Datenschutz – (k)ein Buch mit sieben Siegeln
Schöneberger Forum 2022

Berlin, 9.11.2022

Sebastian Baunack
Fachanwalt für Arbeitsrecht und
Verwaltungsrecht

Tag 1

Datenschutz im Personalratsbüro

Übersicht

- Einführung: wie steht es um den Datenschutz in der Dienststelle und im Personalrat?
- Warum ist der Datenschutz wichtig für den Personalrat?
  - Rechte des Personalrats und Datenschutz
- Die EU-Datenschutzgrund Verordnung
- Wer ist für den Datenschutz verantwortlich?
- Grundbegriffe und Grundsätze des Datenschutzes -DS-GVO und BDSG
- Grundlagen des Datenschutzes in der Dienststelle und im Personalrat
- Der betriebliche Datenschutzbeauftragte
- Einzelheiten des Datenschutzkonzepts des Personalrats

Bestandsaufnahme

- Gibt es eine Vereinbarung / Absprache über den Datenschutz im Personalrat mit dem Dienststellenleiter / dem Datenschutzbeauftragten?
  - Wenn ja, wie sieht die aus?

Worum geht es beim Datenschutz?
Was soll Datenschutz noch?

Was soll eigentlich Datenschutz noch?

- **Offenheit in den sozialen Medien**
- **Big Data?**
- **Ich hab nichts zu verbergen?**
- **Kontrollen im Betrieb?**

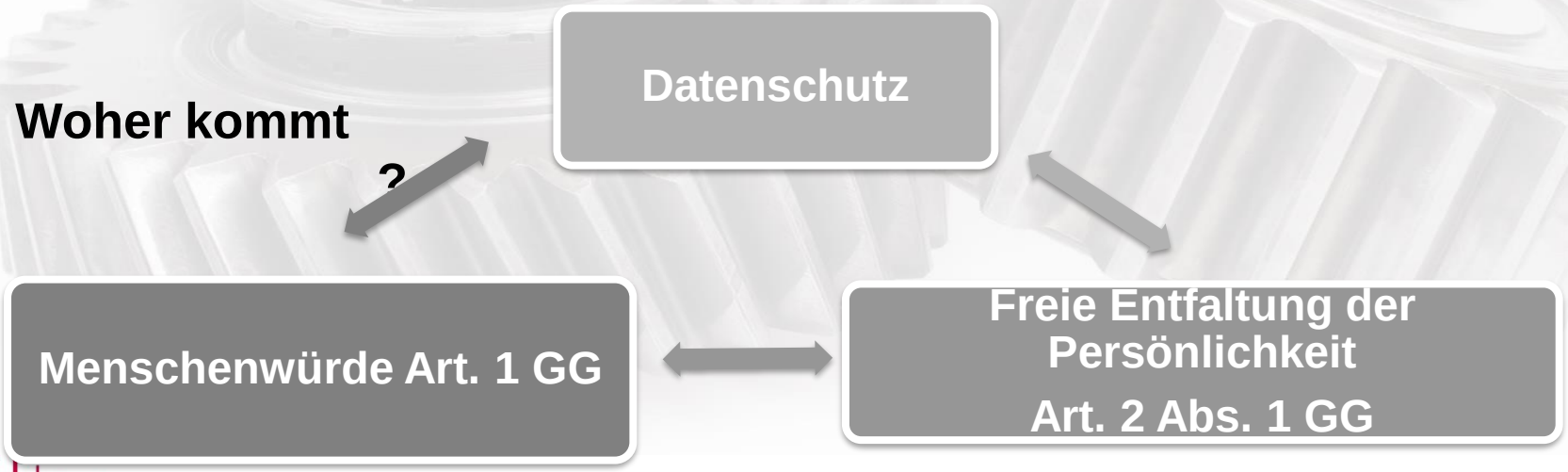
Was ist Datenschutz?

Recht auf informationelle Selbstbestimmung

(Bundesverfassungsgericht 1983 –Volkszählungsurteil) =

– Selbst zu entscheiden, was man über sich preisgibt!!

Woher kommt ?



Warum eine EU-Datenschutzgrundverordnung?

- Schon lange EU-Regelungen zum Datenschutz
  - Problem: Umsetzung in den einzelnen Mitgliedsländern sehr unterschiedlich
  - Mehr grenzüberschreitende Datenverarbeitung
  - keine Harmonisierung auf hohem Niveau
- Ziel einer Verordnung zu Datenschutz in der EU
- EU-Binnenmarkt soll gefördert werden
  - Beginn der Vorarbeiten im Jahr 2000

Gesetzgebungsverfahren

- Entwurf für Verordnung durch Kommission 2012
- Verhandlungen und Beratungen sog. Trilog Gespräche Kommission, EU-Rat (=Vertreter der nationalen Regierungen) und EU-Parlament 2015
  - Verordnung in Kraft getreten 25.05.2016
- VO tritt in allen Mitgliedsländern in Kraft am 25.5.2018
  - Vorher: Überarbeitung Bundesdatenschutzgesetz mit Anpassung an EU-DS-GVO, 2017 verabschiedet, trat zum 25.5.2018 in Kraft

Verhältnis EU DS-GVO und nationales Recht

- EU-Verordnung ist bindendes, unmittelbar geltendes Recht in allen Mitgliedsstaaten der EU
  - DS-GVO gilt ab 25.5.2018 zwingend
- DS-GVO enthält Öffnungsklauseln für nationales Recht
  - Öffnungsklauseln sind z.T. mit Vorgaben versehen, die die nationalen Umsetzungsgesetze einhalten müssen
  - Geändertes, neues Bundesdatenschutzgesetz, gilt ab 25.5.2018

Grundkonzeption der EU-DS-GVO

- Marktortprinzip
  - Regeln gelten für alle Unternehmen, die in der EU tätig sind, unabhängig vom Heimatland
- Verfahrensvereinfachung und einheitliche Rechtsanwendung - One-Stop-Shop - Kohärenzverfahren.
  - Unternehmen klären mit Behörden am Hauptsitz in der EU Datenschutzprobleme bei grenzüberschreitender Verarbeitung, Einbeziehung der Behörden der anderen Länder
  - EDSA Europäischer Datenschutzausschuss soll für einheitliche Anwendung der DS-GVO sorgen

Organisation des Datenschutzes

Datenschutzbeauftragter

- Behördlicher Datenschutzbeauftragter Art. 37 Abs. 1 a) DSGVO
- Bisherige Vorabkontrolle durch Datenschutzbeauftragten wird ersetzt durch Datenschutzfolgenabschätzung nach Art. 35
- Verantwortlicher muss Datenschutzfolgenabschätzung durchführen; berät sich mit Datenschutzbeauftragtem

Durchsetzung des Datenschutzes

- Betonung der Verantwortung der Verantwortlichen Stelle
- Behörden können
  - Verwarnungen oder
  - Anweisungen erteilen
  - Untersagung oder Beschränkung von Datenverarbeitung
- wesentlich erhöhte Bußgelder verhängen
  - Orientierung am Verfahren bei Kartellverstößen
  - Höhe je nach verletzter Vorschrift bis zu 10 bzw. 20 Mio. € oder bei Unternehmen von bis zu 2 oder 4 % des weltweit im Vorjahr erzielten Jahresumsatzes (nicht Gewinn; Art 83 DS-GVO) Umsatzes
  - EDSA und Datenschutzbeauftragte der Bundesländer haben Bußgeldleitlinien erlassen
- Schadensersatzansprüche von Geschädigten (§ 83 BDSG)

Durchsetzung des Datenschutzes

- Aber: Keine Bußgelder gegen öffentliche Stellen (§ 43 Abs. 3 BDSG)

Die Rolle des Personalrats nach der DSGVO

- Datenschutzregeln gelten auch für den Personalrat!
- Wer kontrolliert den Personalrat in Datenschutz-fragen?
  - Der Dienststellenleiter?
  - Der behördliche Datenschutzbeauftragte?
  - Die Aufsichtsbehörde?
  - Der Personalrat selbst?

Personalrat und Datenschutzbeauftragter vor der DS-GVO

- Grundsatzentscheidung des BAG 1997 zum BetrVG
- → interessant auch für Personalvertretungen.

Personalrat und Datenschutzbeauftragter vor der DS-GVO

»BAG Entscheidung 1997:

- Die nach § 36 Abs. IV BDSG bestehende Verschwiegenheitspflicht ist, wie das LAG zutreffend erkannt hat, ebenfalls nicht geeignet, dem Datenschutzbeauftragten im Spannungsverhältnis zwischen Arbeitgeber und Betriebsrat eine neutrale Position zu verschaffen. Sie ist auf die Identität des von der Datenverarbeitung Betroffenen beschränkt. Daten, die den Meinungsbildungsprozeß des Personalrats betreffen, bleiben weitgehend außerhalb der Verschwiegenheitspflicht. Gerade deren Geheimhaltung ist aber erforderlich, soweit es um die Gewährleistung der Unabhängigkeit des Personalrats vom Arbeitgeber geht.

Personalrat und Datenschutzbeauftragter vor der DS-GVO

»BAG Entscheidung 1997:

- Selbst wenn man der Auffassung folgen wollte, daß die Verschwiegenheitspflicht über den Gesetzeswortlaut hinaus generell auch auf alle Daten des Personalrats zu erstrecken ist, erschiene die praktische Wirksamkeit des Schutzes noch zweifelhaft. Die in den §§ 43, 44 BDSG vorgesehenen Sanktionen gelten nämlich nicht für die Verletzung der Verschwiegenheitspflicht durch den Datenschutzbeauftragten. Zivilrechtliche Sanktionsnormen, die insoweit von den Trägern betroffener Persönlichkeitsrechte herangezogen werden können, kommen für den Betriebsrat regelmäßig nicht in Betracht.

Personalrat und Datenschutzbeauftragter vor der DS-GVO

»BAG Entscheidung 1997:

» Die Anwendung von §§ 36, 37 BDSG in der geforderten Weise würde dazu führen, daß dem Arbeitgeber eine Verantwortung für die Rechtmäßigkeit der Amtsausübung des Betriebsrats erwüchse, die ihm nach dem Betriebsverfassungsgesetz nicht zukommt . Das in diesem Zusammenhang vorgetragene Argument, der Arbeitgeber müsse sich davor schützen können, daß er von Betroffenen wegen Gesetzesverstößen des Personalrats in Haftung genommen werde, verfängt nicht.

Personalrat und Datenschutzbeauftragter vor der DS-GVO

»BAG-Entscheidung 1997:

» Dem LAG ist allerdings darin zu folgen, daß der Betriebsrat nicht etwa als „Dritter" im Sinne des BDSG außerhalb der „speichernden Stelle" im Sinne des § 3 Abs. VII BDSG, also des Unternehmens steht. Vielmehr ist er selbst Teil dieser speichernden Stelle. Das entspricht heute hinsichtlich der Betriebsräte wohl allgemeiner Meinung (…).

Personalrat und Datenschutzbeauftragter vor der DS-GVO

»BAG-Entscheidung 1997:

» **Die Zugehörigkeit des Betriebsrats zur speichernden Stelle ergibt sich daraus, daß im nicht-öffentlichen Bereich Stellen im Sinne des Bundesdatenschutzgesetzes nur natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts sind.** Zu diesen gehören Betriebsräte nicht.

Anforderungen an Datenschutz im PR

- PR = verantwortliche Stelle?
  - „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“
    - Art 4 Ziffer 7 DS-GVO

Personalrat Verantwortlicher nach der DSGVO?

- **Was wäre die Konsequenz?**
  - Der Personalrat müsste ein eigenes Verarbeitungsverzeichnis führen, er müsste zudem einen eigenen Datenschutzbeauftragten ernennen, er müsste Auskunftsansprüche der Arbeitnehmer erfüllen.
  - Vor allem aber: Er wäre nach Art. 83 DSGVO bußgeldpflichtig!
  - Und nach § 83 BDSG schadensersatzpflichtig!

Personalrat Verantwortlicher nach der DSGVO?

- **§ 83 BDSG Schadensersatz und Entschädigung**
- Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet.

Personalrat Verantwortlicher nach der DSGVO?

	Alt	Neu
Leichter Verstoß	Bis 50.000 €	Bis 10 Mio./ 2 % Jahresumsatz weltweit
Schwerer Verstoß	Bis 300.000 €, wenn nötig ausnahmsweise mehr	Bis 20 Mio./4 % Jahresumsatz weltweit
	§ 43 Abs. 3 BDSG	Art. 83 Abs. 4-6 DSGVO

Einhaltung der Grundsätze „Verantwortlicher“

- Verantwortlicher ist für die Einhaltung der Grundsätze verantwortlich und muss deren Einhaltung nachweisen können
  - (Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)
- Streit, ob Personalrat Verantwortlicher ist oder nicht?
  - Folgen für Haftung, Verarbeitung, Übermittlung

§ 69 BPersVG:

Bei der Verarbeitung personenbezogener Daten hat der Personalrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Personalrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist die Dienststelle der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Die Dienststelle und der Personalrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften.

Rechte des BR – Datenschutz

- Streit, ob PR datenschutzrechtlich „Verantwortlicher“ ist oder nicht hat Gesetzgeber in Juni 2021 entschieden
  - Rechtlich gibt es Zweifel, ob das den Vorgaben der DS-GVO entspricht
  - Für die Praxis ist § 69 BPersVG bzw. LPersVG maßgebend

Rechte des BR – Datenschutz

- Interessant ist die Abweichung zu § 79a BetrVG. Die folgenden Sätze fehlen im BPersVG:
- *Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. § 6 Absatz 5 Satz 2, § 38 Absatz 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber.*

Rechte des BR – Datenschutz

- Heißt das, das der betriebliche Datenschutzbeauftragte den Betriebsrat kontrollieren darf, aber nicht der behördliche Datenschutzbeauftragte den Personalrat?

Rechte des BR – Datenschutz

- In jedem Fall gilt:

- Der PR muss demnach bei seiner Arbeit die Maßgaben der DSGVO und des BDSG einhalten.

Rechte des BR – Datenschutz

- Vorsicht: Gerade bei hochsensitiven Daten nach Art. 9 DSGVO kann die Dienststellenleitung ggf. die Weiterleitung an den PR verweigern, wenn der PR kein schlüssiges Datenschutzkonzept vorweisen kann.

Rechte des BR – Datenschutz

- Hierzu die aktuelle Rechtsprechung zum BetrVG, welche auf den PersVG übertragbar sein könnte:

- LAG BW v. 20.5.2022 – 12 TaBV 4/21
- BAG v. 9.4.2019 – 1 ABR 51/17

Rechte des BR – Datenschutz

- Welche datenschutzrechtlichen Vorgaben muss der PR demnach bei seiner Amtstätigkeit sicherstellen?

Grundsätze des Datenschutzes – Art. 5 DS-GVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Grundregeln – DS-GVO

- Übermittlung in Drittstaaten (Art. 45 DSGVO; Angemessenes Schutzniveau im Drittland, EU Kommission)
- Betroffenenrechte (Auskunft, Transparenz; Einwilligung, Berichtigung; Löschung)
- Unabhängige Aufsicht
- Effektive Durchsetzung
  - Weitgehende Befugnisse der Aufsichtsbehörden.

Grundbegriffe des Datenschutzrechts

- **Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Grundbegriffe des Datenschutzrechts

- **„ 8. Auslesen**
- Auslesen von personenbezogenen Daten (in der englischen Übersetzung „retrieval“) hat eine doppelte Bedeutung. Auslesen liegt zum einen vor, wenn die Daten der **Sehfunktion** eines Menschen zugänglich gemacht werden. Sie werden dafür auf einem Display oder einem anderen Endgerät sichtbar gemacht. Zum anderen kann unter Auslesen auch verstanden werden, Daten aus einem Datenträger auszulesen, um sie einer weiteren Bearbeitung zugänglich zu machen.“
- Simitis/Hornung/Spieker Datenschutzrecht Art 4 Rn. 22

Grundbegriffe des Datenschutzrechts

- **„personenbezogene Daten“** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
-

Grundbegriffe des Datenschutzrechts

» § 26 BDSG Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

» Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung **oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich** ist.

Auskunftsrecht der betroffenen Person - Art 15 DS-GVO

- Information über:
  - Verarbeitungszwecke
  - Kategorien
  - Empfänger von Daten, insbesondere in Drittländern
  - Geplante Dauer der Speicherung
  - Information über Recht auf Berichtigung bzw. Löschung
  - Herkunft der Daten, wenn keine Direkterhebung
  - über evtl. automatisierte Entscheidungsfindung
- Frist in der Regel ein Monat nach Eingang des Antrags (Art. 12 Abs. 2 DS-GVO)

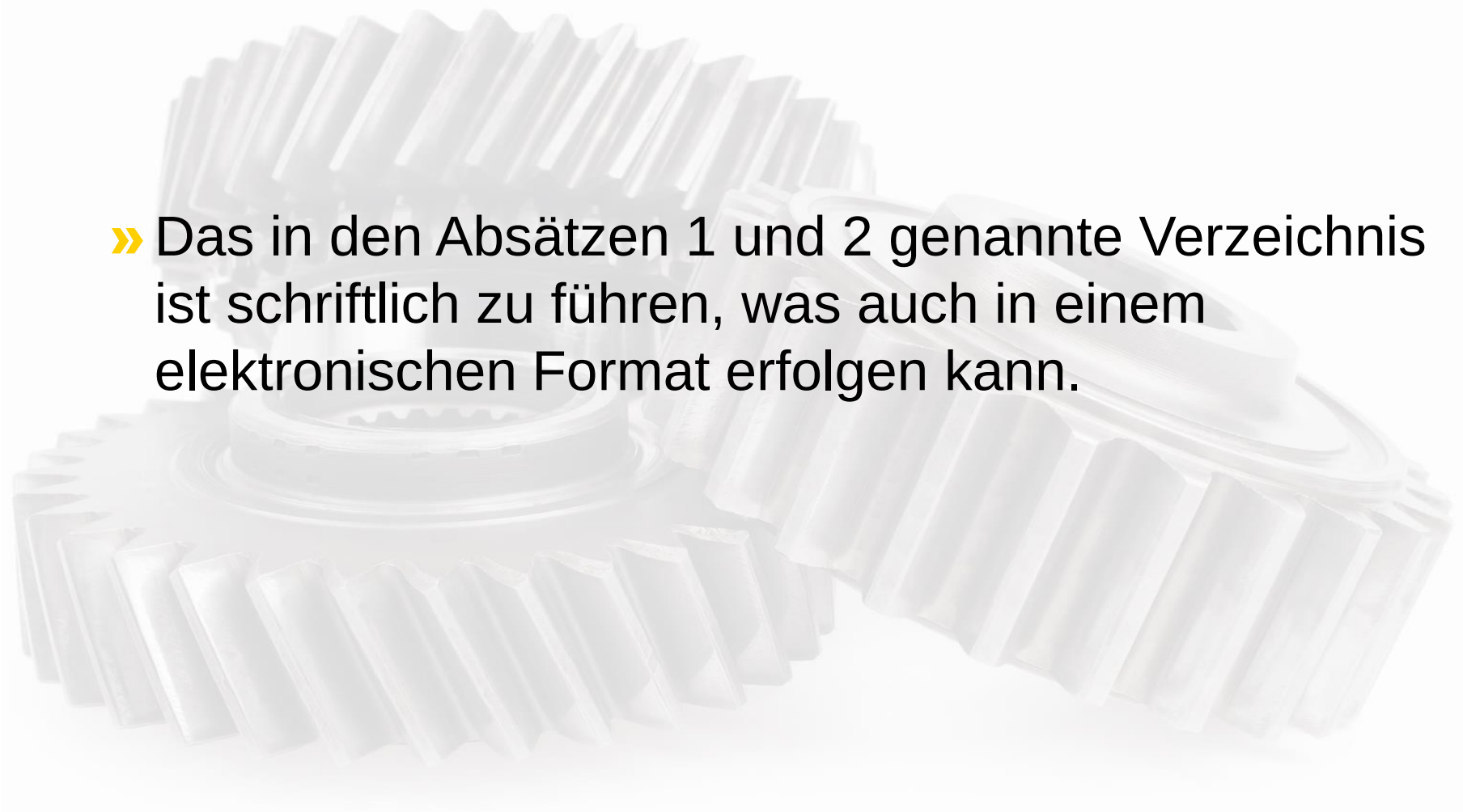
Verzeichnis von Verarbeitungstätigkeiten

- Notwendig für
- a.) den Überblick wer, was wofür und wie verarbeitet
- b.) Basis für Auskunftsverlagen
- d.) Löschung von Daten – setzt ja voraus, das man weiß wo sich Daten befinden
- c.) Prüfung durch den Landesdatenschutzbeauftragten – dieser kann Vorlage verlangen

Verzeichnis von Verarbeitungstätigkeiten
Art. 30 DS-GVO

- Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
  - den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
  - die Zwecke der Verarbeitung;
  - eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
  - die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
  - gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
  - wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
  - wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Verzeichnis von Verarbeitungstätigkeiten
Art. 30 DS-GVO



- Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

Aufgabe

- Erstellt ein konkretes Verzeichnis von Verarbeitungstätigkeiten für Euren Personalrat für jeden Verarbeitungsvorgang
  - Sammelt zunächst das was ihr routinemäßig speichert, z.B. im Rahmen von Anhörungen
  - Welche Daten speichert Ihr wo, wie, warum?
  - Wenn Ihr bei bestimmten Daten nicht wisst, welche Daten ihr habt, erstellt bitte eine Liste mit zu klärenden Fragen – dies könnt Ihr dann bei Rückkehr in die Dienststelle abarbeiten
- Stellt Eurer Ergebnis bitte mit einer Wandzeitung vor

Verzeichnis von Verarbeitungstätigkeiten
Art. 30 DS-GVO

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DS-GVO

Verarbeitungstätigkeit: Benennung: _____	**lfd. Nr.:** _____
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐

Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DS-GVO

Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) ☐ Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine inter-nationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8*

..... Verantwortlicher ..... Datum ..... Unterschrift

Verzeichnis von Verarbeitungstätigkeiten
Art. 30 DS-GVO

- Im Rahmen der Mitbestimmungsaufgaben nimmt der Personalrat Kontroll- und Zustimmungsaufgaben wahr. Bei personellen Angelegenheiten (Einstellung, Beschäftigung, Beendigung, Lohn- u Gehaltsgefüge) verarbeitet der Personalrat personenbezogene Daten. Ergebnisse und Entscheidungen werden dokumentiert.

Zwecke der Datenverarbeitung im Personalrat

Prüffrage: Welche Zwecke könnten bzgl. einzelner Beschäftigtendaten vorliegen?

GRUNDDATEN ÜBER BESCHÄFTIGTE

Personenbezogene Daten	**Beispiele für einen Aufgabenbezug**
Name, Vorname	
Vollzeit-/Teilzeitbeschäftigung	
Einsatztätigkeit	
Organisatorische Zugehörigkeit	
Geburtsdatum	
Art der Beschäftigung (Befristung, Leiharbeit)	
Qualifikation	
Privatadresse (je nach Betrieb)	
Grundlegende Informationen zu familiären Verhältnissen über freiwillige Abfragen	
Bei Eintreten: namentliche Mitteilung einer Schwangerschaft[9]	
Bei Eintreten: Berechtigung zu einem Betrieblichen Eingliederungsmanagement	

Zwecke der Datenverarbeitung im Personalrat

Prüffrage: Welche Zwecke könnten bzgl. einzelner Beschäftigtendaten vorliegen?

GRUNDDATEN ÜBER BESCHÄFTIGTE

Personenbezogene Daten	**Beispiele für einen Aufgabenbezug**
Name, Vorname	Überwachung der Einhaltung von gesetzlichen Vorschriften wie den arbeitsschutzrechtlichen Vorschriften. Unterscheidung eigener von fremden Beschäftigten.
Vollzeit-/Teilzeitbeschäftigung	Personalplanung, Personalbedarfsplanung, Weiterbildung
Einsatztätigkeit	Abgleich mit eventuell bestehender Stellenbeschreibung, Personalbedarfsplanung, personelle Einzelmaßnahme
Organisatorische Zugehörigkeit	Relevant bei Personalratswahl insbesondere bei Matrixstrukturen, Betriebsvereinbarungen, Entsendungen
Geburtsdatum	Personal-/Personalbedarfsplanung, Demographieanalyse, Personalratswahl
Art der Beschäftigung (Befristung, Leiharbeit)	Personalplanung, Beschäftigungssicherung, Weiterbildung, personelle Einzelmaßnahme
Qualifikation	Personelle Einzelmaßnahme, Personalentwicklung, Beschäftigungssicherung, Interessenausgleich/Sozialplan
Privatadresse (je nach Betrieb)	Versetzung und Ähnliches (Benachteiligung, Grenzgängerthematik), Gebietsveränderung Außendienst und Anfahrt; Kommunikation des BR mit den Arbeitnehmern
Grundlegende Informationen zu familiären Verhältnissen über freiwillige Abfragen	Weiterbildung, zwingende Mitbestimmung §§ 87 Abs. 1 Nr. 2 (Arbeitszeiten), Nr. 8 BetrVG (Sozialeinrichtungen, Krippe, Zuschuss), freiwillige Vereinbarungen (Pflege, Unterstützung Alleinerziehender)
Bei Eintreten: namentliche Mitteilung einer Schwangerschaft[9]	Individuelle Gefährdungsbeurteilung aus §§ 10 Abs. 2, 9 Abs. 1 Satz 2 MuSchG mit Blick auf Art. 6 Abs. 2 d RL 89/391/EWG[10]
Bei Eintreten: Berechtigung zu einem Betrieblichen Eingliederungsmanagement	Überwachung der Einhaltung von § 167 SGB IX

Zusammenarbeit PR und Datenschutz beauftragter

- Rolle und Aufgabe des Datenschutzbeauftragten
- Bestellung
  - Mitbestimmung des PR?
- Rechte des DSB
- Abberufung
- Zusammenarbeit DSB Aufsichtsbehörden
- Stellung im Verhältnis zum Dienststellenleiter?
- Unterschied intern – extern?

Mailverkehr - Aufgabe

- Stellt bitte für Euren Personalrat zusammen, wie mit Mails im PR umgegangen wird
  - Einladungen zu Sitzungen
  - Unterlagen zur Tagesordnung
  - Zugriff auf E-Mails mit personenbezogenen Daten im Rahmen der PR-Arbeit
  - Wer hat Zugriff auf die Mails?
  - Stellvertretungen?
  - Zugriff im Krankheitsfall?
- Was sagt Eure Unternehmens-Richtlinie zum Mailverkehr aus?
- Inhalte, Privatnutzung, Schutz, Passwörter

Mailverkehr

- Technik stellt die Dienststelle
- Die Dienststelle (verantwortliche Stelle) hat die Anforderungen der DS-GVO zum Schutz personenbezogener Daten beim E-Mail-Verkehr generelle sicherzustellen
- Anforderungen an die Technik
  - DS-GVO
  - z.B: Orientierungshilfe des Arbeitskreises „Technisch und organisatorischen Datenschutzfragen“ der Datenschutzkonferenz
  - Verschlüsselung usw.

Mailverkehr

- Zugriff auf Mails des Personalrats?
  - Wo werden Mails gespeichert?
  - Wird ein Backup der Mails erstellt im Betrieb?
  - Wenn ja wo, wie was?

Mailverkehr - Aufgabe

- Entwerft bitte eine interne Richtlinie für den Umgang mit Mails und die Speicherung von Daten und den Zugriff auf Daten für Euren Personalrat
  - Einladungen, Speicherung, Zugriff, Aufbewahrung usw.
  - Die Richtlinie muss nicht ausformuliert sein, aber alle Punkte enthalten, die später drin stehen sollen

Zugriff auf Daten innerhalb des Personalrats

- Zugriffskonzept
- i.d.R. alle Mitglieder alles
  - aber Ausnahmen z.B. BEM

Datensicherheit

» Alle Maßnahmen zum Schutz von Daten vor:
» Verfälschung,
» Zerstörung und
» unzulässiger Weitergabe

» Gefahren:
- Technisches Versagen (z.B. Stromausfall)
- Menschliche Fehlhandlungen (z.B. Löschen von Daten)
- Vorsätzliche Handlungen
- Organisatorische Mängel und
- Höhere Gewalt (z.B. Sturm, Erdbeben)

Art. 32 DSGVO Sicherheit der Verarbeitung - Technische Anforderungen

- 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:
  - die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - die 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.

Art. 32 DSGVO Sicherheit der Verarbeitung - Technische Anforderungen

- 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.
- 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.

Notebooks und Speichermedien

» Zutrittskontrolle

- Liegenlassen (z.B. im ICE oder Tagungsräumen) vermeiden
- Zugriff Dritter verhindern (z.B. am Heimarbeitsplatz)

» Zugangskontrolle

- Notebook bei Nichtbenutzung sperren (Strg-Alt-Del)
- Passworte nicht weitergeben
- Einsichtnahme Bildschirm durch Dritte (z.B. im ICE) durch Einsatz
  - » eines *Notebook Privacy Filters* einschränken;

Technische und organisatorische Maßnahmen für Datensicherheit

Art. 25 DSGVO:

- Zutrittskontrolle

  Schutz des räumlichen Zugangs zu DV-Anlagen

  (z.B. Chip, Pförtner, Kamera)

- Zugangskontrolle

  Schutz vor unbefugter Nutzung der DV-Anlagen (z.B. Passwort)

- Zugriffskontrolle

  Vermeidung unberechtigter Zugriffe auf Daten/Dateien (z.B. Rollen/Berechtigungen

- Weitergabekontrolle

  Schutz der Daten vor unbefugtem Zugriff bei Übertragung

Speicherung von Daten

- Wo werden die personenbezogenen Daten mit denen der Personalrat / die Personalratsmitglieder zu haben gespeichert?
- Technische Sicherung
  - Verschlüsselung (z.B. bitlocker)
  - Backup?
  - Aus welchem Laufwerk?
- Zugriffsregelungen?

Meldepflichten bei Datenschutzverletzungen

- Pflicht Meldung der Verletzungen Schutzes personenbezogener Daten
  - Meldung binnen 72 Stunden
  - Verzögerungen müssen begründet werden
- Da Personalrat nicht Verantwortlicher: Meldungen über behördlichen Datenschutzbeauftragten
- Verfahren mit dem Verantwortlichen und behördlichem Datenschutzbeauftragten vereinbaren

Folgen bei Datenschutzpannen /-verletzungen - Meldepflichten

Fallbeschreibung	Meldepflicht an die Aufsichtsbehörde	Informationspflicht an Betroffene	Anmerkungen
Gestohlener USB-Stick mit wirksam verschlüsselten Daten	Nein	Nein	Kein Art.-33-Fall aufgrund der Verschlüsselung. Meldepflicht besteht jedoch, wenn die Daten nicht anderweitig gesichert sind.
Datenzugriff durch Cyber-Attacke	Ja	Ja (abhängig von der Art der Daten)	
Mehrminütiger Stromausfall, dadurch zwischenzeitlich kein Zugriff möglich	Nein	Nein	Aber interne Dokumentation nach Art. 33 Abs. 5
Ransomware-Attacke, die Kundendaten verschlüsselt (Erpressungstrojaner)	Ja (in der Regel)	Ja (in der Regel)	Außer es gibt ein Backup, sodass die Daten zügig wiederhergestellt werden können.
Kontoauszug an falschen Kunden verschickt	Ja	Im Einzelfall i.d.R. nicht, bei Häufung schon	

Folgen bei Datenschutzpannen /-verletzungen - Meldepflichten

Hacker erbeuten Nutzernamen, Passwörter und Kaufhistorie der Kunden eines Onlineshops	Ja	Ja	
Kunden können aufgrund eines Programmierfehlers im Kundenportal fremde Kundendaten einsehen	Ja, wenn Daten abgerufen wurden	Kommt darauf an	
Cyber-Attacke auf Krankenhaus, dadurch für 30 Minuten kein Zugriff auf Patientendaten	Ja	Ja	
Versehentliche Versendung von Schülerdaten an eine Mailingliste	Ja	Ja (in der Regel)	
Werbe-E-Mail mit offenem Mailverteiler (cc statt bcc)	Ja (bei großer Empfängerzahl oder sensiblem Inhalt, z.B. Passwörter)	Ja (außer nur wenige Betroffene und kein sensibler Inhalt)	

Löschen von Daten

- Art. 5 DS-GVO Verarbeitung nur solange wie für Zweck gebraucht
- Anspruch auf Löschung von Daten – Recht auf Vergessenwerden – Art 17 DS-GVO
- Löschung, wenn für
  - Daten sind für den Zweck nicht mehr notwendig
  - Einwilligung wird widerrufen
  - Widerspruch gegen die Verarbeitung
  - Daten wurden unrechtmäßig verarbeitet
- Keine Löschung, wenn u.a.
  - Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich oder z.B.
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Löschen von Daten

- **Art. 17 DSGVO Recht auf Löschung ("Recht auf Vergessenwerden")**
- Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:
  - **Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.**
  - Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
  - Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2
    Widerspruch gegen die Verarbeitung ein.

Löschen von Daten

- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

- Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Löschen von Daten

- Art 17 DS-GVO
- Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist
  - zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
  - **zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;**
  - aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
  - für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
  - **zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen**.

Löschen von Daten

- Personalrat muss, um die Rechte und Pflichten aus dem PersVG wahrzunehmen Daten verarbeiten und auch vorrätig halten z.B.
  - Bewerbungen
  - Einstellungen
  - Versetzung
  - Eingruppierungen
  - Kündigungen
  - BEM-Gespräche
  - Weitere Daten, die sich aus der Umsetzung von Gesetzen, Tarifverträgen und Betriebsvereinbarungen ergeben

Löschen von Daten

- Für die Tätigkeit des PR selbst gelten z.T. auch die steuerrechtlichen Aufbewahrungsfristen
  - Z.B. Reisekosten, Seminarkosten usw.
  - Aufbewahrung / Löschung wie sonstige Buchhaltungsbelege im Unternehmen
- Aufbewahrung von Daten wegen Rechtsstreitigkeiten
  - Unterlagen über Zustandekommen von Betriebsvereinbarungen
- Löschen von Daten im PR-Büro
- Löschen von Daten auf den Rechner der PR-Mitglieder

Grundlagen für Löschfristen

Kategorie	Maßgebliche Norm	Rechtliche Bewertung
Aufbewahrungspflicht für „Handelsbriefe“	§ 257 Abs. 1 Nr. 2–3, Abs. 4 HGB	Empfangene und Kopien versendeter „Handelsbriefe“ müssen für sechs Jahre archiviert werden. Hierzu gehört ein Großteil der in Zusammenhang mit der Anbahnung und Ausführung von Verträgen geführten Korrespondenz einschließlich E-Mails und der Kommunikation durch Call-Center.
Aufbewahrungspflicht für Bilanzen und Buchungsbelege	§ 257 Abs. 1, insb. Nr. 4, Abs. 4 HGB, § 238 Abs. 1 HGB	Bilanzen, Jahresabschlüsse und weitere datenschutzrechtlich meist weniger relevante Dokumente müssen **zehn Jahre** aufbewahrt werden. Die gleiche Frist gilt für Buchungsbelege i. S. d. §§ 257 Abs. 1 Nr. 4, 238 Abs. 1 HGB, die datenschutzrechtlich relevant sein können.
Aufbewahrung, weil Löschung unverhältnismäßig wäre (Backup u. a.)	offen	Die Regelungen der DS-GVO hierzu weichen deutlich von § 35 Abs. 3 Nr. 3 BDSG a. F. ab, wonach lediglich eine Sperrung erfolgen musste, wenn die Löschung gar nicht oder nur mit einem unverhältnismäßig großen Aufwand möglich war.

Aus: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Auflage 2018

Löschen von Daten

- Verjährungsfristen für Rechtsansprüche aus dem Arbeitsverhältnis i.d.R. 3 Jahre - § 195 BGB
- Verjährung in 30 Jahren in besonderen Fällen z.B. rechtskräftige Titel aus Gerichtsverfahren
- 30 Jahre auch für Schadensersatzansprüche für vorsätzliche Verletzung des Körpers, Lebens, der sexuelle Selbstbestimmung

Löschen von Daten - Praxis

- Wann und wie löscht die Personalabteilung die Daten
  - Z.B. über ehemalige Mitarbeiter / BewerberInnen
- Personalrat braucht bestimmte Unterlagen um Mitbestimmung auszuüben
  - Z.B. bei Eingruppierungen um Praxis und begründen / darzulegen
- Wenn Daten aktuell nicht mehr benötigt, aber aufbewahrt werden müssen: Zugriffsbeschränkung

Was ist zu tun?

- Bestandsaufnahme des Datenschutzes im Personalrat
  - Was wird wie an Daten verarbeitet?
  - Verfahrensverzeichnis
  - E-Mail-Verkehr
  - Speicherung von Daten
  - Aufbewahrungsdauer von Daten
    - Löschkonzept

Was ist zu tun?

- Bestandsaufnahme der Datenverarbeitung im PR
  - Speicherung
  - E-Mail
  - Zugriff
- Erarbeitung eines Konzeptes
  - Zusammenarbeit mit behördlichem Datenschutzbeauftragten
- Selbstverpflichtung des Personalrates zum Datenschutz
- Festlegung in einer Datenschutz - Geschäftsordnung

Tag 2

Schutz von Beschäftigtendaten

„Datenschutz ist ein Eckpfeiler des freiheitlichen Rechtsstaats“

(so Richter BVerfG Prof. Dr. *Masing*, NJW 2012, 2305)

Verfassungsrechtlicher Rahmen

Das durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG und Art. 8 Abs. 1 EMRK gewährleistete allgemeine Persönlichkeitsrecht ist im Arbeitsverhältnis zu beachten.

Dieses Recht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf **informationelle Selbstbestimmung** auch den informationellen Schutzinteressen des Einzelnen Rechnung.

Verfassungsrechtlicher Rahmen

Es gewährleistet die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich **selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden**.

Verfassungsrechtlicher Rahmen

Der EuGH verlangt zum Schutz des in Art. 7 der Charta der Grundrechte der Europäischen Union garantierten Grundrechts auf Privatleben, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das *„absolut Notwendige“* beschränken müssen.

ERGO:

Jede Verarbeitung von personenbezogenen Daten berührt das Persönlichkeitsrecht des Betroffenen und bedarf als Grundrechtseingriff einer Erlaubnisgrundlage.

ERGO:

Eine Erlaubnis zur Datenverarbeitung kann sich aus Gesetz, Einwilligung der einzelnen Person oder einer Dienstvereinbarung als Kollektivvereinbarung ergeben. Diese drei Möglichkeiten sollen nachfolgend besprochen werden.

Gesetz als Erlaubnisgrundlage

- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit
  - das Bundesdatenschutzgesetz (vgl. § 26 Abs. S. 1 BDSG)
  - oder eine andere Rechtsvorschrift dies erlaubt oder anordnet, § 26 Abs. 4 BDSG)
  - oder der Betroffene eingewilligt hat (vgl. § 26 Abs. 2 BDSG, Art. 7 DS-GVO).

Gesetz als Erlaubnisgrundlage

Es gilt ein Verbot mit Erlaubnisvorbehalt, Art. 6 DS-GVO

Datenerhebung, -verarbeitung und -nutzung ohne vorherige Einwilligung des Betroffenen sind also nur bei Vorhandensein einer ausdrücklichen gesetzlichen Ermächtigung zulässig.

Gesetz als Erlaubnisgrundlage

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung **erforderlich** ist.

Gesetz als Erlaubnisgrundlage

Erforderlichkeit setzt damit ein berechtigtes Interesse des Arbeitgebers an der Datenverarbeitung voraus, das aus dem bestehenden Arbeitsverhältnis herrühren muss. Es muss ein Zusammenhang mit der Erfüllung der vom Arbeitnehmer geschuldeten vertraglichen Leistung, seiner sonstigen Pflichtenbindung oder mit der Pflichtenbindung des Arbeitgebers bestehen.

Gesetz als Erlaubnisgrundlage

Greift eine Maßnahme in das allgemeine Persönlichkeitsrecht des Arbeitnehmers ein, muss der Eingriff einer Abwägung der beiderseitigen Interessen nach dem Grundsatz der **Verhältnismäßigkeit** standhalten.

Gesetz als Erlaubnisgrundlage

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime **Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Gesetz als Erlaubnisgrundlage

Typische Daten, die für die Durchführung eines Beschäftigungsverhältnisses erforderlich sind (Stammdaten):

- Name und Adresse,
- Bankverbindung, Krankenkasse,
- Ausbildung/Fachrichtung/Abschluss,
- Sprachkenntnisse,
- Familienstand,
- Geschlecht.

Gesetz als Erlaubnisgrundlage

Zur Durchführung des Arbeitsverhältnisses können Daten erhoben werden, die der Arbeitgeber zur Erfüllung seiner Pflichten aber auch zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt. Gestattet sind demnach auch **Maßnahmen zur Kontrolle**, ob der Arbeitnehmer den geschuldeten Pflichten nachkommt.

Gesetz als Erlaubnisgrundlage

Zur Durchführung des AV gehört die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt, zur Beendigung im Sinne der **Kündigungsvorbereitung**, die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann.

Gesetz als Erlaubnisgrundlage

- Zwar ist auch die Verhaltens- und Leistungskontrolle im Grundsatz „Durchführung des Arbeitsverhältnisses“ zulässig, aber:
- Jedes Datum muss einem konkreten, legitimen **Zweck** dienen.
- Es gilt der **Grundsatz der Verhältnismäßigkeit** (oder Erforderlichkeit), daher: Nicht alles, was theoretisch aufschlussreich sein könnte, ist auch zur Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich.
- Ein Speicherungszweck kann sich auch mit der Zeit erschöpfen oder mit den Umständen erledigen.
- Eine Datenspeicherung ohne konkreten Zweck („auf Vorrat“) ist auch im Arbeitsleben unzulässig.

Gesetz als Erlaubnisgrundlage

Art. 9 DS-GVO regelt sensitive Daten:

Gesundheit

Gewerkschaftszugehörigkeit

Sexuelle Orientierung

Gesetz als Erlaubnisgrundlage

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Gesetz als Erlaubnisgrundlage

Insbesondere zulässig zum

- Zweck der Gesundheitsvorsorge,
- für die Beurteilung der Arbeitsfähigkeit

Gesetz als Erlaubnisgrundlage

Zur Aufdeckung von **Straftaten** dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende **tatsächliche Anhaltspunkte** den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung **erforderlich** ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass **nicht unverhältnismäßig** sind.

Gesetz als Erlaubnisgrundlage

Gilt der Erlaubnisgrund auch im Falle von Verstößen gegen den Arbeitsvertrag, die keine Straftat darstellen?

Oder sperrt § 26 Abs. 1 S. 2 BDSG eine solche Datenverarbeitung?

Gesetz als Erlaubnisgrundlage

Eingriffe in das Recht der Arbeitnehmer am eigenen Bild durch verdeckte Videoüberwachung sind dann zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder **einer anderen schweren Verfehlung zu Lasten** des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.

Gesetz als Erlaubnisgrundlage

Soll einem konkreten Verdacht zielgerichtet nachgegangen werden, muss diese Maßnahme den Anforderungen des § 26 Absatz 1 Satz 2 BDSG genügen.

Gesetz als Erlaubnisgrundlage

Die verdeckte Überwachung eines einer schweren Pflichtverletzung verdächtigen Arbeitnehmers ist nur unter den vergleichbaren Voraussetzungen zulässig wie zur Aufdeckung einer Straftat.

Gesetz als Erlaubnisgrundlage

Auch hier ist der Verhältnismäßigkeitsgrundsatz zu beachten.

Gesetz als Erlaubnisgrundlage

Erforderlich iSd. § 26 Abs. 1 Satz 2 BDSG bzw. **verhältnismäßig** im Sinne einer Beschränkung des allgemeinen Persönlichkeitsrechts kann eine Maßnahme demnach nur sein, wenn sie geeignet, erforderlich und angemessen ist.

Gesetz als Erlaubnisgrundlage

Soweit genug zu den gesetzlichen Erlaubnistatbeständen des § 26 Abs. 1 S. 1 und 2 BDSG!

Nun zur Erlaubnisnorm der Einwilligung

Einwilligung als Erlaubnisgrundlage

Die Einwilligung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht (Art. 6 Abs. 1 S. 1 Nr. 1a, 7 DS-GVO).

Einwilligung als Erlaubnisgrundlage

Auch im Rahmen eines Arbeitsverhältnisses können Arbeitnehmer sich grundsätzlich „frei entscheiden“, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollen. Dem steht weder die grundlegende Tatsache, dass Arbeitnehmer abhängig Beschäftigte sind, noch das Weisungsrecht des Arbeitgebers aus § 106 GewO entgegen.

Einwilligung als Erlaubnisgrundlage

Art. 7 Abs. 2 DS-GVO:

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Einwilligung als Erlaubnisgrundlage

Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr **Widerrufsrecht** nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

Einwilligung als Erlaubnisgrundlage

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche (also der Arbeitgeber) nachweisen können, dass die betroffene Person (Arbeitnehmer) in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Einwilligung als Erlaubnisgrundlage

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. **Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.**

Einwilligung als Erlaubnisgrundlage

Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

DV als Erlaubnisgrundlage

Nun kommen wir zum letzten Erlaubnisgrund:

Die Datenverarbeitung kann auch durch eine Dienstvereinbarung erlaubt werden.

DV als Erlaubnisgrundlage

§ 71 Abs. 1 PersVG und § 72 Abs. 1 Nr. 2 PersVG verpflichten die Dienstvertretungsparteien zur Wahrung der grundrechtlich geschützten Freiheitsrechte.

Sie haben daher insbesondere auch das in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeits-recht zu beachten.

DV als Erlaubnisgrundlage

Diese Verpflichtung stellt eine Schranke für die Regelungsbefugnis der Dienststellenparteien und den Inhalt der von ihnen getroffenen Regelungen dar.

DV als Erlaubnisgrundlage

Die den Dienststellenparteien auferlegte Pflicht, die Rechte der Beschäftigten zu schützen, verbietet nicht jede Dienstvereinbarung, die zu einer Einschränkung des allgemeinen Persönlichkeitsrechts führt.

DV als Erlaubnisgrundlage

Art. 26 Abs. 4 BDSG:

Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig.

Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

DV als Erlaubnisgrundlage

Art. 88 Abs. 2 EU-DSGVO:

Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

DV als Erlaubnisgrundlage

Dies bedeutet, dass jede Art von Datenverarbeitung geregelt werden muss.

DV als Erlaubnisgrundlage

Es gilt nach Art. 5 Abs. 1 c) EU-DSGVO der Grundsatz der Datenminimierung.

Dies stellt auch die Grenzen für die Regelungen in Dienstvereinbarungen dar.

Handlungsmöglichkeiten des PR

Welche Handlungsmöglichkeiten haben die Personalvertretungen demnach?

Handlungsmöglichkeiten des PR

Das wichtigste rechtliche Instrument des Personalrats zum Schutz der Beschäftigten vor ungerechtfertigter Verhaltens- und Leistungskontrolle ist sein Mitbestimmungsrecht gemäß § 85 Abs. 1 Nr. 13b PersVG.

Handlungsmöglichkeiten des PR

Es genügt die objektive Möglichkeit der Überwachung um das Mitbestimmungsrecht des Personalrats auszulösen.

Handlungsmöglichkeiten des PR

Auf eine Überwachungsabsicht der Dienststellenleitung kommt es nicht an.

Daher werden praktisch alle denkbaren technischen Einrichtungen und Vorgänge, die in der Lage sind, personenbezogene Verhaltens- und Leistungsdaten über die Beschäftigten zu erheben und zu verarbeiten in das Mitbestimmungsrecht einbezogen.

Handlungsmöglichkeiten des PR

Bei der Verarbeitung von personenbezogenen Daten hat der Personalrat gemäß § 72 Abs. 1 Nr. 2 PersVG die Aufgabe, die Einhaltung des Landesdatenschutzgesetzes zugunsten der Beschäftigten der Dienststelle zu überwachen.

Handlungsmöglichkeiten des PR

Zur Erfüllung der Überwachungsaufgabe nach § 71 Abs. 1 und § 72 Abs. 1 PersVG hat die Dienststellenleitung den Personalrat nach § 73 PersVG rechtzeitig und umfassend über alle Formen der Verarbeitung und Nutzung der gespeicherten Daten der Arbeitnehmer zu unterrichten.

Dies betrifft insbesondere die Einführung neuer IT-Systeme und Anlagen, die zur Verhaltens- und Leistungskontrolle geeignet sind.

Handlungsmöglichkeiten des PR

Auf Verlangen sind dem Personalrat sämtliche einschlägigen Unterlagen vorzulegen (§ 73 Abs. 1 S. 2 PersVG).

Das Informationsrecht des Personalrats besteht auch dann, wenn die Erhebung und Verarbeitung der personenbezogenen Daten der Beschäftigten nicht im »eigenen« Unternehmen, sondern bei einem anderen Unternehmen erfolgt (also beim Auftragsdatenverarbeiter).

Handlungsmöglichkeiten des PR

Der Personalrat kann zweierlei tun:

Er kann versuchen, mit der Dienststellenleitung eine Rahmendienstvereinbarung zu IT-Verfahren aufzustellen. Hier besteht jedoch kein zwingendes Mitbestimmungsrecht.

Er darf vor der Einführung die Regelung eines jeden Systems und Verfahrens verlangen. Dies unterliegt seiner zwingenden Mitbestimmung.

Handlungsmöglichkeiten des PR

Der Personalrat muss jedoch erst einmal Informationen über das System erhalten. Dazu sollte er einen Fragenkatalog an die Dienststellenleitung richten. Dazu beispielhafte Fragen:

Handlungsmöglichkeiten des PR

1. Benennung des Systems nebst Versionsnummer und Anbieter
2. Umfang des Systems und vollständige Beschreibung aller genutzten und gesperrten Funktionalitäten nebst einer übersichtlichen Darstellung
3. Vorlage des Systemhandbuchs
4. Benennung der Datenfelder und der in jedem Datenfeld jeweils verarbeiteten personenbezogenen Daten
5. Welche Daten werden als Stammdaten eingestuft?

Handlungsmöglichkeiten des PR

6. Zweck der Nutzung der Funktionalitäten und der Verarbeitung der personenbezogenen Daten
7. Abschließende Auflistung aller Rollen nebst den ihnen zugeordneten Rechten in Bezug auf die Datenfelder (Lesen/Schreiben). Wer darf welche Daten einsehen, wer darf sie verändern?
8. Darstellung der Zuordnung der Rollen zu Hierarchieebenen
9. Darstellung aller Schnittstellen zu anderen IT-Systemen und Auflistung aller Importe/Exporte, auch wenn diese manuell erfolgen

Handlungsmöglichkeiten des PR

10. Aufstellung aller Reports und Protokolle
11. Werden alle Zugriffe protokolliert?
12. Besteht eine Auftragsdatenverarbeitung?
13. Vorlage des Auftragsdatenverarbeitungsvertrags

Handlungsmöglichkeiten des PR

15. Wie soll eine barrierefreie Gestaltung sichergestellt werden?

17. Wie wurden die technisch-organisatorischen Maßnahmen umgesetzt?

18. Welche Auditierungsrechte hat die Arbeitgeberin? Welche Auditierungsrechte hat der PR?

19. Wie lange werden die personenbezogenen Daten gespeichert? Wann werden sie gelöscht?

20. Was passiert mit personenbezogenen Daten ausscheidender Arbeitnehmer?

Handlungsmöglichkeiten des PR

21. Welche Einsichtsrechte haben die Arbeitnehmer in die über sie gespeicherten Daten? Können sie die gespeicherten Daten selbst löschen oder die Löschung durch die Arbeitgeberin durchsetzen?

22. Wer sind die IT-Beauftragten der Einrichtungen und welche Befugnisse haben sie?

Handlungsmöglichkeiten des PR

26. Wird weiterhin ein Mobile Device Management eingesetzt? Welches? Wie ist dies konfiguriert? Soll dies in einer Dienstvereinbarung geregelt werden?
27. Wie wird sichergestellt, dass keine Nutzung des Systems außerhalb der Arbeitszeit erfolgt?
28. Wie wird der log-in in das System gesichert?
29. Wer administriert das System?

Handlungsmöglichkeiten des PR

30. Wie werden die Arbeitnehmer in den Funktionalitäten, dem Datenschutzrecht und die abzuschließende Dienstvereinbarung geschult?

31. Wie werden alle Arbeitnehmer umfassend über alle innerhalb des Betriebs gespeicherten personenbezogenen Daten informiert, die im Zusammenhang mit der Systemeinführung und dem laufenden Einsatz des Systems über sie erfasst oder später angelegt wurden?

33. Wie beabsichtig der Arbeitgeber künftig die Information über die Einführung, Aktivierung bzw. Funktionsweise neuer Komponenten sicherzustellen?

Ergebnis

Also:

Wenn ein IT-System eingeführt werden soll, dann sollte der Personalrat zur Fristwahrung die Zustimmung begründet verweigern.

Er sollte dann konkrete Fragen stellen und zum Abschluss einer DV als Kollektivvereinbarung nach § 26 Abs. 4 BDSG auffordern.

Eine solche Dienstvereinbarung schützt nicht nur die Beschäftigten, sie stellt für die Dienststelle auch eine rechtssichere Erlaubnisgrundlage dar.

Vielen Dank.

Sebastian Baunack
dka · Immanuelkirchstraße · 3–4 · 10405 Berlin
Telefon 030 4467920
baunack@dka-kanzlei.de
www.dka-kanzlei.de