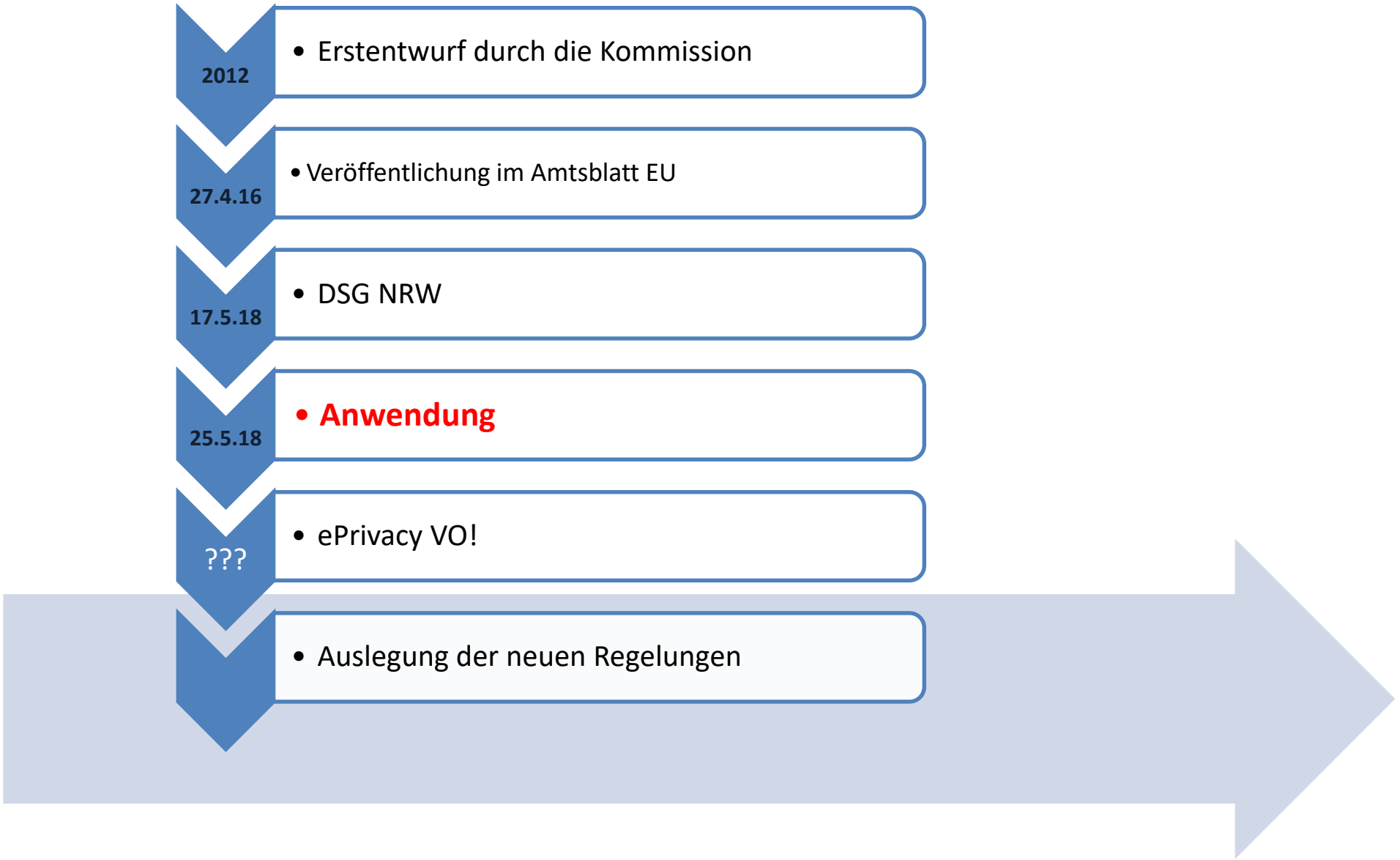
Europäische Datenschutzreform

DATENSCHUTZ-
BEAUFTRAGTER DSB

Zeitablauf DS-GVO



Voraussetzungen der Anwendung des Datenschutzrechts

Verarbeitung in „Dateisystem“

Personenbezogene Daten natürlicher Personen

Personenbezogene Daten sind alle Angaben, die sich auf eine identifizierte oder aber auch nur identifizierbare Person beziehen.

Geburtsjahr

Telefon-
nummer

Wohn-
verhältnisse

Name

Kreditkarten-
nummer

Vermögens-
verhältnisse

Gehalt

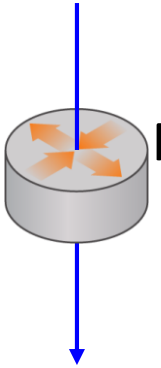
Adresse

Personenbezogene Daten

Identifiziert ist eine Person, wenn sich ihre Identität direkt aus den Daten selbst ergibt.

Identifizierbar wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Informationen feststellbar wird.

IP Adresse



Providerabfrage

Besondere personenbezogene Daten

Weitaus strengere Regeln gibt es für den Umgang mit sogenannten besonderen Arten personenbezogener Daten, da diese besonders schützenswert sind.

Politische Meinung

Ethnische Herkunft

Genetische und Biometrische Daten

Sexual-leben

Gewerkschafts-zugehörigkeit

Religiöse Überzeugung

Gesundheit

Beispiele datenschutzrelevanter Verarbeitungen

Befragungen	Interviewdaten	Videoaufzeichnungen zu Forschungszwecken
Projektabrechnungen	Adressdatenbestände in Lehrstühlen Newsletter	Prüfungsverwaltung
Bewerbungs- und Berufungsverfahren	Selbstgenutzte Kooperationsplattformen	Veröffentlichte Informationen auf Webseiten

„Verarbeitung“?

Erheben	Erfassen	Organisieren	Ordnen
Speichern	Anpassen oder Verändern	Auslesen	Abfragen
Verwenden	Offenlegung durch Übermittlung	Verbreiten oder andere Form der Bereitstellung	Abgleich oder die Verknüpfung
	Einschränken	Löschen oder die Vernichtung	

Vorrang Verordnungen - EU-Verordnung vor nationalem Recht

BISHER

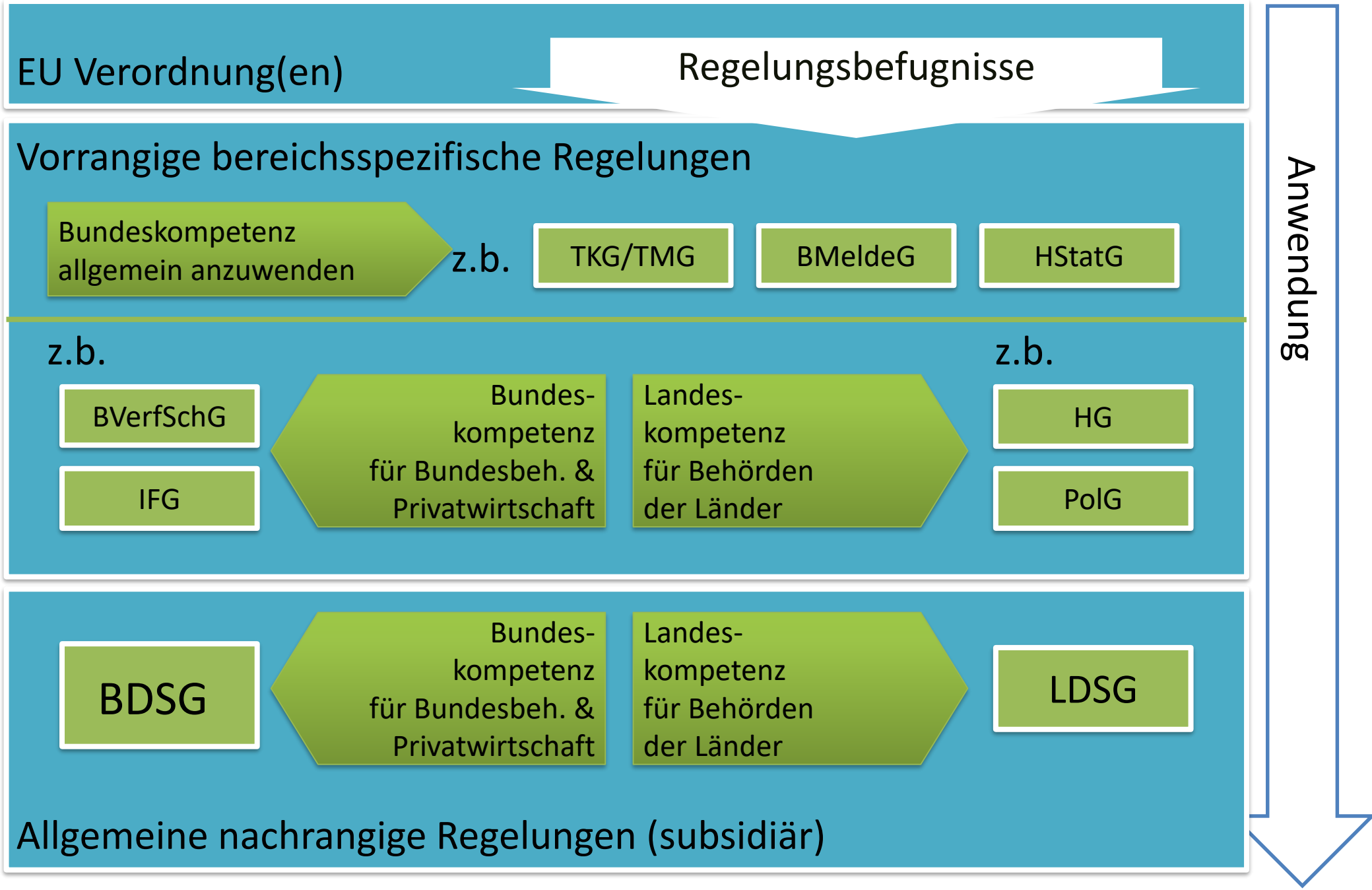
- DATENSCHUTZ-RICHTLINIEN
- Richtlinie = Umsetzung durch Mitgliedsstaaten mittels nationalem Gesetz
- bspw. RL 95/46 EG => Umsetzung im BDSG und DSG NRW

NEU

- VERORDNUNG = UNMITTELBARE GELTUNG IN JEDEM EU-MITGLIEDSSTAAT
- EU-Verordnung = grds. Anwendungsvorrang vor jedem nationalen Gesetz → kein Umsetzungsgesetz im nationalen Recht nötig
- sofern in VO vorgesehen, dann nationale Regelungen möglich
  - bspw. generelle Öffnungsklausel für öffentlichen Bereich
  - bspw. spezielle Öffnungsklauseln wie für Beschäftigten-datenschutz
  - bspw. sog. ePrivacy-VO (Nachfolge RL 2002/58/EG)
- Ausgestaltungspflicht durch nationalen Gesetzgeber, sofern durch VO angeordnet

→ NEUER RECHTSRAHMEN MIT ANWENDUNGSVORRANG VOR NATIONALEN GESETZEN

→ KEINE DEUTSCHE AUSLEGUNG, SONDERN EU-AUSLEGUNG


EU Verordnung(en)
Regelungsbefugnisse
Vorrangige bereichsspezifische Regelungen
Bundeskompetenz allgemein anzuwenden
z.b.
TKG/TMG
BMeldeG
HStatG
z.b.
BVerfSchG
IFG
Bundes-kompetenz für Bundesbeh. & Privatwirtschaft
Landes-kompetenz für Behörden der Länder
z.b.
HG
PolG
BDSG
Bundes-kompetenz für Bundesbeh. & Privatwirtschaft
Landes-kompetenz für Behörden der Länder
LDSG
Allgemeine nachrangige Regelungen (subsidiär)
Anwendung

DSG NRW

Beschluss 17.5.2018

- **Regelung gemäß DS-GVO - Verordnung (2016) 679**
- **Auch Regelung der Justizrichtlinie: Richtlinie (2016) 680**

- **Struktur wie BDSG:**
  - **Teil 3 Justizrichtlinie – nicht anzuwenden!**

Datenschutzgrundsätze

Bisher eher versteckt – Neu Artikel 5 DSGVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Zweckbindung

Datenminimierung

Richtigkeit

Speicherbegrenzung

Integrität und Vertraulichkeit

Rechenschaftspflicht

Rechtmäßigkeit:
Erlaubnis für Verarbeitungen nach Art. 6

Einwilligung

Vertragserfüllung oder vorvertraglich erforderlich

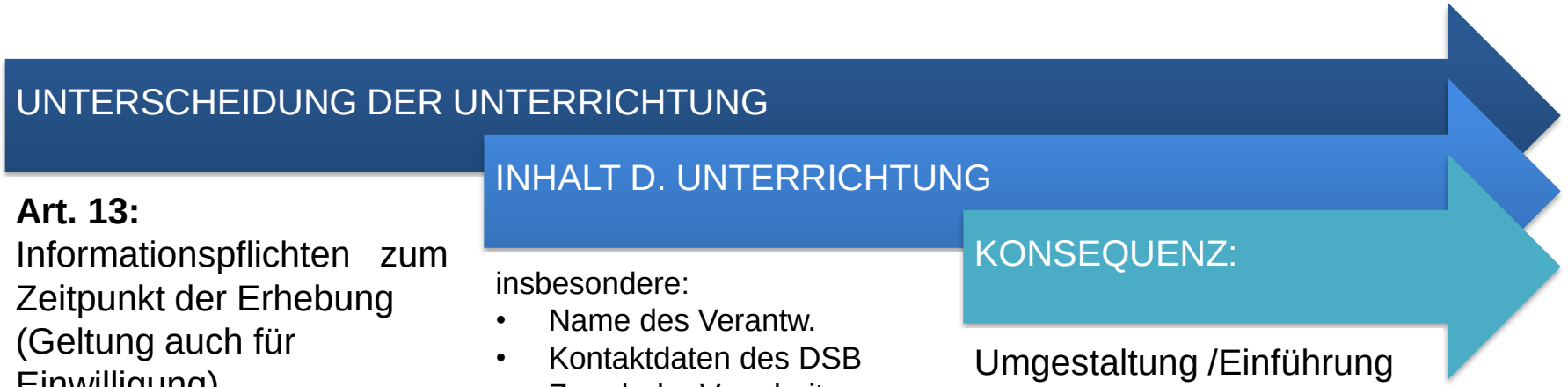
Rechtliche Verpflichtung zur Verarbeitung

Lebenswichtige Interessen des Betroffenen/Dritter

Erforderlich für öffentliche Aufgabe

Überwiegende berechtigte Interessen

INFORMATIONSPFLICHTEN



Art. 13:
Informationspflichten zum Zeitpunkt der Erhebung (Geltung auch für Einwilligung)
Art. 14: Wenn die Daten nicht bei der betroffenen Person erhoben werden
Art. 15:
Auskunftsansprüche des Betroffenen

insbesondere:

- Name des Verantw.
- Kontaktdaten des DSB
- Zweck der Verarbeitung sowie Rechtsgrundlage
- Empfänger von Daten
- Absicht der Drittland-übermittlung und Grundlage der Zulässigkeit

Umgestaltung /Einführung von Informationsblättern
Datenschutzerklärung
Infoseiten zu Masken

Datenschutzgrundsätze

Bisher eher versteckt – Neu Artikel 5 DSGVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Zweckbindung

Datenminimierung

Richtigkeit

Speicherbegrenzung

Integrität und Vertraulichkeit

Rechenschaftspflicht

Zweckbindung

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;

(Art 5 Abs. 1 Buchst b)

Zweckbindung - aufgehoben DS-GVO

- Für die Forschung und Statistik
- Bei Zweckkompatibilität: Berücksichtigung von
  - jeder Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
  - dem Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
  - der Art der personenbezogenen Daten (..besonders vertrauliche Daten..),
  - den möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
  - dem Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Zweckbindung - Ausnahmen DSG NRW

Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit

Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person

Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten und Unterrichtung der Strafverfolgung geboten

Überprüfung der Angaben der betroffenen Person aufgrund tatsächlicher Anhaltspunkte für deren Unrichtigkeit

Wahrung eines rechtlichen Interesses eines Dritten und das Geheimhaltungsinteresse der betroffenen Person nicht überwiegt oder Widerspruch liegt vor

öffentliches Interesse

(ohne Widerspruch)

Übermittlung § 8 DSG NRW

(1) Die Verantwortung für die Zulässigkeit einer Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. Erfolgt die Übermittlung aufgrund eines Ersuchens einer öffentlichen Stelle, trägt diese die Verantwortung. Die übermittelnde Stelle hat dann lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn hierzu im Einzelfall Anlass besteht. Die ersuchende Stelle hat in dem Ersuchen die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

Datenminimierung

- Erforderlichkeitsprinzip
  - Daten sind erst dann erlaubt, wenn sie für den Zweck erforderlich sind.
  - Ist die Aufgabe auch ohne die Daten zu erfüllen?

Speicherbegrenzung: Löschung

- Oft keine Aufbewahrungsverpflichtungen!

- Grundregel:

Daten sind zu löschen, sobald der Zweck, für den sie erfasst wurden nicht mehr vorliegt.

Grundsätzlich: Aufbewahrungsverpflichtung?

- Verantwortlichkeit für die Aufbewahrung
- Aufbewahrung nur einmal!!
- Vernichtung von Akten – Universitätsarchiv (Anbietungspflicht s. Aufbewahrungsrichtlinie)
- Aufbewahrungsordnungen regeln die Dauer der Aufbewahrung – für Aufbewahrungswürdiges:
  - 30 Jahre Zweitschriften von Zeugnissen/Urkunden
  - 10 Jahre Listen(!) zu Prüfungsvorleistungen (Nachweise)
  - 2 Jahre Prüfungsarbeiten (Rückgabe an Prüfling)
  - 5 Jahre sonstiges

Besondere Verpflichtungen:
Personal, Buchungsbelege,

TECHNISCH-ORGANISATORISCHE MAßNAHMEN „Sicherheit der Verarbeitung“, Art. 32

- Zielsetzung
  - Gewährleistung eines dem *Risiko* angemessenen Schutzniveaus

- Umsetzung durch geeignete technische und organisatorische Maßnahmen, die getroffen werden
  - unter Berücksichtigung des Stands der Technik,
  - der Implementierungskosten
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
  - sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten
  - Beachten: auch im Kontext der Auftragsverarbeitung

- *Wesentliche Aufgabe Risikobewertung*

- ***Privacy by Design / Privacy by Default.***

Rechenschaftspflicht

- Beweislastumkehr?
  - Accountability /Responsibilité
- Unter der Gesamtverantwortung zu verarbeiten
- Nachweispflichten
  - Übersicht der Verarbeitungstätigkeiten
  - (erweiterte) Auskunftsrechte der betroffenen Person
  - Informationssicherheits- und Datenschutzmanagement
  - Dokumentation über Datenschutzüberlegungen
  - Dokumentation (Protokollierung) von Verarbeitungen
  - Dokumentation einer Sicherung nach „Stand der Technik“
    - Sicherheitskonzept
  - Nachweise der Einwilligungen

Datenschutzgrundsätze

Bisher eher versteckt – Neu Artikel 5 DSGVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Zweckbindung

Datenminimierung

Richtigkeit

Speicherbegrenzung

Integrität und Vertraulichkeit

Rechenschaftspflicht

Nebenverpflichtungen

Meldepflicht bei Datenschutzverstößen

AUSLÖSER DER MELDEPFLICHT

„Verletzung des Schutzes personenbezogener Daten", Art. 4 Abs. 9

keine Beschränkung auf bestimmte Daten

Meldung an Aufsichtsbehörde, Art. 33

Ausschluss, falls „*voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt*“

➔ grds. Meldepflicht, aber Ausnahmen

Benachrichtigung der betroffenen Personen, Art. 34

Meldepflicht, falls Wahrscheinlichkeit für hohes Risiko

aber dennoch: Ausnahmen möglich

➔ nicht allein ausreichend: Verletzung des Schutzes personenbezogener Daten

- plus: Verlangen der Unterrichtung bzw. Feststellung der Pflicht zur Unterrichtung

Auftragsdatenverarbeitung

- Auftragsverarbeiter ist kein Dritter, Art. 4 Abs. 10

- Verantwortlicher für Verarbeitung bleibt verantwortlich
  - Pflichtinhalte bei der Beauftragung
  - Angemessenheit der Schutzmaßnahmen
  - Nachweis der ausreichenden Schutzmaßnahmen, auch über Verhaltensregeln oder Zertifizierung möglich
  - Einbindung von Subunternehmern formalisierter geregelt

  - gemeinsame Haftung (Art. 28) des Auftraggebers und des Auftragnehmers

- Risiko für Auftragsverarbeiter: Haftung mit Auftraggeber
- Eigene Verarbeitungsübersicht
- Auch bei Fernwartung

BETROFFENENRECHTE

Art. 15: jeweiligen Daten, die Verarbeitungszwecke, die verarbeiteten Daten, Empfänger etc.
i.d.R. unentgeltlich

4 Wochenfrist zur Beantwortung des Auskunftsersuchen!

Auskunftsersuchen elektronisch.

Art 17: Bisher Löschung

Nicht anwendbar.

Weitere

Art. 21 Widerspruchsrecht

Art. 18 Einschränkung der Verarbeitung

Art. 16 Recht auf Berichtigung

Strafen?

Neu Schadensersatz:

- **DSGVO:** Art. 82
- Schadensersatzpflicht ohne Nennung einer Summe

- (Bsp OLG Köln 30.9.2016 (Az. 20 U 83/16): Vergleich auf 90.000 € wegen Unrechtmäßiger Weitergabe von Gesundheitsdaten BU Versicherung an Arbeitgeber)

Strafen?

Strafbewährte Handlungen:

- **DSG NRW nF** § 31

Wer entgegen der Vorschriften, geschützte personenbezogene Daten:

1. erhebt, speichert, unbefugt verwendet, verändert, übermittelt, weitergibt, zum Abruf bereithält, den Personenbezug herstellt oder löscht oder
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung oder Weitergabe an sich oder andere veranlasst.

Deanonymisierung

Strafen?

- **Ordnungswidrig:** DSG NRW nF § 30
- Wer gegen Regeln die genannten Handlungen ausführt. – 50.000 €

- **Straftat:** DSG NRW nF § 31 nahezu wortgleich zur bisherigen Regelung:

(1) Wer in Ausübung seiner Tätigkeit für eine öffentliche Stelle in der in § 30 Absatz 1 genannten Verstöße gegen Entgelt oder in der Absicht sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

Dokumentationspflichten: Verzeichnis von Verarbeitungstätigkeiten, Art. 30

Pflicht für den **Verantwortlichen** (Art. 30 Abs. 1) und Auftragsverarbeiter (Art. 30 Abs. 2)

keine Herausgabepflicht an Jedermann (Stichwort: Jedermannsverzeichnis) -- aber erweiterte Auskunftsrechte

Abweichende Inhalte für Verantwortlichen und Auftragsverarbeiter

gegenüber Aufsichtsbehörde auf Anforderung zur Verfügung stellen

Aufzeichnungen sind schriftlich zu führen, elektronisches Format genügt

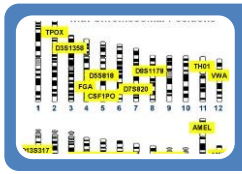
DATENSCHUTZ-FOLGENABSCHÄTZUNG

Privacy Impact Assessment, Art. 35

- durch den für die Verarbeitung Verantwortlichen (Art. 35 Abs. 1)
  - wenn die Form der Verarbeitung *„aufgrund der Art, des Umfangs und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge“* hat
  - Dokumentation der eingesetzten Abhilfemaßnahmen zur Eindämmung des Risikos, einschließlich Nachweisanforderungen

DSFA/DPIA - Hohes Risiko aufgrund

Verwendung neuer Technologien



der Art

des Umfangs

der Umstände

der Zwecke

Vorgegebene Fallkategorien

- Persönlichkeitsbewertung
- Profiling
- umfangreiche Verarbeitung besonderer Kategorien
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Kriterien WP 29

- Können Menschen durch die Technik eingeschätzt oder bewertet werden?
- Finden Entscheidungen mit Rechtswirkung oder ähnlichem automatisiert statt?
- Kann die Verarbeitung als eine systematische Überwachung angesehen werden?
- Werden besonders vertrauliche oder höchst persönliche Daten verarbeitet?
- Wird voraussichtlich ein großer Umfang erreicht?
- Werden vormals getrennte Daten zusammengeführt oder abgeglichen?
- Werden Daten von Schutzbedürftigen verarbeitet?
- Findet eine innovative Nutzung oder der Einsatz neuer Technologien statt?
- Werden betroffene Personen an der Ausübung der Betroffenenrechte behindert?

WESENTLICHSTE ÄNDERUNGEN AN HOCHSCHULEN

Änderung bei den Grundsätzen: Rechtsgrundlagen und Rechenschaftspflicht

Informierungspflicht

Systemeinführungsprozess:
Vorabkontrolle (neu DPIA → Mitbestimmung) (nicht Dokumentationspflicht)

Datenschutzmanagementsysteme

Prozessänderungen: Meldepflicht bei Datenschutzverstoß,
Auskunftsanfragen

Auftragsdatenverarbeitung

Bußgelder

Nächste Schritte

Aufsichtsbehörden	• EU-DA: Standpunkte • Handlungshilfen (DSK!)
Hochschulübergreifende geförderte Projekte	• Best Practice • Materialien erarbeiten • Schulungsmaterial
RUB	• Vorlagen und Beispiele in Projekten mit Verwaltung und Wissenschaftlicher Einrichtung • Erweitern Informationssicherheitsleitlinie