Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

SCHULUNG FÜR DATENSCHUTZ-KOORDINATOR:INNEN

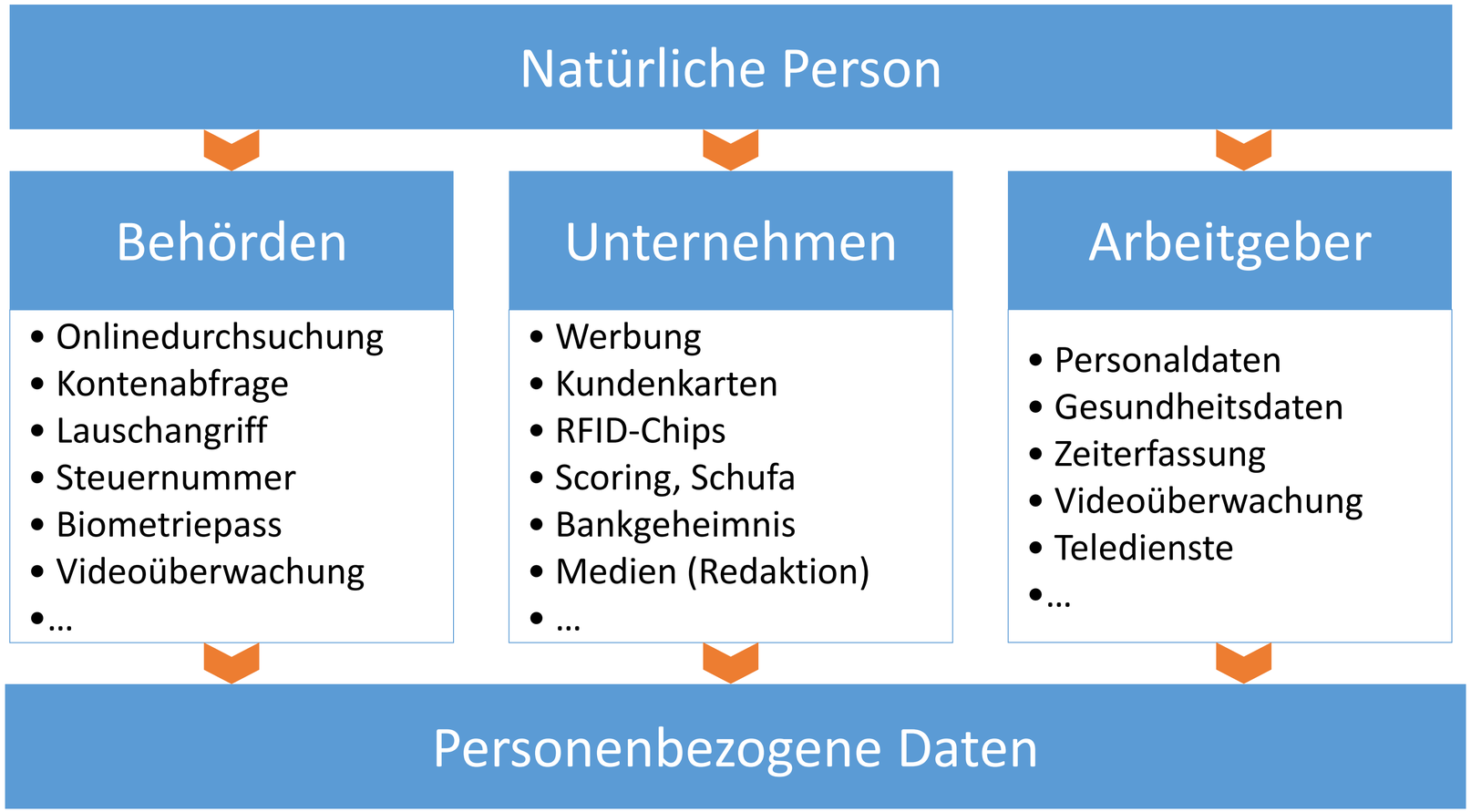
09.10.2025 • Dr. Martin Eßer • Manfred Höffken

INHALT

GRUNDLAGEN DES DATENSCHUTZES

- Worum geht es?
- Was sind personenbezogene Daten?
- Rechtsgrundlagen
- Wo endet Datenschutz?
- Anonymisierte und pseudonymisierte Daten

WO SPIELT DATENSCHUTZ EINE ROLLE?



TYPISCHER ZIELKONFLIKT

Datenschutz zielt auf…	Behörde möchte …
… präventiven Schutz durch restriktiven und an Erforderlichkeit und Zweckbindung orientierten Zugriff	… ungehinderten Zugriff auf alle Daten, Möglichkeit zur Datenverknüpfung und zur Auswertung zu vielen Zwecken

Datenschutz bewirkt Einschränkung der Datenverarbeitung zur Wahrung der Betroffenenrechte

ZWEI SCHUTZBEREICHE

Datenschutz in der Behörde

Interner Bereich

Datenschutzkonformer
Umgang mit den personen-
bezogenen Daten
der Beschäftigten der Behörde

Externer Bereich

Datenschutzkonformer
Umgang mit den personen-
bezogenen Daten
aller Personen, mit denen
die Behörde im Rahmen
Ihrer Aufgabenerfüllung in
Berührung kommt

WELCHE REGELUNGEN SIND IN BEHÖRDEN ZU BEACHTEN?

EU-Datenschutz-Grundverordnung (DSGVO)

- Europäisches Gesetz, VO (EU) 679/2016

Landesdatenschutzgesetz (DSG NW)

- ergänzt als deutsches Gesetz die DSGVO

sowie weitere spezielle Gesetze (situations- und themenabhängig), z.B. Hochschulrecht

WAS IST DATENSCHUTZ?

Schutz des Einzelnen vor den Gefahren, die eine Verarbeitung seiner Daten durch Unternehmen oder staatliche Stellen (=Behörden) mit sich bringt.

Mögliche Gefahren:

Unbegrenzte Auswertung, Verknüpfung, Speicherung, Übermittlung an andere Stellen usw.

Mögliche Folgen:

„Gläserner Mensch“, Kenntnisnahme Unbefugter, Ausschluss von Leistungen, teurere Leistungen usw.

Legaldefinition in Art. 4 Nr. 1 DSGVO:
Personenbezogene Daten sind alle Informationen[1], die sich auf eine identifizierte oder identifizierbare[2] natürliche Person[3] beziehen.

Beispiele: Name, Anschrift, Telefonnummer, Emailadresse, Familienstand, Geburtsdatum, Staatsangehörigkeit, Beruf, Vermögen, vertragliche oder sonstige Beziehungen zu Dritten, Lebenslauf, Straftaten, Wertpapiergeschäfte einer Person, …

UM WELCHE DATEN GEHT ES?

1) Informationen

- Angaben über den Betroffenen selbst, seine Identifizierung und Charakterisierung, auch Werturteile (persönliches Datum)
- Angaben über einen auf den Betroffenen beziehbaren Sachverhalt (sachliches Datum)

2) Identifizierte oder identifizierbare Person

- Regel: unmittelbarer Personenbezug
- Aber auch: Personenbezug herstellbar, abhängig von Kenntnissen, Mitteln und Möglichkeiten der speichernden Stelle

UM WELCHE DATEN GEHT ES?

3) Natürliche Person

- Nur natürliche (und lebende) Personen unterliegen dem Schutz der DSGVO (und des BDSG)
- Juristische Personen (z.B. AG, GmbH) und Personengemeinschaften (z.B. OHG, KG, GbR) werden nicht geschützt
- Einzelkaufleute werden geschützt

Legaldefinition in Art. 9 Abs. 1 DSGVO:

Besondere personenbezogene Daten sind Angaben über
die **rassische und ethnische Herkunft**,
politische Meinungen,
religiöse oder weltanschauliche Überzeugungen,
Gewerkschaftszugehörigkeit,
genetische Daten, biometrische Daten, Gesundheitsdaten,
Daten zum Sexualleben oder Daten zur sexuellen Orientierung.

Diese sog. „sensitiven Daten“ werden aufgrund Ihrer Sensibilität besonders geschützt und es gelten strengere Maßstäbe für ihre Verarbeitung (z.B. Art. 9 Abs. 2 DSGVO).

SACHDATEN NICHT GESCHÜTZT

- Daten ohne Personenbezug (Sachdaten) werden durch die DSGVO und das BDSG nicht geschützt.
  - ➢ Zum Beispiel: Fachdaten (die keine personenbezogenen Daten enthalten), Geschäfts- und Betriebsgeheimnisse, statistische Untersuchungen, Bilanzen, …
- Wenn kein Bezug der Daten zu einer Person besteht, ist das Persönlichkeitsrecht nicht berührt.

UM WELCHE DATEN GEHT ES NICHT?

Betriebs- und Geschäftsgeheimnisse

1) Vertraglich vereinbarte Geheimhaltungspflichten
2) Gesetzliche Geheimhaltungspflichten
   - ➢ § 30 AO (Steuergeheimnis), § 35 SGB I (Sozialgeheimnis), …
   - ➢ im unternehmerischen Bereich weniger relevant als vertragliche Geheimhaltungspflichten

PSEUDONYMISIERTE DATEN ART. 4 NR. 5 DSGVO

Pseudonymisierte Daten

- Personenbezug wird erschwert, indem der Name (oder ein anderes Identitätsmerkmal) durch ein Kennzeichen ersetzt wird.

Folge:

- Es bleiben personenbezogene Daten.
- Datenschutzrecht bleibt anwendbar.

ANONYMISIERTE DATEN ERWGR 26 SATZ 5

Anonymisierte Daten

- Daten, die einer Person nicht mehr zugeordnet werden können.

Folge:

- Keine personenbezogenen Daten
- Datenschutzrecht ist nicht anwendbar.

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

- Was ist es?
- Wer muss es führen?
- Was muss enthalten sein?

INHALT UND ZWECK DES VERZEICHNISSES

- Enthält einen Eintrag für jede Verarbeitung personenbezogener Daten eines Verantwortlichen oder eines Auftragsverarbeiters
- Schafft interne Transparenz (für den Verantwortlichen, den Auftragsverarbeiter und den Datenschutzbeauftragten)
- Schafft externe Transparenz, da die Aufsichtsbehörde es einsehen kann, Art. 30 Abs. 4
- Kein Einsichtsrecht für Jedermann (dieses Einsichtsrechts galt nur unter dem alten Recht bis 24.05.2018)

WAS IST IN DAS VERZEICHNIS AUFZUNEHMEN?

- Ein Eintrag pro Verarbeitung
  - automatisierte Verarbeitungen
  - teilweise automatisierte Verarbeitungen
  - nicht-automatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen → z.B. Akten
- „Dateisystem“ (definiert in Art. 4 Nr. 6): strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist (→ z.B. durchsucht werden kann); Akten oder Aktensammlungen, die nach bestimmten Kriterien geordnet sind, sind als „strukturiert“ anzusehen (ErwGrd. 15)
- Das Verzeichnis kann schriftlich oder elektronisch geführt werden, Abs. 3

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Hochschule Bonn-Rhein-Sieg
University of Applied Sciences

Inhalt beim Verantwortlichen Art. 30 Abs. 1

a) Name, Kontaktdaten des Verantwortlichen

b) Zwecke der Verarbeitung

c) Kategorien betroffener Personen und Kategorien von Daten

d) Kategorien von Empfängern, einschließlich in Drittländern oder an internationalen Organisationen

e) Dokumentation geeigneter Garantien bei Übermittlungen nach d)

f) Löschfristen

g) Wenn möglich, allgemeine Beschreibung der TOM nach Art. 32 Abs. 1

Inhalt beim Auftragsverarbeiter Art. 30 Abs. 2

a) Name und Kontaktdaten der Auftragsverarbeiters

b) Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden

c) Dokumentation geeigneter Garantien bei Übermittlungen in Drittländer oder an Internationale Organisationen

d) Wenn möglich, allgemeine Beschreibung der TOM nach Art. 32 Abs. 1

WER MUSS EIN VERZEICHNIS FÜHREN?

- Grundsätzlich nur Verantwortliche oder Auftragsverarbeiter mit mehr als 250 Beschäftigten
- Ausnahmsweise ist das Verzeichnis auch bei weniger als 250 Beschäftigten zu führen, wenn die Verarbeitung:
  a) mit einem Risiko für die Betroffenen verbunden ist,
  b) nicht nur gelegentlich erfolgt oder
  c) besondere personenbezogene Daten (Art. 9 Abs. 1) oder Daten im Zusammenhang mit Strafbarkeiten betrifft

WER MUSS EIN VERZEICHNIS FÜHREN?

Die Ausnahmen sind so weit, dass fast jede Stelle darunter fallen dürfte.

- zur Ausnahme a) „Risiko“
  - Risiko bedeutet „ein Risiko“ nicht „erhebliches“ oder „hohes“ Risiko, wie es z.B. bei der Datenschutz-Folgenabschätzung verlangt wird
  - Die Schwelle liegt hier niedriger, so dass bereits eine Videoüberwachung ausreichen kann, da damit ein Risiko für Verhaltens- und Leistungskontrolle bestehen kann
- zur Ausnahme b) „nicht nur gelegentlich“
  - nicht nur gelegentlich liegt vor bei der regelmäßigen Verarbeitung von Kunden- oder Beschäftigtendaten
- zur Ausnahme c) „besondere personenbezogene Daten“
  - Jeder Arbeitgeber dürfte über Gesundheitsdaten seiner Beschäftigten verfügen

VORGEHENSWEISE

- Das Verzeichnis ist Teil der Dokumentation (Rechenschaftspflicht, Art. 5 Abs. 2)
  - dient als Grundlage für eine strukturierte Datenschutzdokumentation
- Struktur: Die Angaben im Verzeichnis sind
  - Stammdaten und
  - Daten für jedes einzelne Verfahren
- Es gibt Muster (auch elektronische) zur Erstellung des Verzeichnisses
- Der Datenschutzbeauftragte kann, muss das Verzeichnis aber nicht erstellen / führen; es ist Aufgabe des Verantwortlichen oder Auftragsverarbeiters

BETROFFENENRECHTE

- Überblick
- Was sind die wichtigsten Betroffenenrechte in der Praxis?
- Wie werden sie gewahrt?

Permission	Intervention	Information	Petition	Kompensation
Einwilligung	Widerruf der Einwilligung Widerspruch Löschung Vergessenwerden Einschränkung der Verarbeitung Berichtigung	Auskunfts- und Einsichtsrechte Transparenz-pflichten Datenpannen Daten-übertragbarkeit	Datenschutz-beauftragter Aufsichtsbehörde	Haftung und Schadensersatz

Systematisierung nach *Franck*, RDV 2016, S. 111

TRANSPARENTE INFORMATION, ART. 12

- Form- und Verfahrensvorschrift zu den Betroffenenrechten, insbes. zu den Informationspflichten der Art. 13 und 14
- Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, Abs. 1
- Schriftlich, elektronisch oder in anderer Form, Abs. 1
- Betroffenenrechte nach Art. 15 bis 22: Frist 1 Monat, Verlängerungsmöglichkeit um 2 Monate unter Angabe der Gründe, Abs. 3
- Unentgeltlichkeit, Abs. 5 – Ausnahme bei Exzess, häufiger Wiederholung, offensichtlicher Unbegründetheit
- Bildsymbole als Möglichkeit der Information, Abs. 7, 8

INHALT DER INFORMATIONSPFLICHT ART. 13 DSGVO

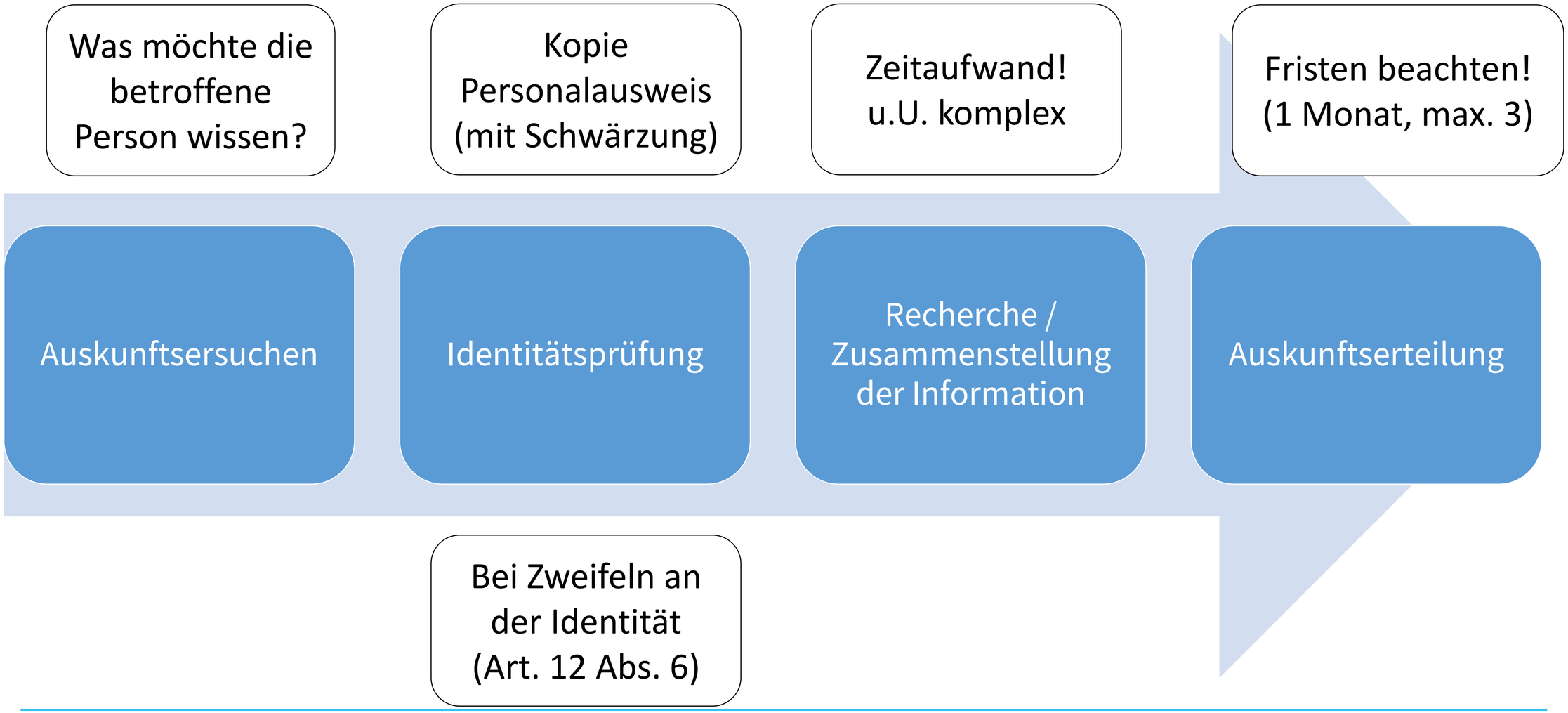
1. Kontaktdaten des Verantwortlichen und der/des Datenschutzbeauftragten
2. Verarbeitungszweck
3. Rechtsgrundlage für die Datenerhebung
4. Absicht, die personenbezogenen Daten an Empfänger in einem Drittland oder an eine internationale Organisation zu übermitteln
5. Empfänger der Daten
6. Speicherdauer
7. Betroffenenrechte
8. Bestehen einer automatisierten Entscheidungsfindung (inklusive Profiling)
9. Grundlage für die Bereitstellung der Daten und Folgen bei Nichtbereitstellung der personenbezogenen Daten

AUSKUNFTSRECHT, ART. 15 UND § 34 BDSG

1) Recht auf Auskunft, ob der Verantwortliche personenbezogene Daten verarbeitet hat (Art. 15 Abs. 1 und 2)
   - Soweit keine personenbezogenen Daten verarbeitet wurden, ist dies der betroffenen Person mitzuteilen
   - Der Umfang der Daten, die in einer Auskunft erhalten sein müssen ergibt sich aus Art. 15 Abs. 1 und 2
2) Recht auf Kopie (Art. 15 Abs. 3)
   - Gibt der betroffenen Person ein Recht auf Kopie von Daten, die Gegenstand der Verarbeitung sind
   - Wird der Antrag elektronisch gestellt, ist die Kopie in gängigem elektronische Format zur Verfügung zu stellen
3) Auskunft und Kopie sind grundsätzlich unentgeltlich (siehe aber Art. 12 Abs. 5, Art. 15 Abs. 3)

AUSKUNFTSPROZESS

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences



ANSPRUCH AUF KOPIE, ART. 15 ABS. 3

- Eigenständiger Anspruch neben dem Auskunftsanspruch (Abs. 1)
- In der Verwaltung kann die betroffene Person nicht nur Auskunft über ihre Daten (z.B. „gespeicherte Stammdaten“) verlangen, sondern eine Kopie aus der Akte, auch der elektronischen Akte (z.B. PDF, Screenshots)
  - ➢ weitreichender Anspruch: kann großen Aufwand verursachen
  - ➢ umfasst Anspruch auf elektronische Kopie (z.B. PDF)
- Ausnahmen vom Anspruch:
  1) Wenn Rechte Dritter entgegenstehen (z.B. Namen anderer Personen in Kopie), Art. 15 Abs. 4
  2) Backup-Daten (weil nicht Gegenstand der Verarbeitung) - *umstritten* -,
  3) Daten, die wegen gesetzlicher Pflichten aufbewahrt werden - *umstritten* -,
  4) Wissenschafts-, Forschungs-, Statistikdaten (s. § 27 Abs. 2 BDSG) - *umstritten* -,
  5) Archivgut (bei öffentlichem Archivzweck, s. § 28 Abs. 2 BDSG) – *umstritten* -.

DATENSCHUTZFOLGENABSCHÄTZUNG

- Was ist eine DSFA?
- Wann muss man sie durchführen?
- Wer ist dafür zuständig?

WANN MUSS EINE DSFA DURCHGEFÜHRT WERDEN?

- Grundregel in Art. 35 Abs. 1: Wenn die Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, insbesondere
  - bei Verwendung neuer Technologien, oder
  - aufgrund der Art,
  - des Umfangs,
  - der Umstände und
  - der Zwecke
  - der Verarbeitung.

WANN MUSS EINE DSFA DURCHGEFÜHRT WERDEN?

Insbesondere nach Art. 35 Abs. 3 bei:

a) systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen

WANN MUSS EINE DSFA DURCHGEFÜHRT WERDEN?

(Fortsetzung)

b) umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z.B. Videoüberwachung)

WANN MUSS EINE DSFA DURCHGEFÜHRT WERDEN?

Nach ErwGr. 91, wenn Verarbeitungsverfahren eingesetzt werden :

- bei denen den Betroffenen die Ausübung ihrer Rechte erschwert wird, (insbes. bei kaum spürbaren oder wenig transparenten Verfahren),
- die nach Auffassung der zuständigen Aufsichtsbehörde wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, (insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen).

WANN MUSS EINE DSFA DURCHGEFÜHRT WERDEN?

Leitfaden WP 248 der Art. 29-Gruppe sieht folgende Beurteilungskriterien vor, bei denen zwangsläufig eine Datenschutz-Folgeabschätzungen durchgeführt werden müssen:

a) Bewertung und Einstufung (Scoring) einschließlich Prognosen und Profilerstellung

b) Automatische erfolgende Entscheidungen mit rechtlichen oder ähnlich signifikanten Auswirkungen für Betroffene

c) Systematisches Monitoring

d) Sensitive, insbesondere personenbezogene Daten

e) Umfangreiche Datenmengen

WANN MUSS EINE DSFA DURCHGEFÜHRT WERDEN?

(Fortsetzung)

f) Vergleich oder Kombination von Datensätzen

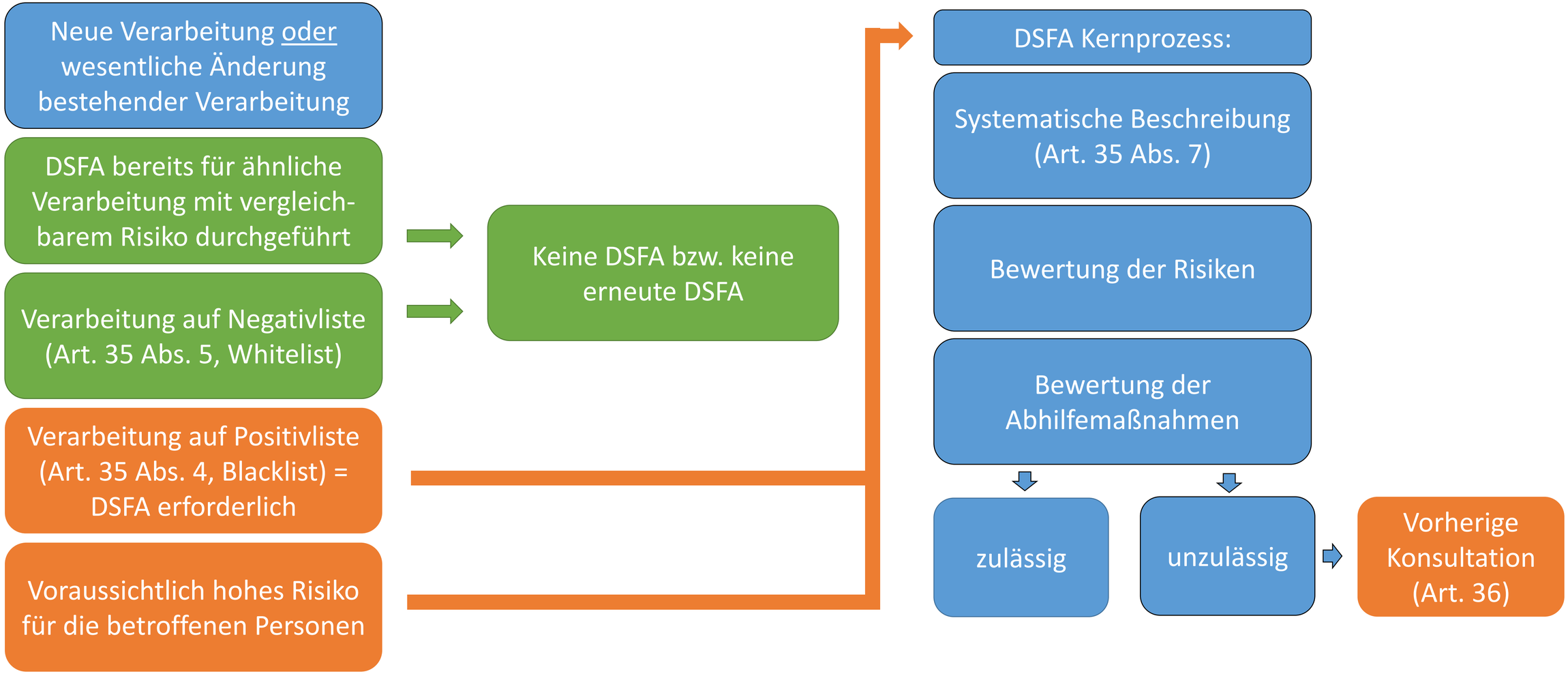
g) Daten ungeschützter Betroffener

h) Einsatz innovativer Technologien oder neuartiger organisatorischer Lösungen

i) Datentransfers in Länder außerhalb der EU (Drittländer)

j) Verhinderung, dass die betroffene Person ein Recht ausüben oder eine Dienstleistung oder einen Vertrag ausführen kann

VORGEHENSWEISE - ABLAUFSCHEMA



WER FÜHRT DIE DSFA DURCH?

- Verantwortlicher führt die DSFA durch, Art. 35 Abs. 1
  - ➢ Leitung muss die Aufgabe einer Stelle zur Erledigung zuweisen
- DSB hat nur Beratungsfunktion
  - ➢ Art. 39 Abs. 1 lit. c) zur Aufgabe des DSB: „Beratung - auf Anfrage - im Zusammenhang mit der DSFA und Überwachung ihrer Durchführung gemäß Art. 35“
  - ➢ Art. 35 Abs. 2: „Verantwortlicher holt bei Durchführung der DSFA den Rat des DSB ein“
- Es sollte ein Team gebildet werden, bestehend aus
  - ➢ IT / IT-Sicherheitsbeauftragte/r
  - ➢ Fachabteilung / Fachbereich, der die Verarbeitung verantwortet
  - ➢ DSB

MELDEPFLICHT BEI DATENPANNEN

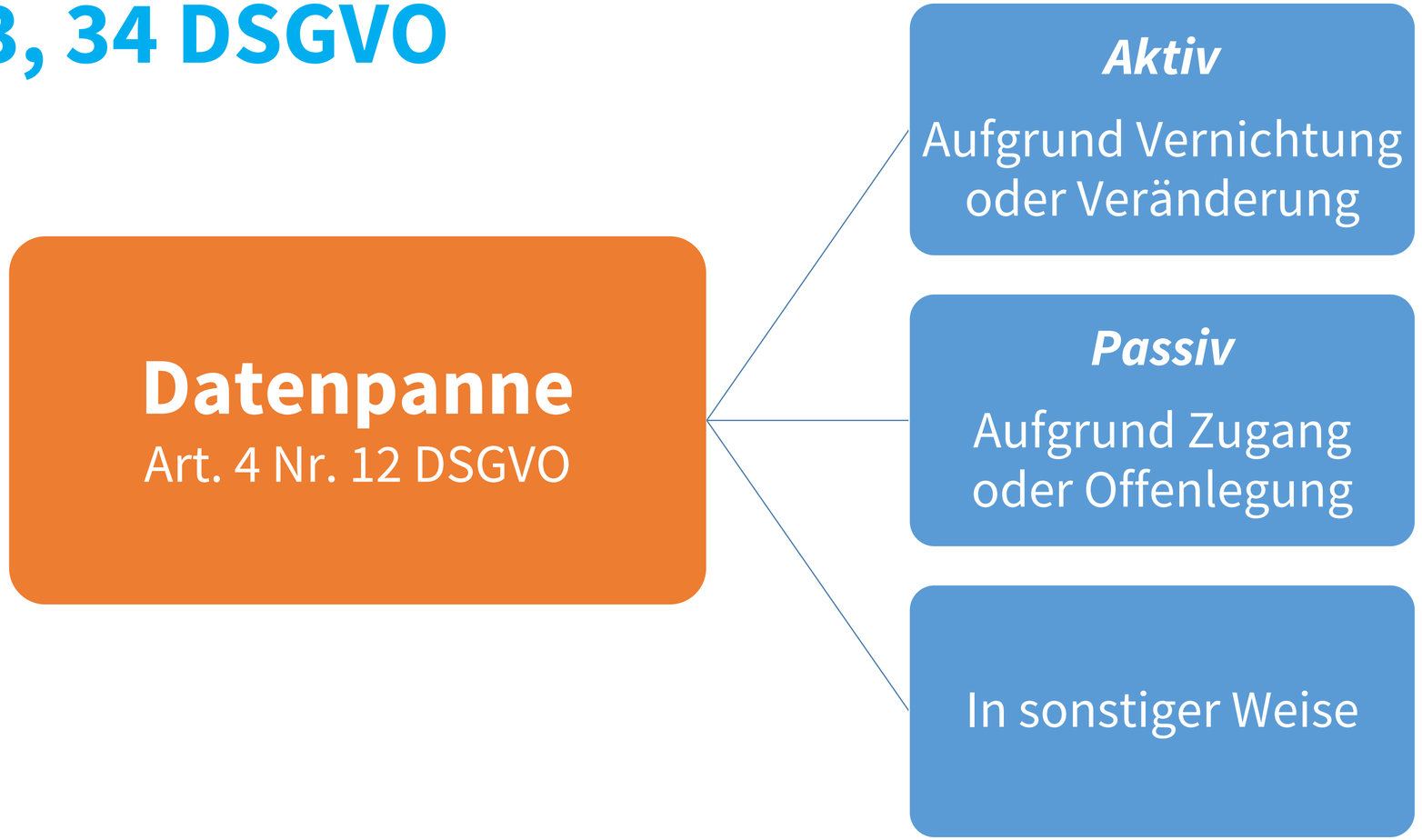
- Was ist eine Datenpanne?
- Was ist bei einem Verdacht auf eine Datenpanne durch wen zu tun?
- Was ist bei Vorliegen einer Datenpanne zu tun?

DATENPANNEN, ART. 4 NR. 12 DSGVO

„Verletzung des Schutzes personenbezogener Daten“ = Datenpanne

- Verletzung der Sicherheit, die,
  - ob unbeabsichtigt oder unrechtmäßig,
- zur Vernichtung, zur Veränderung, oder
- zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt.

UMGANG MIT DATENPANNEN ART. 33, 34 DSGVO



UMGANG MIT DATENPANNEN
RT. 33, 34 DSGVO

Risikoeinschätzung

Besteht ein Risiko für die Rechte und Freiheiten der betroffenen Personen?

UMGANG MIT DATENPANNEN
ART. 33, 34 DSGVO

Meldepflicht

gegenüber der Aufsichtsbehörde

Art. 33 DSGVO

Unterschiedliche Voraussetzungen:

1. Art des Risikos
2. zeitlich
3. inhaltlich
4. formal

gegenüber den Betroffenen

Art. 34 DSGVO

CHECKLISTE ZUR PRÄVENTIVEN ORGANISATION

✓Schwachstellenanalyse und Sicherungsmaßnahmen (Verschlüsselung mobiler Datenträger, Laptop, USB, Smartphone,…)

✓Prüfung/Erstellung Richtlinie für den Umgang mit Datenschutzvorfällen

- Meldepflicht für Mitarbeiter
- Bildung eines Datenschutzvorfall-Teams, das den DSB einschließt
- Klärung des Sachverhalts durch das Team
- Abwägung/Prognose schwerwiegender Beeinträchtigung

CHECKLISTE ZUR PRÄVENTIVEN ORGANISATION

- Information der Geschäftsleitung
- Dialogaufnahme mit der Datenschutzaufsicht
- Prüfung Strafanzeige/-antrag
- Vorsorgliche Information der Aufsichtsbehörde bei Vorliegen eines Art. 33/34 DSGVO-Falles

✓Sensibilisierung der Mitarbeiter

✓Auftragsdatenverarbeiter (Art. 28 DSGVO) einbeziehen

✓Kontaktweg zur Datenschutzaufsicht klären

VERSCHIEDENES UND FRAGEN

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

VIELEN DANK!

Dr. Martin Eßer • Manfred Höffken

datenschutzbeauftragte@h-brs.de