Der Datenschutz im Betrieb

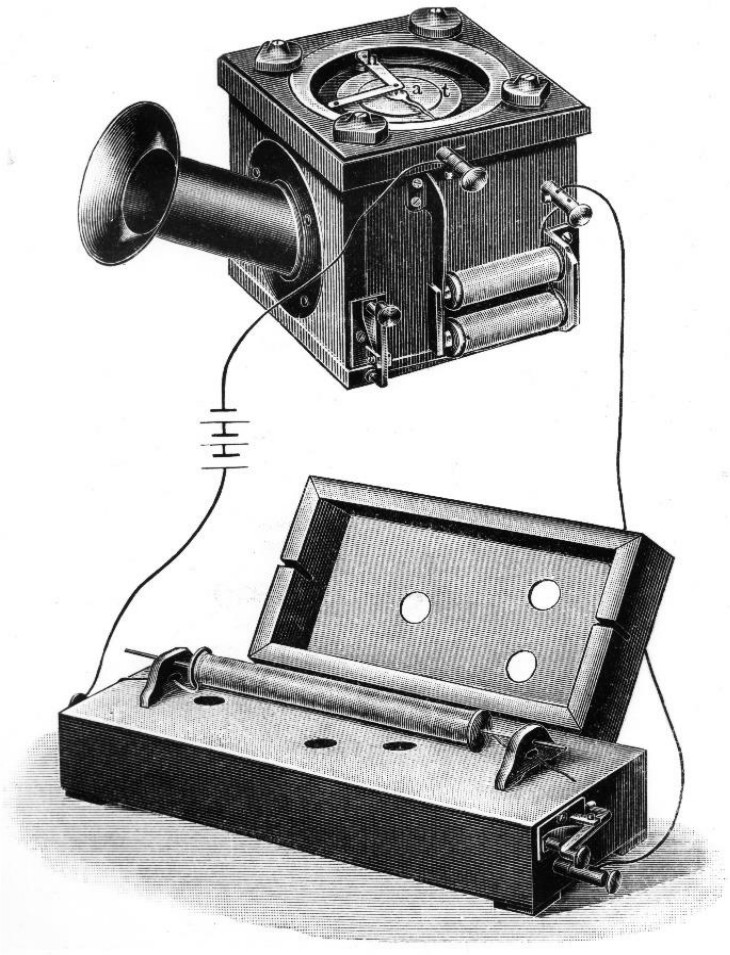
Mag.ª Clara Fritsch
Abteilung Arbeit & Technik

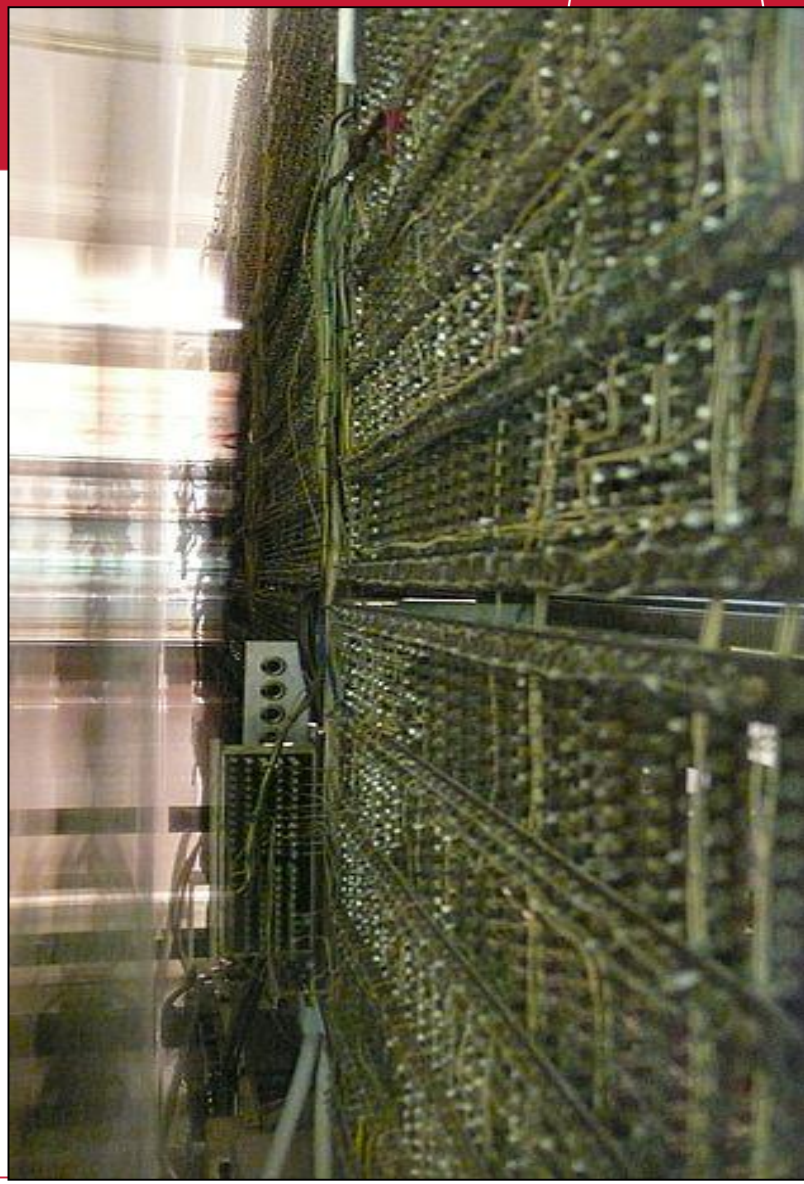
Seminar der GPA-djp
14.-16. Jänner 2020

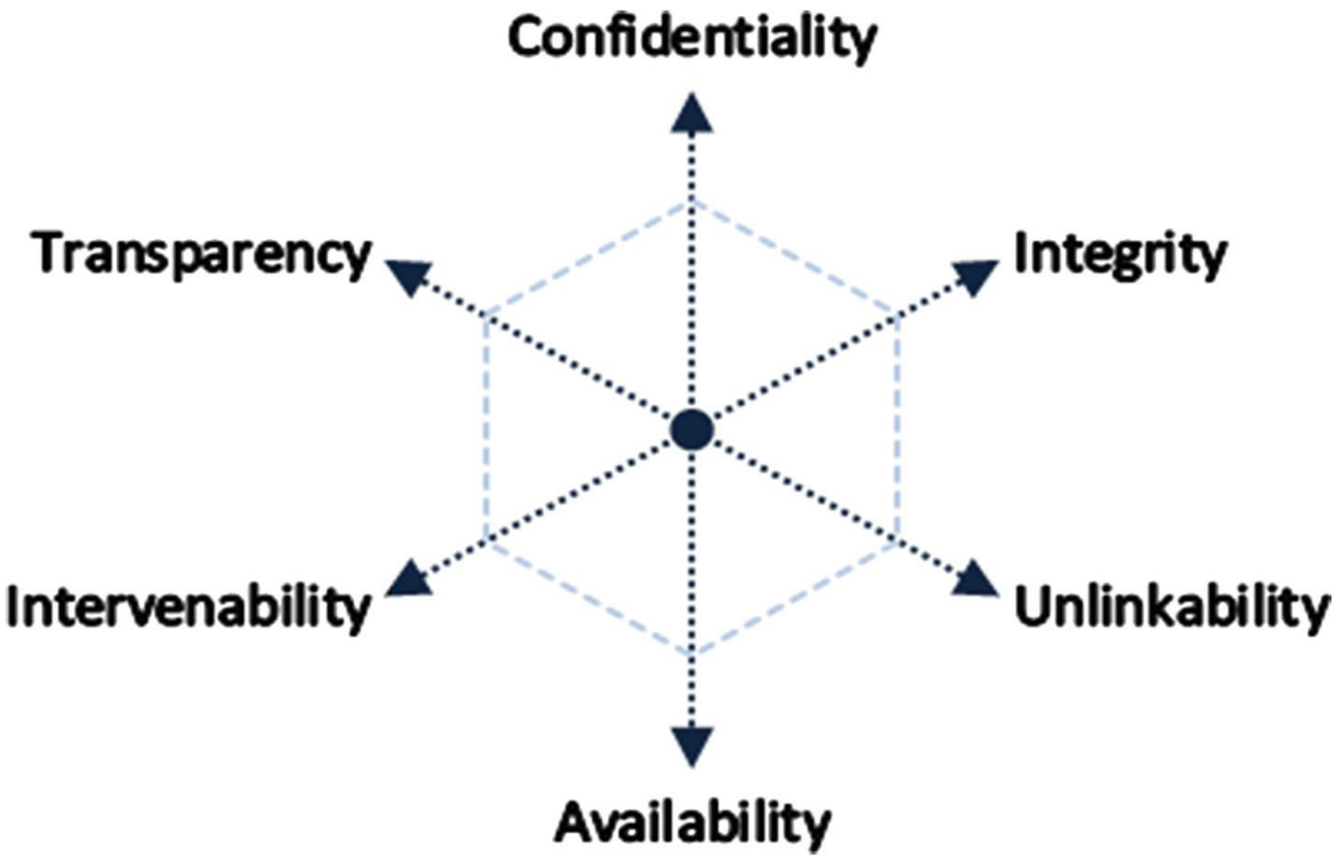
GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

IKT-Systeme im Betrieb -
Technische Grundlagen
14-01-20

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER







Vertraulichkeit
vs
Verfügbarkeit

Integrität
vs
Gestaltbarkeit

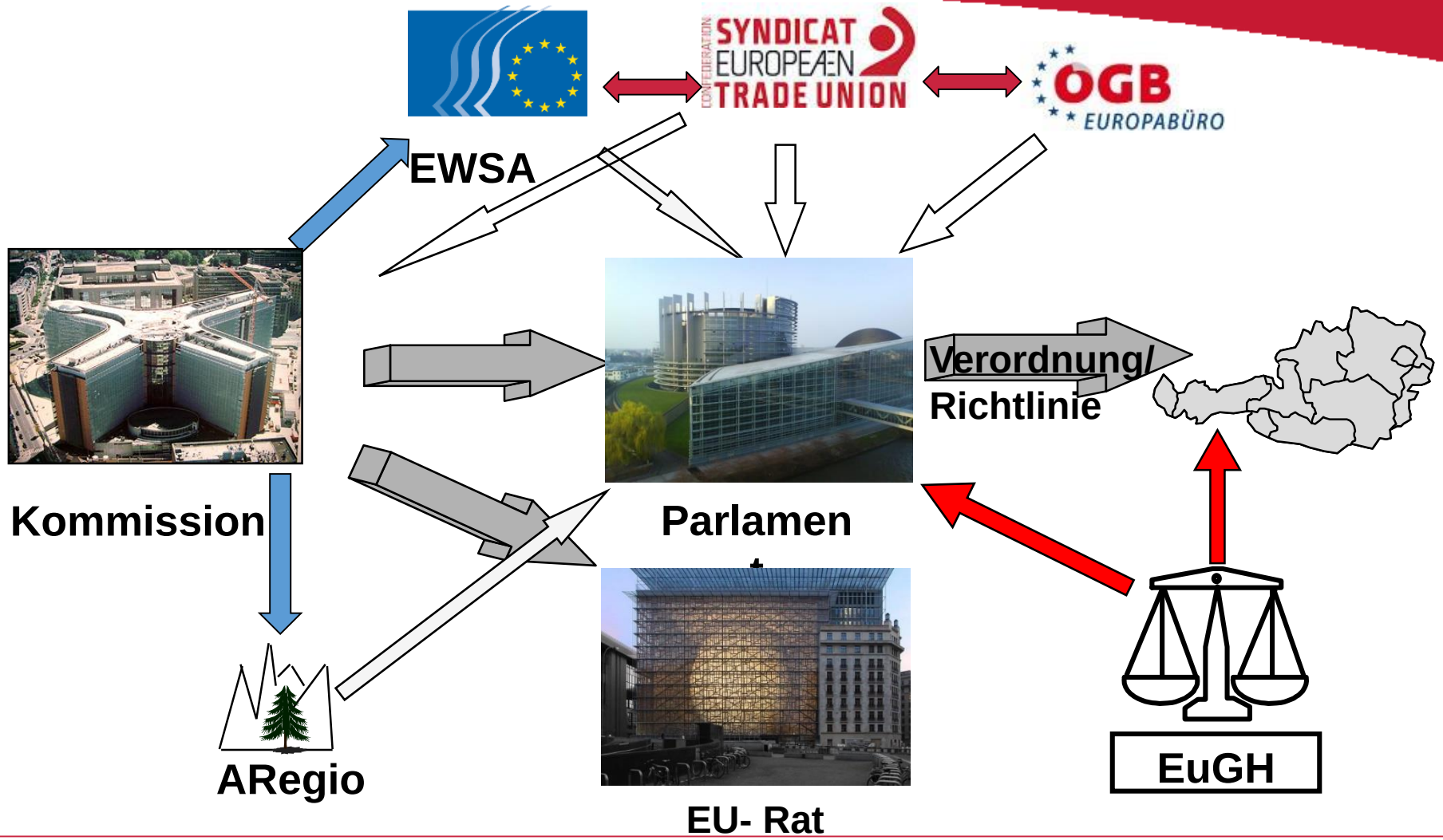
Transparenz
vs
Nicht-Vernetzbarkeit

Quelle: Rost Martin (CC)

Recht und Gericht -
rechtliche Grundlagen
15-01-20

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Lobbying der Sozialpartner



personenbezogene Daten im Betrieb

- Bild
- Ton
- Text
- Gehalt
- Stammdaten
- Einkommen
- Leistung
- Ortung
- Protokolle
- Qualifikation
- Zeiterfassung
- Zutritt

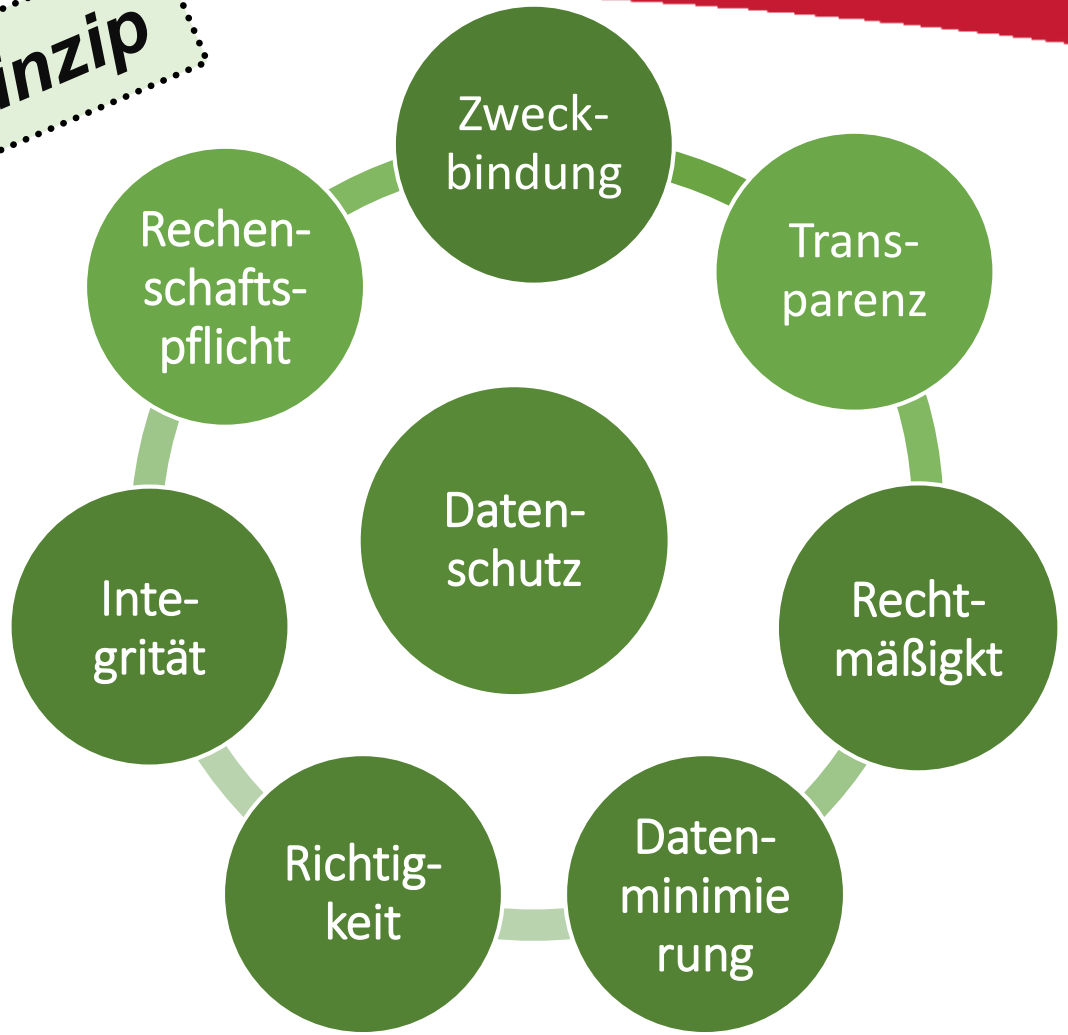
- Gesundheit
- Gewerkschaftszugehörigkeit
- Politische Meinung
- Sexuelle Orientierung
- Biometrische Daten
- Genetische Daten
- religiöse/weltanschauliche Überzeugung
- rassische/ethnische Herkunft

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; … direkt oder indirekt, mittels Zuordnung zu einer Kennung“ (Art 4 Z 1 DSGVO)

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Grundsätze des Datenschutzes

NEU: Marktortprinzip



GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Grundlagen der Datenverarbeitung (Art 6)

- Einwilligung
- Vertrag
- Gesetz, rechtliche Verpflichtung
- Lebenswichtiges Interesse
- Öffentliches Interesse
- Berechtigtes Interesse des Verantwortlichen

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Betroffenenrechte

- Auskunftsrecht (Art 15)
- Recht auf Berichtigung und Löschung („Recht auf Vergessenwerden“; 17)
- Widerspruchsrecht (Art 21)
- Verbot von automatisierten Einzelentscheidungen („Profiling“; Art 22)
- *Recht auf Einschränkung der Verarbeitung* (Art 18)
- *Recht auf Datenübertragbarkeit* („Portabilität“; Art 20)
- umfassende Informationspflichten des Verantwortlichen (Art 13f)

Datenschutz durch Technik (Art 25)

- „privacy by design“ & „privacy by default“
- technische und organisatorische Maßnahmen, z.B. Pseudonymisierung
- *Voreinstellung* in Produkten, um Zweckbindung und Datensparsamkeit zu gewährleisten
- *Konzepte zum Löschen*
- Zugriffseinstellungen
- *Zertifizierungsverfahren* als Nachweis möglich

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Verarbeitungsverzeichnis (Art 30)

- wenn >250 MA
- wenn Risiko für Rechte von Personen
- wenn Profiling
- wenn besondere Datenkategorien umfangreich verarbeitet werden
- wenn strafrechtlich Relevantes
- Inhalte: Name, Zweck, Kategorien, Empfänger, *Löschfristen*, Sicherheitsmaßnahmen
- Muss der Behörde vorgelegt werden

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Technische und organisatorische Maßnahmen (=TOM: Art 32)

- je nach Datenart und Umfang, Zweck und Risiko, *Eintrittswahrscheinlichkeit, Kosten und Stand der Technik*
- *Pseudonymisierung und Verschlüsselung*
- Wiederherstellen nach Zwischenfall
- *Regelmäßige Überprüfung und Evaluierung*
- kann auch in *Verhaltensregeln/ Zertifizierung* festgelegt sein

Meldung einer Datenschutzverletzung (Art 33)

→ Behörde (binnen 72 h) (Art 33)

→Betroffene (unverzüglich) (Art 34)

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Folgenabschätzung (Art 35f)

- wenn Risiko für Rechte von Personen
- wenn automatisierte Einzelentscheidung bzw. Profiling stattfindet
- wenn besondere Datenkategorien umfangreich verarbeitet werden
- wenn öffentlicher Bereich überwacht wird
- Rat des betriebl. Datenschutzbeauftragten
- **Betroffene bzw. deren VertreterInnen müssen Standpunkt abgeben**
- MUSS-Inhalte: Zweck, Notwendigkeit, Verhältnismäßigkeit, Risikobewertung, geplante Maßnahmen zur Abhilfe
- bei Risiko → Vorab-Konsultation der Behörde
- Behörde muss Auskunft erhalten
- Behörde erstellt Liste (DSFA-AV DSFA-V)

Datenschutzbeauftragte/r (Art 37ff.)

- Verpflichtend einzuführen, wenn
  - Behörde
  - Kerntätigkeit umfangreiche Datenverarbeitung mit regelmäßiger u. systematischer Beobachtung von Personen
  - Kerntätigkeit besondere Kategorien von Daten umfasst
- innerbetrieblich oder extern
- Unterrichtung und Beratung
- Überwachung der DSGVO
- Sensibilisierung und Schulung
- AnsprechpartnerIn für Datenschutz-Behörde
- berufliche Qualifikation und Fachwissen erforderlich
- Wahrung der Geheimhaltung und Vertraulichkeit
- Mitarbeit bei Datenschutzfolgenabschätzung und (allfälliger) Vorab-Konsultation

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Datenverarbeitung in Drittstaaten

- *Verhaltensregeln* f. Unternehmen/ Branchen (Art 40f)
  - freiwillige Selbstverpflichtung
  - selbst erarbeitet
  - Genehmigung u. Veröffentlichung durch DS-Behörde
- *Zertifizierung* (Art 42f)
  - DS-Behörde akkreditiert eigene Zertifizierungsorganisationen
- *interne Datenschutzvorschriften* f. Konzerne (Art 47)
  - enthalten durchsetzbare Rechte für Betroffene
  - Genehmigung durch DS-Behörde
  - Schulungen für Personal verpflichtend
- Standarddatenschutzklauseln (Art 48 Abs 2c)
- Angemessenheitsbeschluss (Art 45)

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

„One-stop-shop"

- *Verantwortlicher für DS in EU* muss benannt werden
- *Hauptniederlassung* muss benannt werden
- Aufsichtsbehörde der Hauptniederlassung in allfälligen Auseinandersetzungen federführend (Art 56)
- Behörde im jeweils betroffenen Mitgliedstaat hat Überwachungsbefugnisse (Art 57-58)
- Enge Zusammenarbeit zwischen den Behörden geboten (Art 60-62)
- *Kohärenzverfahren* zur einheitlichen Rechtsanwendung (Art 63-67)

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Haftung und Geldbußen (Art 83)

- wirksam, verhältnismäßig & abschreckend
- bis zu ***20 Mio. EUR*** *od.* ***4 %*** *des weltweiten Umsatzes*
  - Art, Schwere und Dauer des Verstoßes?
  - frühere Verstöße?
  - fahrlässig oder vorsätzlich?
  - Welche Datenarten?
  - Wie viele Betroffene?
  - Wurden Maßnahmen zur Abhilfe getroffen?
  - Wurde die Behörde involviert?
  - Wurden (allfällig vorhandene) interne Richtlinien eingehalten?

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Datenverarbeitung im Beschäftigungskontext (Art 88+EWG 155)

- „Öffnungsklausel“: spezifischere Vorschriften durch Gesetz oder Kollektivvereinbarungen
  (= Betriebsvereinbarungen) möglich
- *„zur Wahrung der menschlichen Würde der berechtigten Interessen und der Grundrechte“*
- Beispiele:
  - Transparenz
  - Übermittlung personenbezogener Daten innerhalb des Unternehmens/ Konzerns
  - Überwachungssysteme

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Datenverarbeitung im Beschäftigungskontext 2

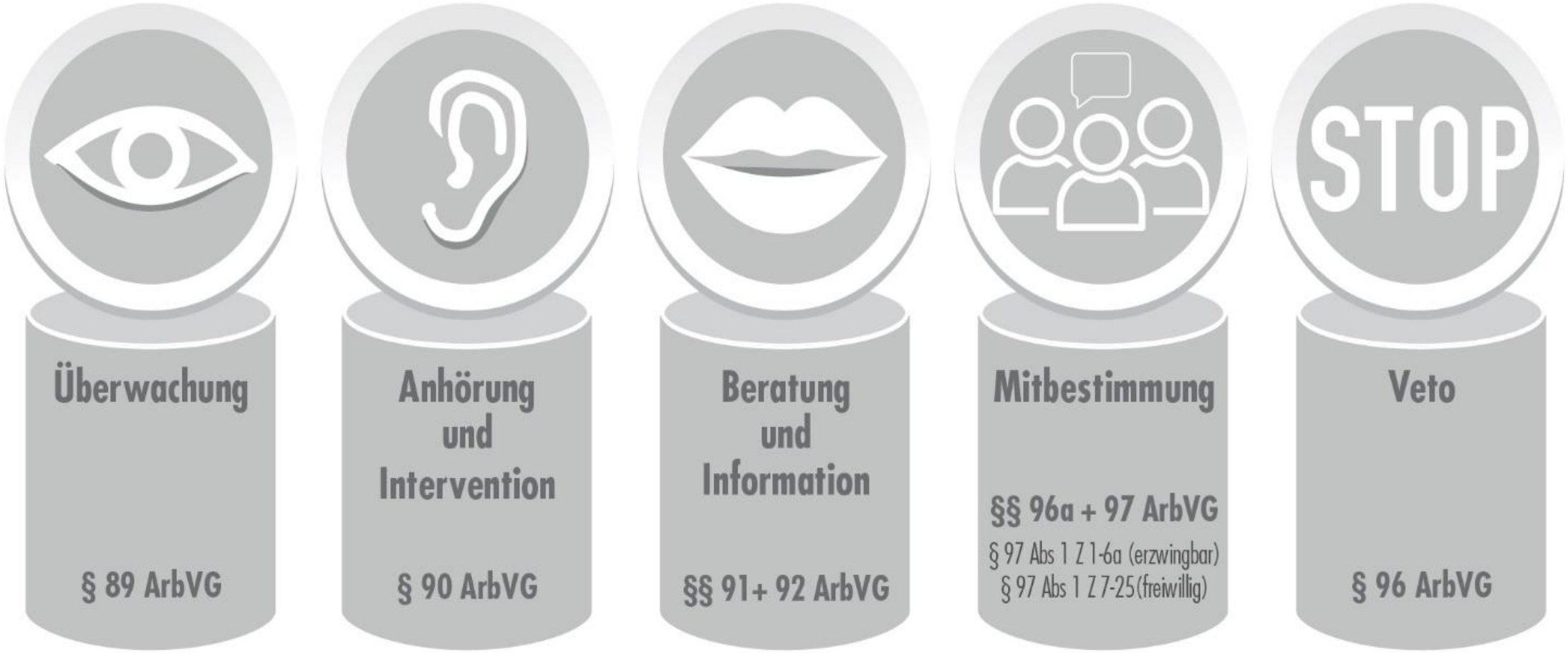
„insbesondere für Zwecke der“:

- Einstellung, Beendigung des Arbeitsverhältnisses
- Erfüllung des Arbeitsvertrages
- Planung der Arbeit
- Gleichheit und Diversität
- Sicherheit und Gesundheit
- Schutz des Eigentums

ArbVG ist notifiziert

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Rechte des Betriebsrats



GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

BR-Rechte gemäß ArbVG

1. Anhörung und Intervention (§ 90 ArbVG)
2. Information (§ 91 ArbVG insbes Abs 2)
3. Beratung (§ 92 ArbVG)
4. **Mitbestimmung → Betriebsvereinbarung**
    1. Veto (§ 96 ArbVG)
        1. Personalfragebögen (nicht nur allg. Angaben)
        2. Kontrollmaßnahme, die die Menschenwürde berührt)
    2. Ersetzbare Zustimmung durch Schlichtungsstelle (§ 96a ArbVG)
        1. Systeme mit personenbezogenen AN-Daten
        2. Beurteilungssysteme
        3. Nutzung der Betriebsmittel (§ 97 Z 1 Abs 6)
    3. „Freiwillig“ bzw. fakultativ (§ 97 ArbVG)
        1. Benützung von Betriebsmitteln (Z 6)
        2. Menschengerechte Arbeitsgestaltung (Z 9)
        3. Sicherung von Gegenständen der AN (Z 17)
        4. Betriebliche Bildungsmaßnahmen (Z 19)

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Die betriebliche Umsetzung
16-01-20

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Grundrechte

„Jeder Mensch hat angeborne, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten.“
(§ 16 ABGB; seit 1.1.1812)

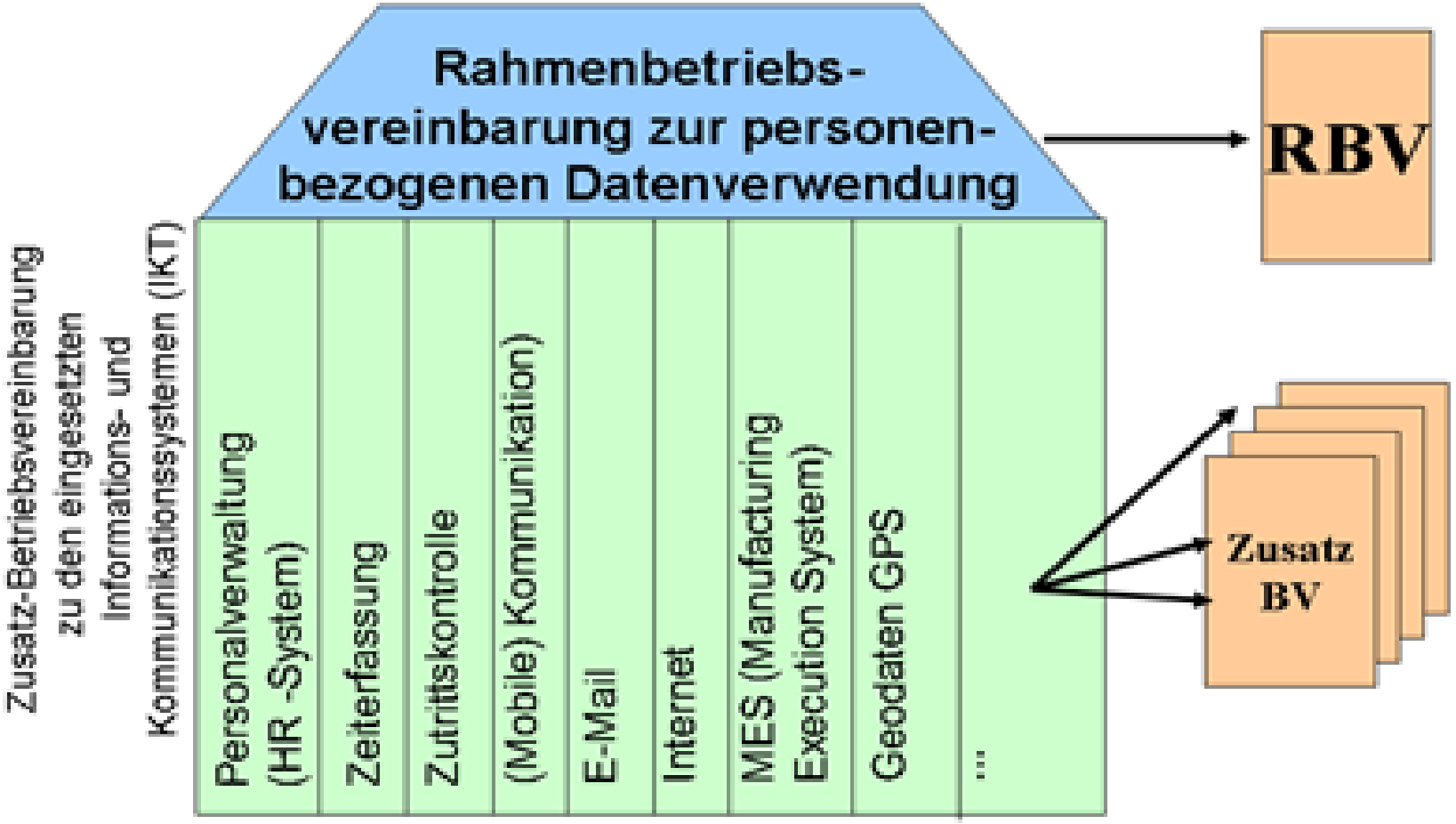
„…an employer’s instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.”
(EGMR am 5.9.2017)

Ist die BV auf die DSGVO abgestimmt?

- Zweckbindung und Datensparsamkeit/Löschregelungen
- Datenschutz-Folgenabschätzung
- Datenschutz durch Technik
- Sicherheitsvorkehrungen
- Evaluierung der TOM
- Betriebliche/r Datenschutzbeauftragte/r
- Verarbeitungsverzeichnis – inkl. Einsicht des BR
- Benachrichtigung bei DS-Verletzungen – auch an den BR
- Rechtsgrundlage Einzelzustimmung
- Rechtsgrundlage für Datenübermittlung in Drittländer
- Profiling

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

RBV und IKT-Zusatzvereinbarung(en)



Vor- und Nachteile der Rahmen-BV

- einheitliche Vorgangsweise im Betrieb
- grundlegend
- die Mitbestimmungskultur wird geklärt
- Rechtsgrundlage?
- AG hat zunehmend Interesse (vermutl. DSGVO?)
- AG wollen oft „Super-BV“ (mit Blanko-Zustimmung)
- Ausarbeitung und Aushandlung ist zeitintensiv
- langfristig gesehen Arbeits- und Zeitersparnis

→ bewusste Entscheidung innerhalb der BR-Körperschaft

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Stufenweise Kontrollverdichtung

- Stufe 1: IT-Abt. fordert betroffenen Personenkreis (ohne Personenbezug) auf, Fehlverhalten einzustellen
- Stufe 2: Der/die einzelne wird von IT-Abt. aufgefordert
- Stufe 3: Offenlegung der personenbezogenen Daten gegenüber dem/r Vorgesetzten unter Hinzuziehung des BR; Gespräch mit Vorgesetztem/r (wenn noch immer Fehlverhalten vorliegt: ev. Sanktion nach vorheriger Beratung mit dem/r BR)

Stufe 1 und 2 können nur bei Fällen einer **konkreten unmittelbaren Gefährdung der IKT-Infrastruktur** bzw. bei begründeten Verdacht eines **Verstoßes gegen strafrechtliche Bestimmungen** übersprungen werden.

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Mitstreiter*innen

- Kolleg*innen
- Betriebliche*r Datenschutzbeauftragte*r
- ZBR/ EBR
- HR-Abteilung
- IT-Abteilung
- Rechtsabteilung
- Gewerkschaft
- Arbeiterkammer
- Datenschutzbehörde
- Arbeitsinspektorat, Allgemeine Unfallversicherung
- Kund*innen/ Klient*innen
- Geschäftspartner*innen

Kennzeichen einer guten Betriebsvereinbarung

- Beschränkung des Zweckes
- Beschränkung der Quantität
- Beschränkung der Weitergabe
- festgelegte Speicherzeit
- klare Zuständigkeit (z.B. Ansprechpersonen)
- klare Abläufe (z.B. „Stufenweise Kontrollverdichtung“,…)
- Bekanntheit (z.B. Schulung,…)
- Einhaltung (z.B. Evaluierung,…)

Info für Betriebsrät*innen

Gute Arbeit!

Anlage zu § 9 BDSG:

Die acht Gebote zum Datenschutz

1. Zutrittskontrolle	Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verar-beitet oder genutzt werden, zu verwehren.
2. Zugangskontrolle	Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
3. Zugriffskontrolle	Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
4. Weitergabekontrolle	Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
5. Eingabekontrolle	Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem per-sonenbezogene Daten in Datenverarbeitungssyste-me eingegeben, verändert oder entfernt worden sind.
6. Auftragskontrolle	Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
7. Verfügbarkeitskontrolle	Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
8. Getrennte Verarbeitung	Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Wesentliche BV-Inhalte

- Datenminimierung ← Zweckbindung ← Zielsetzung
- Transparenz: welche Auswertungen werden wozu erstellt/ weitergeleitet/ eingesehen?
- Speicherdauer: wie lange werden Daten/-kategorien jeweils aufgebhoben?
- BR-Rechte (Einsicht, Beratung, Mitbestimmung)
- Betroffenenrechte (Auskunft, Löschen, Einschränken, Richtigstellen, Widerruf)
- Vorgehensweise im Verdachtsfall (Definition, „stufenweise Kontrollverdichtung“)
- Ansprechpersonen (ev. interne DS-Kommission)
- Evaluierung (z.B. jährlich)

Datenverarbeitung im Büro

- Vorgehensweise + Zuständigkeiten im BR regeln
- Ist der BR Verantwortlicher im Sinne der DSGVO?
- Von wem stammen die Daten? (z.B. AG, AN)
- Über wen sind die Daten? Wer sind die Betroffenen? (z.B. aktive/ ausgeschiedene AN, Angehörige, Externe,…)
- An wen werden die Daten weitergegeben? (z.B. Apotheke, Reiseveranstalter,…)
- Wie sind die Daten gesichert?
- Gibt es eine regelmäßige Aktualisierung?

Unterstützung der GPA-djp für BetriebsrätInnen

- Seminare/ Workshops/ Referate
- betriebliche Fallberatung mit den Regionalen BetriebsbetreuerInnen
- Externer Berater*innen-Pool aus IT-Expert*innen
- Materialien (Checkliste DSGVO, Muster-Rahmen-BV, Broschüre „DS-GVO aus AN-Sicht“, Flyer, Muster für Verarbeitungsverzeichnisse, etc.)
- Informationen am Blog http://arbeitundtechnik.gpa-djp.at/

Gute Arbeit!

Es gibt vieles,

für das es sich lohnt,

organisiert zu sein.