mitarbeiter, landwirtschaftliche Maschinen.
- Erlauben Sie einem Dienst keinen Zugriff auf Standortdaten von zB Mitarbeitern, soweit dieser nicht notwendig ist.
- Erlauben Sie einem Dienst (zB social media) keinen Zugriff auf Kontaktdaten von zB Zulieferern, Mitarbeitern oder Kunden, soweit dieser nicht notwendig ist.
- Sofern Ihre Einstellungsoptionen über die Default settings hinausgehen, holen Sie sich die Einwilligung der Betroffenen (zB Mitarbeiter, Kunden, Zulieferer) ein.

CERHA HEMPEL

Vertragliche Umsetzungs-möglichkeiten

Vertragliche Umsetzungsmöglichkeiten
Einleitung

- Differenzierung bei den Vertragsarten nach den **datenschutzrechtlichen Rollen**
  - Verantwortlicher
  - Auftragsverarbeiter
  - Gemeinsam Verantwortliche
- Vertragsarten
  - Auftragsverarbeitervertrag
  - Controller-Controller Vertrag
  - Vertrag über die gemeinsame Verantwortung
  - Sonderfall: Standardvertragsklauseln
- **Wie wird in diesen Verträgen Privacy by Design und by Default berücksichtigt?**

CERHA HEMPEL

Auftragsverarbeiter vertrag

Vertragliche Umsetzungsmöglichkeiten
Auftragsverarbeitervertrag

- Voraussetzung
  - Verantwortlicher beauftragt einen Auftragsverarbeiter mit der Datenverarbeitung
  - Beispiel:
    - Ein Landwirt bietet einen Webshop an und nutzt hierfür die Dienste eines IT-Unternehmens.
- Formerfordernisse
  - Schriftlich (digital oder analog)

Vertragliche Umsetzungsmöglichkeiten

Auftragsverarbeitervertrag

- Inhalt
  - Gegenstand und Dauer der Verarbeitung
  - Art und Zweck der Verarbeitung
  - Art der personenbezogenen Daten
  - Kategorien betroffener Personen
  - Pflichten und Rechte des Verantwortlichen
  - Dokumentiere Weisung des Verantwortlichen
  - Vertraulichkeit (soweit keine gesetzliche Verschwiegenheitspflicht besteht)
  - **Pflicht des Auftragsverarbeiters, geeignete technische organisatorische Maßnahmen zu treffen**
  - Bedingungen für Subauftragsverarbeitung
  - **Unterstützungspflichten des Auftragsverarbeiters (unter anderem bei der Erfüllung der organisatorlich-technischer Sicherheitsmaßnahmen)**
  - **Löschungs- und Herausgabepflichten nach Beendigung der Verarbeitungsleistung**
  - Informationspflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen
  - Ermöglichung von und Mitwirkung bei Kontrollen des Verantwortlichen oder von diesem beauftragten Dritten
  - Etc.

Vertragliche Umsetzungsmöglichkeiten
Auftragsverarbeitervertrag

- Wie wird Privacy by Design und by Default im Auftragsverarbeitervertrag berücksichtigt?
- Privacy by Design und by Default finden grundsätzlich nicht Eingang in den Vertrag
  - Eigentlich ist die Auswahl des Auftragsverarbeiters bereits eine Maßnahme iSd Privacy by Design
  - Aber die Rechte und Pflichten, die sich aus diesen Konzepten ergeben, finden sich dennoch auch indirekt im Vertrag, obgleich sich diese eher auf Datensicherheit (Art 32 DSGVO) beziehen
    - Pflicht des Auftragsverarbeiters, geeignete technische organisatorische Maßnahmen zu treffen
    - Unterstützungspflichten des Auftragsverarbeiters (unter anderem bei der Erfüllung der organisatorisch-technischen Sicherheitsmaßnahmen)
    - Löschungs- und Herausgabepflichten nach Beendigung der Verarbeitungsleistung

CERHA HEMPEL

Controller-Controller-Vertrag

Vertragliche Umsetzungsmöglichkeiten
Controller-Controller-Vertrag

- Konstellation
  - Ein Verantwortlicher übermittelt personenbezogene Daten an einen weiteren Verantwortlichen, der diese zu eigenen Zwecken verarbeitet
  - Beispiel:
    - Ein Landwirt übermittelt Daten an eine Forschungseinrichtung, die diese Daten für eine Studie zu landwirtschaftlichen Geräten verarbeitet.
- Vereinbarung zwischen eigenständigen Verantwortlichen
  - Gesetzlich nicht geregelt
  - *Praxistipp*: Abschluss eines Controller-Controller Vertrages, wenn besonders viele und/oder besonders sensible Daten verarbeitet werden.
- Vertragsform (Empfehlung)
  - Schriftlich
  - Verbindlicher Rechtsakt

Vertragliche Umsetzungsmöglichkeiten
Controller-Controller-Vertrag

- Regelung von Privacy by Design und by Default?
  - In der Praxis meist kein Vertragsbestandteil, weil diese Pflicht die Verantwortlichen unabhängig von der Vereinbarung trifft und die Auswahl des Vertragspartners bereits eine organisatorische Maßnahme iSd Privacy by Design darstellt.
  - Datensicherheit (Art 32) typischerweise Vertragsbestandteil – Diese Klauseln decken indirekt auch Privacy by Design oder by Default ab.

CERHA HEMPEL

Vertrag über die gemeinsame Verantwortung

Vertragliche Umsetzungsmöglichkeiten

Vertrag über die gemeinsame Verantwortung

- Voraussetzung
  - Mehrere Verantwortliche entscheiden gemeinsam über Mittel und Zweck der Verarbeitung
  - Beispiel:
    - Ein Landwirt nutzt einen Facebook-Pixel auf seiner Homepage, um sein Marketing zu verbessern.
- Notwendiger Inhalt der Vereinbarung
  - Beschreibung der Funktionen der Vertragsparteien
  - Art und Weise des Zusammenwirkens
  - Verteilung/Aufteilung der datenschutzrechtlichen Pflichten
- Andere (optionale) Vertragsinhalte sind denkbar

Vertragliche Umsetzungsmöglichkeiten

Vertrag über die gemeinsame Verantwortung

- Keine Formerfordernisse, aber
  - Transparente Vereinbarung: Klare, verständliche und nachvollziehbare Formulierung
  - Offenlegung der wesentlichen Vertragsinhalte gegenüber Betroffenen
  - Schriftform
  - Empfehlung der EDPB: Vertrag oder andere rechtsverbindliche Vereinbarung
- Rechtswirkung
  - Uneingeschränkte Wirkung im Innenverhältnis und gegenüber Aufsichtsbehörden
  - Betroffene können ihre datenschutzrechtlichen Rechte gegenüber jedem einzelnen Verantwortlichen geltend machen!
  - Optionale Regelungen haben keine Außenwirkung

Vertragliche Umsetzungsmöglichkeiten
Vertrag über die gemeinsame Verantwortung

- Wie wird Privacy by Design und by Default im Vertrag über die gemeinsame Verantwortung berücksichtigt?
  - Privacy by Design und by Default finden grundsätzlich nicht Eingang in den Vertrag, aber
    - Die Auswahl des Vertragspartners ist bereits eine organisatorische Maßnahme iSd Privacy by Design
    - EDPB empfiehlt die Aufteilung der datenschutzrechtlichen Verpflichtungen durch Vertrag über die gemeinsame Verantwortung, um Privacy by Design und by Default umzusetzen,
    - Optionale Klauseln könnten die Datensicherheit und damit indirekt auch Privacy by Design oder by Default abdecken zB
      - ✓ Sicherstellung der Richtigkeit und Aktualität der Daten
      - ✓ Sicherstellung der Löschung von Daten, nach Ablauf der Speicherdauer
      - ✓ Einwilligung (Verantwortung für die Einholung, Dokumentation, Belehrung, Widerruf, Altersfeststellung, etc)
      - ✓ Vertraulichkeit

CERHA HEMPEL

Spezialfall

Standardvertrags-klauseln

Vertragliche Umsetzungsmöglichkeiten
Spezialfall: Standardvertragsklauseln

- Voraussetzung
  - Datenübermittlung in Drittländer
  - Kein Angemessenheitsbeschluss liegt vor
- Standardvertragsklauseln
  - Der Datenimporteur und -exporteur garantieren, dass die ins Drittland übermittelten Daten einem der DSGVO angemessenen Schutzniveau unterliegen.
  - Die Aufsichtsbehörden und Gerichte des EU-Landes sind zuständig.
- Privacy by Design und by default?
  - Datensicherheit durch technische und organisatorische Maßnahmen spielt eine entscheidende Rolle im Rahmen der Standardvertragsklauseln.
- Seit der EuGH Entscheidung *Schrems II* (16.7.2020, C 311/18) sind Standardvertragsklauseln problematisch.
- Draft der geplanten neuen Standardvertragsklauseln wurde allerdings erst kürzlich veröffentlicht.

CERHA HEMPEL

Zusammenfassung

Zusammenfassung

- Privacy by Design und by Default als technische Instrumente zum Schutz der Betroffenen
  - Durch technische und organisatorische Maßnahmen und Voreinstellungen sollen so wenige personenbezogene Daten wie notwendig gesammelt werden.
  - Die Verpflichtung zu Privacy by Design und by Default trifft die Verantwortlichen (also häufig die Landwirte), nicht die Hersteller und Entwickler der technischen Geräte.
- Privacy by Design und by Default werden in den datenschutzrechtlichen Verträgen grundsätzlich nicht berücksichtigt.
  - Idealvorstellung
    - Der Verantwortliche lenkt die Nachfrage, indem er sich für jene Vertragspartner entscheidet, die organisatorisch und technisch ein hohes Datenschutzniveau garantieren.
  - Realität
    - Aufgrund der Marktmacht vieler Unternehmen (gerade in der precision agriculture und im social media Sektor) eher unrealistisch!

CERHA HEMPEL

Vielen Dank für *Ihre Aufmerksamkeit!*

CERHA HEMPEL

RA Dr. Hans Kristoferitsch, LL.M. (Harvard)

Partner

Cerha Hempel Rechtsanwälte GmbH

Parkring 2

A-1010 Wien

Telefon: +43/1/514 35-291

E-Mail: hans.kristoferitsch@cerhahempel.com