

Wir haben doch nichts zu verbergen...



Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

In Kooperation mit:



dtb – Datenschutz- und Technologieberatung



Wir haben doch nichts zu verbergen...

... beobachtet, bewertet, beurteilt
Seminar für Betriebs- und Personalräte
vom 5. bis 7. November 2019 in Berlin

Diesen Vortrag und weitere Informationen finden Sie auf unserer Website: www.ecovis.com/datenschutzberater/ -> Veranstaltungen

Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

- | | | | |
|----|---|----|---|
| 1. | Vorgaben der DSGVO | 4. | Datenschutz durch Technik |
| 2. | Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung | 5. | Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen |
| 3. | Datenschutz-Folgenabschätzung – ein neues Instrument: wie umsetzen? | 6. | Fazit |

EIN ÜBERBLICK - in 45 min

Der Schutz von Beschäftigendaten:

Ausgangsthesen



- › Beschäftigte sind auch Menschen!
- › meine Wohnung ist meine Privatsphäre (privacy)!



- › Bürgerrechte sind national
- › Datenschutzrecht ist europäisch
 - › mit globalem Anspruch
- › Datenverarbeitung ist global,
 - › aber rechtlich unregelt!



- › meine Arbeitsstätte ist nicht Privat!
- › ABER: auch hier bin ich Mensch (und muss es sein dürfen)
 - › (privacy => data protection)
- › Was ist mein HOMEOFFICE?
 - › Work / Life Balance



- › „Lieber Geld verlieren, als Vertrauen!“
 - › Robert Bosch, 1861-1942
- › „Es gibt kein belangloses Datum mehr“
 - › (BVerfG, 1983)
- › Datenschutz ist mehr
 - › als Privatsphärenschutz

Der Schutz von Beschäftigendaten:

Vorgaben der DSGVO

- | | | | |
|----|---|----|---|
| 1. | Vorgaben der DSGVO | 4. | Datenschutz durch Technik |
| 2. | Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung | 5. | Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen |
| 3. | Datenschutz-Folgenabschätzung – ein neues Instrument: wie umsetzen? | 6. | Fazit |

Der Schutz von Beschäftigtendaten:

Vorgaben der DSGVO

- Beschäftigte werden datenschutzrechtlich (fast) wie Betroffene behandelt
- Alle Rechte der Betroffenen gelten hier im Rahmen gesetzlicher Vorschriften, des Arbeitsvertrages und von Kollektivvereinbarungen.
Hierdurch entstehen weitergehende Überwachungspflichten und Kontrollrechte zugunsten der Arbeitnehmer (Arbeitsschutz, Gesundheitsschutz) und der Gemeinschaft (Steuerrecht, Führungszeugnis, AGG).

Der Schutz von Beschäftigtendaten:

Vorgaben der DSGVO

- Beschäftigte sind aber zugleich als Mitarbeiter des Verantwortlichen datenschutzrechtlichen Kontroll- und Überwachungspflichten des Arbeitgebers/Verantwortlichen unterworfen:

Gewährleistung der Vertraulichkeit	Dokumentation von Datentransfers
Protokollierung von Datenzugriffen	Protokollierungen bei der Überwachung von Zugangs- und Zugriffsrechten

Der Schutz von Beschäftigendaten:

Vorgaben der DSGVO

› Art. 29 Gruppe: Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz 8. Juni 2017

- Arbeitgeber sollten sich stets bewusst sein, dass unabhängig von der eingesetzten Technologie elementare Datenschutzgrundsätze einzuhalten sind.
- Für den Inhalt der elektronischen Kommunikation aus Geschäftsräumen gilt derselbe Schutz grundlegender Rechte wie für die analoge Kommunikation.
- Es ist überaus **unwahrscheinlich**, dass die Einwilligung der Beschäftigten eine Rechtsgrundlage für die Datenverarbeitung am Arbeitsplatz darstellt, es sei denn die Beschäftigten können die Einwilligung ohne nachteilige Folgen verweigern.

Der Schutz von Beschäftigendaten:

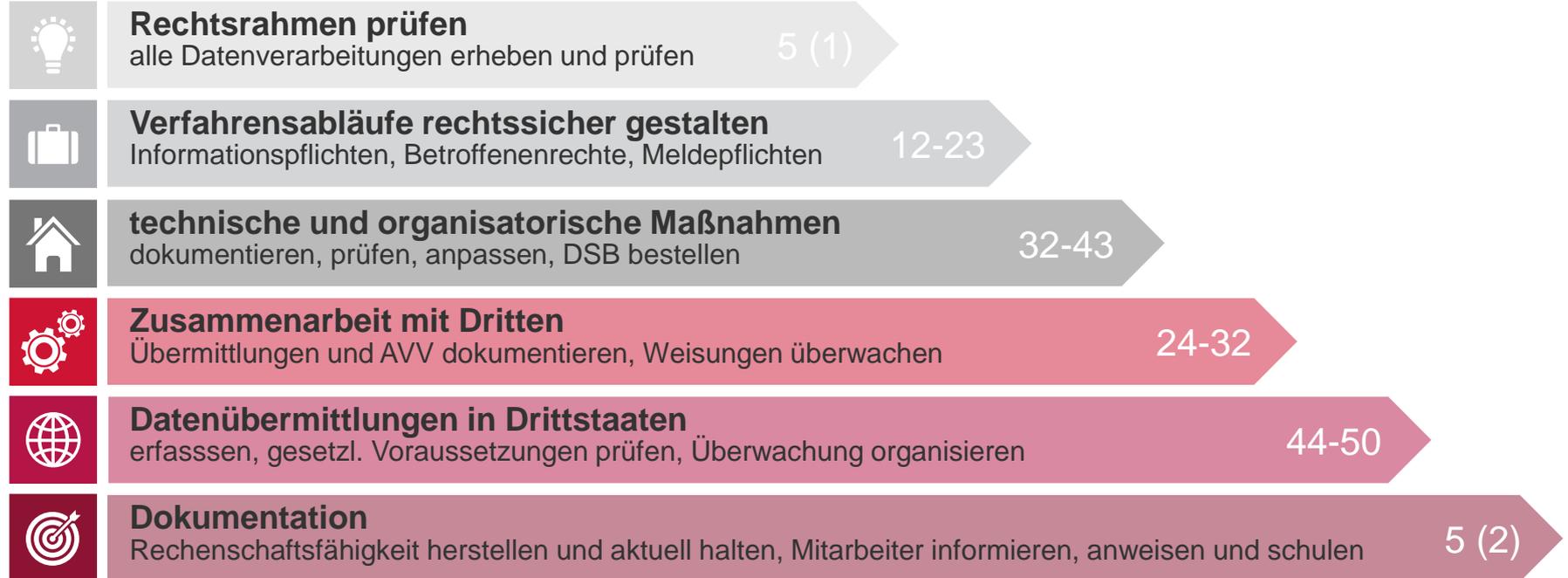
Vorgaben der DSGVO

- In **einigen Fällen** können die **Erfüllung eines Vertrags und berechnete Interessen als Rechtsgrundlage** herangezogen werden, sofern die Verarbeitung für einen rechtmäßigen Zweck unbedingt erforderlich ist und den Grundsätzen der Verhältnismäßigkeit und der Subsidiarität entspricht.
- Die Beschäftigten **sollten wirksam über die erfolgende Überwachung informiert** werden.
- Eine **internationale Übermittlung** von Beschäftigendaten darf nur erfolgen, wenn ein angemessenes Schutzniveau gewährleistet wird.

„Ein Beispiel einer unrechtmäßigen Weiterverarbeitung ist der Einsatz von rechtmäßig für Zwecke des Eigentumsschutzes installierten Systemen für die Überwachung von Arbeitnehmern hinsichtlich der Verfügbarkeit, der Leistung und des freundlichen Umgangs mit Kunden.“

Der Schutz von Beschäftigendaten:

Vorgaben der DSGVO



Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

- | | | | |
|----|---|----|---|
| 1. | Vorgaben der DSGVO | 4. | Datenschutz durch Technik |
| 2. | Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung | 5. | Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen |
| 3. | Datenschutz-Folgenabschätzung – ein neues Instrument: wie umsetzen? | 6. | Fazit |

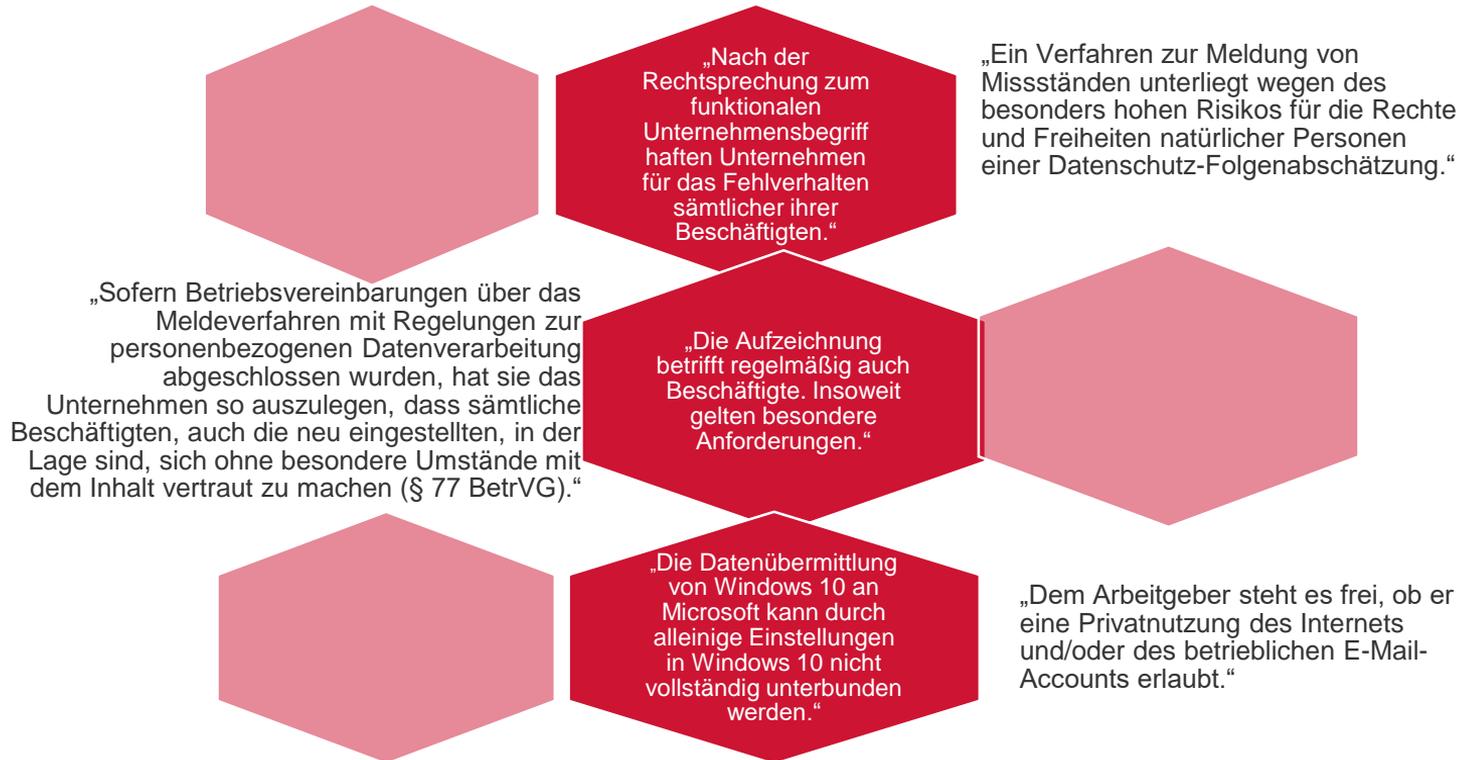
Der Schutz von Beschäftigtendaten:

Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung

- › Art. 29 Gruppe: Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz 8. Juni 2017
- › 14.11.2018 - Orientierungshilfe der Datenschutzaufsichtsbehörden Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz
- › Januar 2016 - Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz
- › Beschluss der DSK vom 23.03.2018 - Aufzeichnung von Telefongesprächen
- › Entschließung DSK vom 03.04.2019 - Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten! -

Der Schutz von Beschäftigtendaten:

Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung



Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

- | | | | |
|----|---|----|---|
| 1. | Vorgaben der DSGVO | 4. | Datenschutz durch Technik |
| 2. | Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung | 5. | Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen |
| 3. | Datenschutz-Folgenabschätzung – ein neues Instrument: wie umsetzen? | 6. | Fazit |

Europäischer Datenschutzausschuss:

[WP 248 rev.01 – Leitlinien zur Datenschutz-Folgeabschätzung und zur Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt"](#)

Der Schutz von Beschäftigtendaten:

Datenschutzfolgenabschätzung

Datenschutz

Folgen

Risikoeinschätzung

- › Betroffene
 - › Kunden
 - › Mitarbeiter
 - › Angehörige
 - › Dritte
- › Art der Daten/Kategorie
 - › bes. Arten
 - › Zahlungsdaten / Einkommensdaten
- › Umfang der Daten

Risikobewertung

- › Wirkungsanalyse bei
 - › Vernichtung
 - › Verlust
 - › unrechtmäßige Nutzung
 - › Kenntnisnahme durch Dritte
- › je Betroffenenengruppe
- › je Datenkategorie

Risikominimierung

- › Datenminimierung
- › Pseudonymisierung
- › technische und organisatorische Maßnahmen
- › Transparenz

Ist das (immer) verbleibende Restrisiko (aus Sicht der Betroffenen) angemessen?

› Einbeziehung der Betroffenenvertreter (BetrRat): Art. 35 (9) !

Abschätzung

Der Schutz von Beschäftigendaten:

Datenschutzfolgenabschätzung

Art. 35 (1):

› Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten* natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten** durch.“



1. Feststellen	Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
2. Abschätzen	Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten**
3. Beurteilen	Risiko für die Rechte und Freiheiten natürlicher Personen*?
JA	=> „hohes“ Risiko ? => regelmäßige Auditierung, Art. 35 (11)
NEIN	=> Dokumentation der Gründe gem. Art. 5 (2)

Der Schutz von Beschäftigendaten:

Datenschutzfolgenabschätzung

* Risiko für die Rechte und Freiheiten, EW 75:

Verarbeitung personenbezogener Daten, die zu einem

physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn:

die Verarbeitung zu einer

- Diskriminierung,
- einem Identitätsdiebstahl oder -betrug,
- einem finanziellen Verlust,
- einer Rufschädigung,
- einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- der unbefugten Aufhebung der Pseudonymisierung oder
- anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen **kann**,

Der Schutz von Beschäftigendaten:

Datenschutzfolgenabschätzung

* Risiko für die Rechte und Freiheiten, EW 75:

insbesondere wenn:

die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten **zu kontrollieren**,

personenbezogene Daten, aus denen die

rassistische oder ethnische Herkunft,

politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder

die Zugehörigkeit zu einer Gewerkschaft hervorgehen,

und

genetische Daten, Gesundheitsdaten oder das Sexualleben

oder

strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten

verarbeitet werden,

Der Schutz von Beschäftigtendaten:

Datenschutzfolgenabschätzung

insbesondere wenn:

persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die

- die Arbeitsleistung,
- wirtschaftliche Lage,
- Gesundheit,
- persönliche Vorlieben oder Interessen,
- die Zuverlässigkeit oder das Verhalten,
- den Aufenthaltsort oder Ortswechsel betreffen,

analysiert oder **prognostiziert** werden, um persönliche Profile zu erstellen oder zu nutzen,

personenbezogene Daten **schutzbedürftiger** natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden

oder die Verarbeitung eine

- große **Menge** personenbezogener Daten und
- eine große **Anzahl** von betroffenen Personen betrifft.

Der Schutz von Beschäftigendaten:

Datenschutzfolgenabschätzung

** Schutz personenbezogener Daten nach Art. 4 Nummer 12:
„**Verletzung des Schutzes personenbezogener Daten**“ :

eine Verletzung der Sicherheit, die

- zur Vernichtung,
- zum Verlust oder
- zur Veränderung,

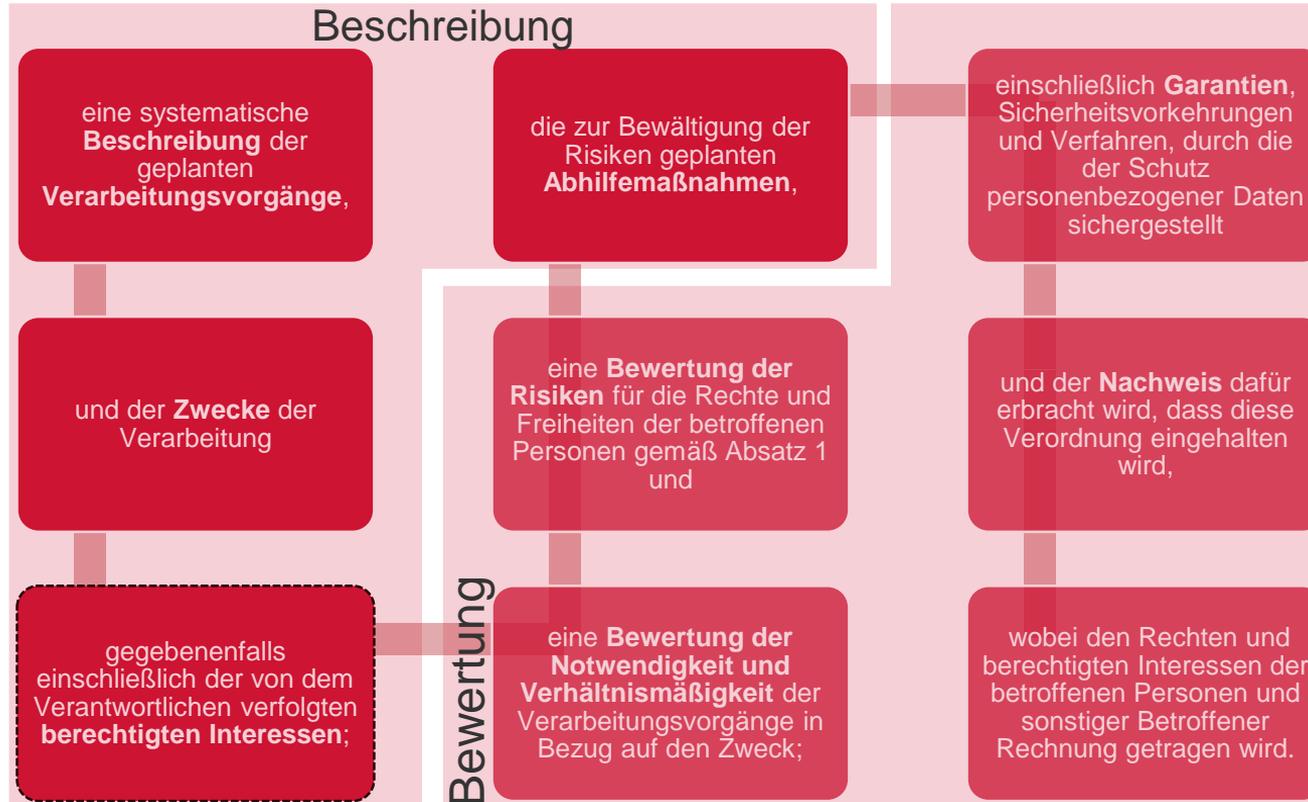
ob unbeabsichtigt oder unrechtmäßig,

- oder zur unbefugten Offenlegung
von

- beziehungsweise zum unbefugten
Zugang zu personenbezogenen
Daten führt,
- die übermittelt,
- gespeichert oder
- auf sonstige Weise verarbeitet
wurden;

Der Schutz von Beschäftigendaten:

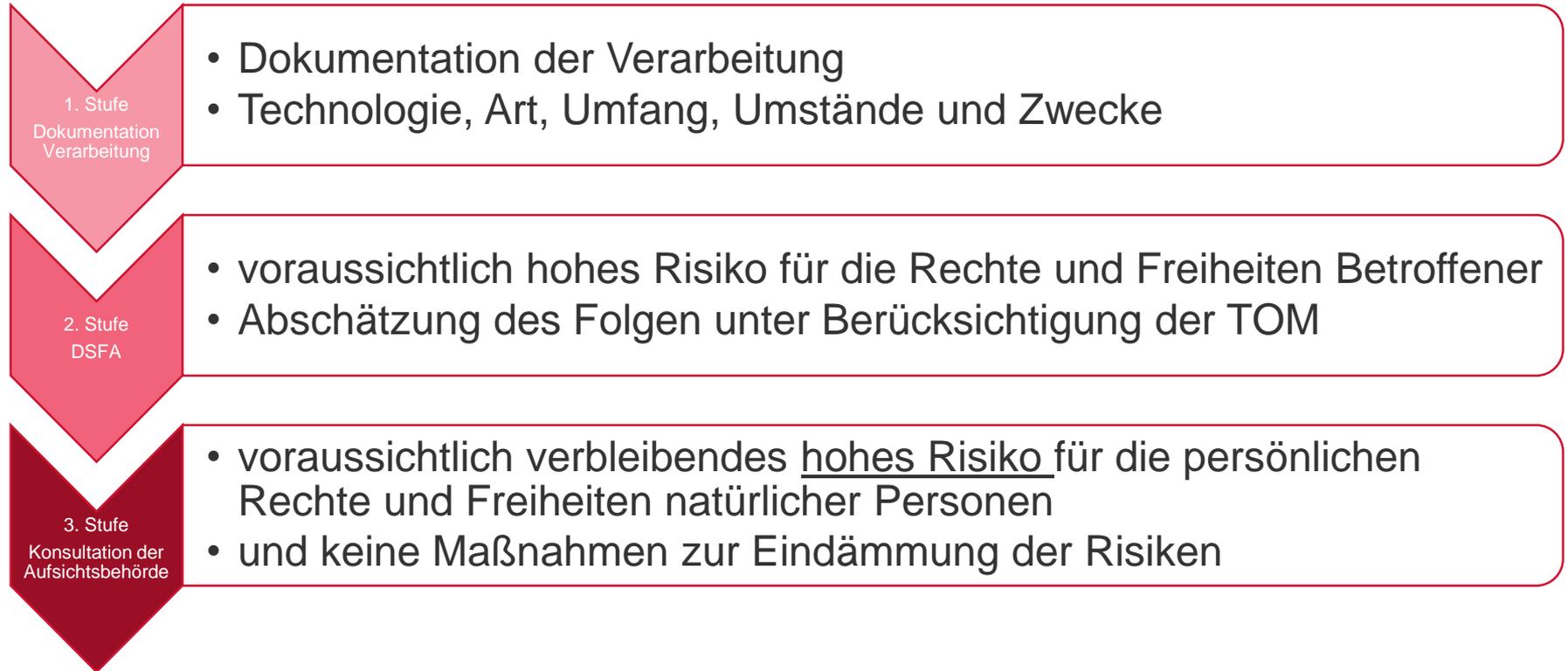
Datenschutzfolgenabschätzung



Für den Fall, dass unklar ist, ob eine DSFA erforderlich ist, empfiehlt die WP29-Gruppe dennoch die Durchführung einer DSFA, weil den für die Verarbeitung Verantwortlichen damit ein hilfreiches Instrument für die Einhaltung der Datenschutzgesetze zur Verfügung steht.
=> Art. 5 (2)

Der Schutz von Beschäftigtendaten:

Datenschutzfolgenabschätzung



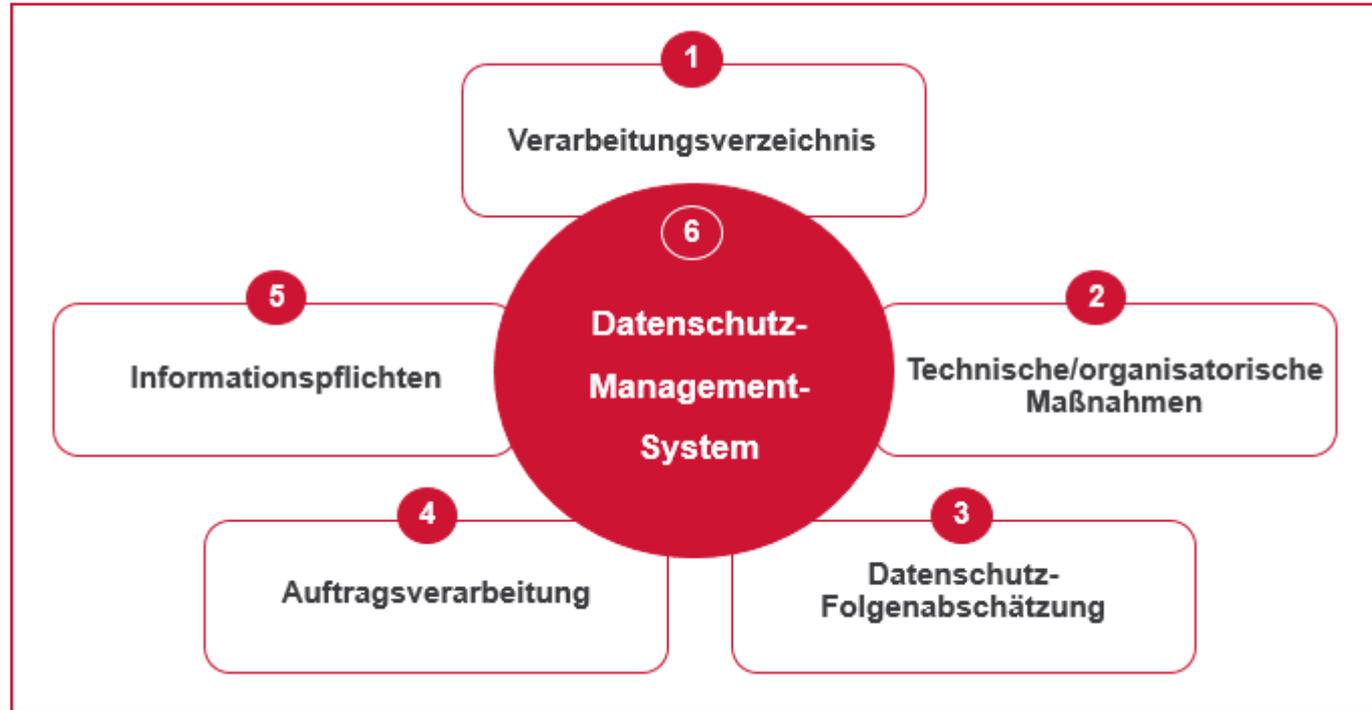
Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

1. Vorgaben der DSGVO
2. Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung
3. Datenschutz-Folgenabschätzung – ein neues Instrument: wie umsetzen?
- 4. Datenschutz durch Technik**
5. Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen
6. Fazit

Der Schutz von Beschäftigtendaten:

technische und organisatorische Maßnahmen



Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

Art. 25 DSGVO: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

trifft der Verantwortliche

- sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch
- zum Zeitpunkt der eigentlichen Verarbeitung

geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind,

- die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und
- die notwendigen Garantien in die Verarbeitung aufzunehmen,

um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

Art. 25 DSGVO: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

- Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.
- Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.
- Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

- | | | | |
|----|---|----|---|
| 1. | Vorgaben der DSGVO | 4. | Datenschutz durch Technik |
| 2. | Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung | 5. | Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen |
| 3. | Datenschutz-Folgenabschätzung – ein neues Instrument wie umsetzen? | 6. | Fazit |

Der Schutz von Beschäftigtendaten: technische und organisatorische Maßnahmen

Standard-Datenschutzmodell

SDM

Das Standard-Datenschutzmodell liegt zunächst in einer Erprobungsfassung vor. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Heinz Müller, bittet alle für die Verarbeitung personenbezogener Daten verantwortlichen Stellen, das SDM zu erproben und über die Erfahrungen bei der Anwendung des SDM zu berichten. Auf diese Weise soll die Praxistauglichkeit erprobt und die ständige Weiterentwicklung unterstützt werden.

Bezeichnung	Format	Größe
<ul style="list-style-type: none"> Das Standard- Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele Version 1.1 	PDF	1.37 MB
<ul style="list-style-type: none"> The Standard Data Protection Model A concept for inspection and consultation on the basis of unified protection goals Version 1.0 	PDF	0.31 MB
<ul style="list-style-type: none"> AK Technik-Workshop 2015 „Das Standard-Datenschutzmodell – der Weg vom Recht zur Technik“ 	PDF	3.04 MB

Maßnahmenkatalog



Der Schutz von Beschäftigtendaten: technische und organisatorische Maßnahmen

Maßnahmenkatalog

Der Maßnahmenkatalog zum SDM befindet sich noch in der Erarbeitungsphase. Die einzelnen Bausteine des Katalogs werden sukzessive veröffentlicht und zur Anwendung freigegeben.

Wir weisen ausdrücklich darauf hin, dass die hier veröffentlichten Bausteine noch nicht in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder abgestimmt worden sind. Wir empfehlen den Anwendern, ihre Erfahrungen bei der Erprobung der Bausteine den an der Entwicklung der Bausteine beteiligten Datenschutzbehörden mitzuteilen (z. B. unter sdm@datenschutz-mv.de), und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

Bezeichnung	Format	Größe
• Baustein 11 "Aufbewahrung"	PDF	0.22 MB
• Baustein 41 "Planung und Spezifikation"	PDF	0.24 MB
• Baustein 42 "Dokumentation"	PDF	0.23 MB
• Baustein 43 "Protokollierung"	PDF	0.22 MB
• Baustein 50 "Trennung"	PDF	0.25 MB
• Baustein 60 "Löschen und Vernichten"	PDF	0.24 MB
• Baustein 80 "Datenschutzmanagement"	PDF	0.39 MB

Newsletter



➤ siehe auch [Software der CNIL \(französische Datenschutzaufsichtsbehörde\)](#)

Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

1. Vorgaben der DSGVO
2. Anforderungen der Aufsichtsbehörden zur Risikoabwägung und -bewertung
3. Datenschutz-Folgenabschätzung – ein neues Instrument wie umsetzen?
4. Datenschutz durch Technik
5. Standardmodell der Aufsichtsbehörden, weitere geeignete Vorgehensweisen
6. Fazit

Der Schutz von Beschäftigendaten:

technische und organisatorische Maßnahmen

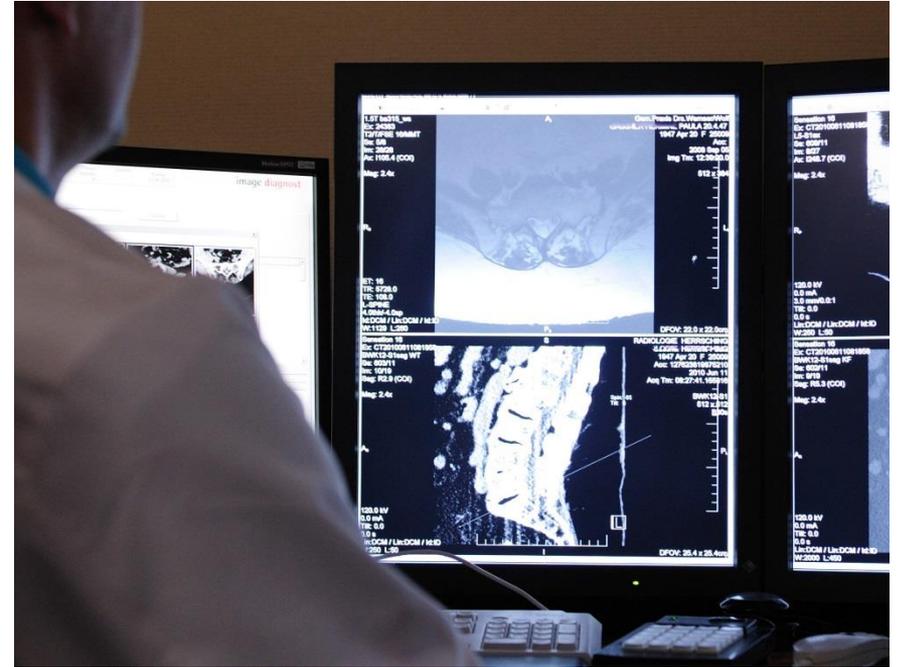
- ⚠ Mitarbeiterüberwachung wird immer weiter und differenzierter durch die Einführung komplexer und vernetzter technischer Systeme ermöglicht.
- ⚠ Eine technische „Überwachung der Überwachung“ stößt sehr schnell an Grenzen.
- ⚠ Bei einer Kündigung aufgrund einer unzulässigen Datenverarbeitung bleibt dem Betroffenen nur (aber immerhin) ein Schadenersatzanspruch.
- ⚠ Bleibt eigentlich nur ein striktes arbeitsrechtliches Beweisverwertungsverbot – das es leider in Deutschland/Europa nicht gibt!

Viele Dank für Ihre Aufmerksamkeit!

...das Thema ist nicht neu, aber aktuell

Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

BVerfG, Urteil v. 15.12.1983, sog. „Volkszählungsurteil“



Ihr Datenschutz-Nord Team

am Standort Rostock



Karsten Neumann

Landesbeauftragter für
Datenschutz M-V a.D.

Senior Associate



Birgit Dethloff

Dipl.-Kauffrau
Datenschutzbeauftragte
(TÜV)
Beratungsassistenz
Datenschutz



Kathleen Fink

M. Sc. DLM

Beratungsassistenz
Datenschutz



Anja Heidepriem

LL.M. Wirtschaftsrecht

Beratungsassistenz
Datenschutz

Ihr Datenschutz-Nord Team

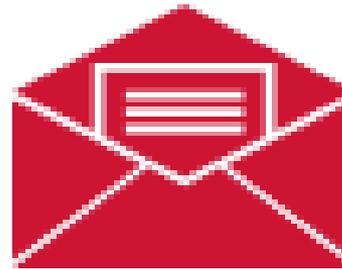
Persönlich gut beraten



Herzlichen Dank für Ihr Interesse!

ECOVIS Grieger Mallison Rechtsanwälte PartG mbB | Am Campus 1-11 | 18182 Rostock-Bentwisch | Tel. +49 381 64 92-10

Eine Haftung für die hier genannten Informationen kann aufgrund der sich ständig ändernden Gesetzeslage nicht übernommen werden.



dsb-nord
@ecovis.com

Diesen Vortrag und weitere Informationen finden Sie auf unserer Website: www.ecovis.com/datenschutzberater/ => Veranstaltungen