Republik Österreich
Datenschutzbehörde

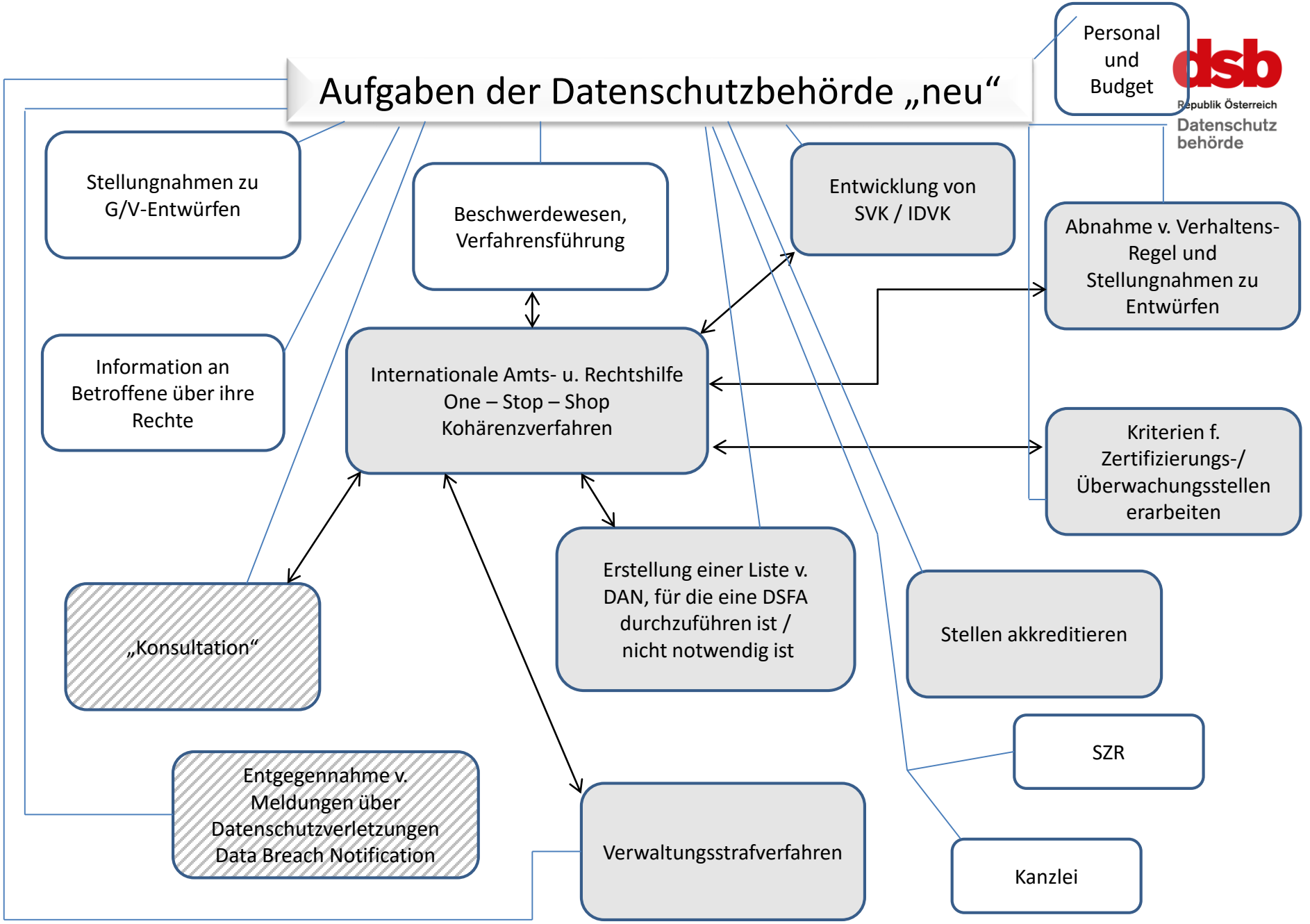
Datenschutzgrundverordnung

Aufgaben und Befugnisse der Behörde
Aufgaben
der datenschutzrechtlich Verantwortlichen

WKO
12. Oktober 2017

Dr. Andrea Jelinek

Aufgaben der Datenschutzbehörde „neu“



Datenschutz-Grundverordnung

- gilt nur für natürliche Personen
- „hinkende Verordnung“
- Zielsetzungen:

  einheitlicher Rechtsschutz

  einheitliche Regeln für Datenverarbeitung

  einheitlicher Vollzug
- detaillierter und umfangreicher als DS-RL

Republik Österreich
Datenschutzbehörde

Aufgaben und Befugnisse der Aufsichtsbehörde nach der DSGVO

Struktur und Unabhängigkeit der Aufsichtsbehörde

Republik Österreich
Datenschutzbehörde

- unabhängige Behörde – keine externen Weisungen
- Funktionsperiode: zumindest vier Jahre
- Personalhoheit und eigenes Budget
- Ausübung der hoheitlichen Befugnisse im eigenen Staatsgebiet
- Keine Zuständigkeit für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen

Räumliche Zuständigkeit der Aufsichtsbehörde

- Zuständigkeit für die Ahndung von Rechtsverletzung auf dem eigenen Staatsgebiet, v.a. wenn
  - der Verantwortliche oder Auftragsverarbeiter seinen Sitz im Staatsgebiet hat
  - es sich um eine Behörde oder einen beliehenen Rechtsträger des Mitgliedsstaates handelt
  - eine Datenanwendung von einem Verantwortlichen oder Auftragsverarbeiter mit Sitz in einem Drittstaat betrieben wird und die Datenanwendung auf Betroffene im eigenen Staatsgebiet abzielt

Aufgaben der Aufsichtsbehörde

Republik Österreich
Datenschutz
behörde

- Anwendung der DSGVO **überwachen und durchsetzen**
- **Beschwerdeverfahren**
- **Zusammenarbeit** mit anderen Datenschutzbehörden
- Meldungen und Auswirkungen iZm Datenschutz-Verletzungen
- „Blacklist“/„Whitelist“ erstellen

Aufgaben der Aufsichtsbehörde

- bei „Vorheriger Konsultation“ beraten
- Standardvertragsklauseln festlegen
- **Informationen über Betroffenenrechte zur Verfügung stellen**
- **Eingabeformulare** bereitstellen
- offenkundig unbegründete oder exzessive Eingaben **ablehnen oder Vorschreibung von Kosten**

Befugnisse der Aufsichtsbehörde

- **Untersuchungsbefugnisse**

  Zutrittsrecht zu Räumlichkeiten
- **Abhilfebefugnisse**:

  Warnung, Verwarnung
- Anweisung Verarbeitungsvorgänge in Einklang mit DSGVO bringen
- Verhängung einer **Geldbuße zusätzlich zu oder statt** einer Abhilfemaßnahme
- **Genehmigungsbefugnisse und beratende Befugnisse:**

  Stellen akkreditieren, Zertifizierungen erteilen

DSGVO Kapitel IV

- Die Aufgaben der (datenschutzrechtlich) Verantwortlichen des öffentlichen und privaten Bereichs (bis dato: Auftraggeber) siehe § 26 DSG (BGBl I Nr.120/2017) rücken stärker in den Focus als in der RL aus dem Jahr 1995

DSGVO

- Überblick über die wesentlichsten Pflichten, welche auf die Verantwortlichen (bzw. auf die Auftragsverarbeiter) im Zuge der DSGVO zukommen (Art 24 ff DSGVO)
- Leitfaden: https://www.dsb.gv.at/datenschutz-grundverordnung

Abschnitt 1:

- „Allgemeine Pflichten“ (Art 24-29)
- Verzeichnis von Verarbeitungsvorgängen (Art. 30)
- Zusammenarbeit mit der Aufsichtsbehörde (Art. 31)

Verzeichnis von Verarbeitungsvorgängen I

- Entfall der DVR-Meldepflicht *(mit 25. Mai 2018)*
- Schriftliches Verzeichnis aller Verarbeitungs-tätigkeiten (=Datenanwendungen)
- Inhalt umfasst unter anderem die Zwecke der Verarbeitung sowie die Kategorien betroffener Personen, Daten, Empfänger. Wenn möglich auch Löschfristen sowie technische und organisatorische Beschreibungen usw.
- Auf Anfrage der Aufsichtsbehörde vorzulegen

Verzeichnis von Verarbeitungsvorgängen II

- Ausnahme: Unternehmen/Einrichtungen mit weniger als 250 Beschäftigten sofern…
  - kein Risiko für Rechte und Freiheiten von Betroffenen,
  - die Verarbeitung nur gelegentlich (!) erfolgt,
  - keine Verarbeitung von sensiblen oder Strafdaten

DVR Online Exportfunktion

- Um einem Auftraggeber die Möglichkeit zu bieten, seine vorhandenen DVR-Meldungen zu sichern, ist es ab sofort möglich, in der Internet-Applikation DVR-ONLINE elektronisch verfügbare Meldungsinhalte sowohl als PDF-Dokumente als auch als XML-Dateien zu exportieren. Hierfür wurden im DVR-ONLINE-Meldebereich des Auftraggebers entsprechende Funktionen (rote Buttons, siehe Screenshot) eingefügt.

DVR Online Exportfunktion

dsb
Republik Österreich
Datenschutzbehörde

Auftraggeber (AG)

DVR-Nummer	0000027 (Registriert)
Auftraggeber	Datenschutzbehörde
Adresse	Hohenstaufengasse 3, 1010 Wien, Österreich

AG-Daten ändern | AG-Daten lesen | Streichen | Exportiere PDF | Exportiere XML

Datenanwendungen (DAN)

Auswahl	Nummer	Bezeichnung/Zweck	Datum	Status
○	0000027/001	REGISTERFÜHRUNG	02.09.1996 00:00	Registriert
○	0000027/002	Aktenverwaltung (Büroautomation)	30.04.2004 00:00	Registriert
○	0000027/003	Öffentlichkeitsarbeit und Informationstätigkeit	30.04.2004 00:00	Registriert
○	0000027/004	Ergänzungsregister für sonstige Betroffene (ERsB) im Sinne des § 6 Abs 4 E-GovG	14.10.2005 00:00	Registriert
○	0000027/005	Bezeichnung: Ergänzungsregister für natürliche Personen Zweck: Ergänzungsregister zur Errechnung von Stammzahlen für natürliche Personen, die nicht im zentralen Melderegister eingetragen sind. Es dient der Aufzeichnung von Daten, die für den Nachweis einer eindeutigen Identität (§ 2 Z 2 E-GovG) notwendig sind.	14.04.2011 00:00	Registriert
○	0000027/006	Stammzahlenregister Zweck: Errechnung von Stammzahlen, bereichsspezifischen Personenkennzeichen und verschlüsselten bereichspezifischen Personenkennzeichen. Es werden Identitätsdaten aus dem zentralen Melderegister und Identitätsdaten aus dem Ergänzungsregister für natürliche Personen verwendet, um Personen eindeutig zu identifizieren. Es werden Identitätsdaten von öffentlichen und privaten Auftraggebern mit den Identitätsdaten des zentralen Melderegisters und den Identitätsdaten des Ergänzungsregisters für natürliche Personen verwendet, um Personen eindeutig zu identifizieren. Für eindeutig identifizierte Personen kann sowohl eine Stammzahl auf Grundlage der ZMR Zahl oder der ERnP Ordnungsnummer als auch bereichsspezifische Personenkennzeichen und verschlüsselte bereichsspezifische Personenkennzeichen berechnet werden. Stammzahlen werden nur an Bürgerkartenregistrierungsstellen überlassen, die als Dienstleister der Stammzahlenregisterbehörde im Zuge der Eintragung der Stammzahl in ein geeignetes elektronisches Medium zur Aktivierung der Bürgerkartenfunktion tätig werden, oder an öffentliche Auftraggeber zur unverzüglichen Berechnung eines bereichsspezifischen Personenkennzeichens und/oder eines verschlüsselten bereichsspezifischen Personenkennzeichens übermittelt. Bereichsspezifische Personenkennzeichen und/oder verschlüsselte bereichsspezifische Personenkennzeichen werden nur an Auftraggeber übermittelt, deren Berechtigung zum Bezug dieser Personenkennzeichen zuvor überprüft wurde. Das Stammzahlenregister speichert keine Identitätsdaten, Stammzahlen oder bereichsspezifische Personenkennzeichen über den Zeitraum hinaus, der für die Errechnung dieser Kennzeichen erforderlich ist.	15.04.2011 00:00	Registriert
○	0000027/007	Vollmachtenservice Zweck: Register zur Aufzeichnung von erteilten und widerrufenen Vollmachten auf der Bürgerkarte. Es dient der Aufzeichnung von Daten, die für die Nachvollziehbarkeit und Beauskunftung von erteilten und widerrufenen Vollmachten (§ 5 E-GovG) notwendig sind. Jedermann kann anhand der Seriennummer des Vertretungsdatensatzes den Status einer Vollmacht überprüfen. Die Applikation errechnet das bereichsspezifische Kennzeichen ZP („zur Person") anhand der aus den Bürgerkarten ausgelesenen Stammzahl. Die Stammzahlen von natürlichen Personen werden nicht gespeichert, sondern sofort nach der bPK Berechnung unwiderruflich gelöscht.	07.06.2011 00:00	Registriert
○	0000027/008	IVS vom 22.6.16	22.06.2016 13:27	Registriert

DAN-Daten ändern | DAN-Daten lesen | DAN-Erstmeldung | Streichen | Stornieren | Registerauszug | Exportieren aller DANs als PDF | Exportieren einzelner DAN als PDF
Exportieren aller DANs als XML | Exportieren einzelner DAN als XML

Abschnitt 2

- „Sicherheit personenbezogener Daten“
- Sicherheit der Verarbeitung (Art. 32)
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33)
- Information an betroffene Personen (Art. 34)

Meldung von Verletzungen an die Aufsichtsbehörde

Republik Österreich
Datenschutzbehörde

- Meldung an die DSB, wenn durch eine Datenschutzverletzung ein Risiko für die Rechte und Freiheiten der Betroffenen besteht.
- Unverzüglich *(möglichst binnen 72 Std.)*
- Samt aller notwendigen Informationen zu dem Vorfall (Beschreibungen, Dokumentation)

Benachrichtigung der von einer Verletzung betroffenen Person

Republik Österreich
Datenschutzbehörde

- Meldung an die Betroffenen, wenn durch eine Datenschutzverletzung ein hohes Risiko für die Rechte und Freiheiten besteht.
- Ohne ungebührliche Verzögerungen

Abschnitt 3

- „Datenschutz-Folgenabschätzung und vorherige Konsultation“
- Datenschutzfolgenabschätzung (Art. 35)
- Vorherige Konsultation (Art. 36)

Datenschutzfolgenabschätzung

- Vor Inbetriebnahme eines neuen Datenverarbeitungssystems durchzuführen
- Wenn unter Berücksichtigung aller Umstände ein hohes Risiko für die Rechte und Freiheiten von Personen
- Insbesondere bei Profiling, der Verwendung von sensiblen oder Strafdaten, Überwachung öffentlicher Plätze
- DSB erhält VO-Ermächtigung zur Erstellung einer Positiv- und (optional) einer Negativliste

Konsultation

- Vor Inbetriebnahme eines neuen Datenverarbeitungssystems.

1. *Datenschutzfolgenabschätzung durchgeführt*
2. *Hohes Risiko*
3. *Keine Maßnahmen*

=> DSB kann schriftliche Empfehlungen erteilen, wenn Datenverarbeitung nicht im Einklang mit der DSGVO

Datenschutzfolgeabschätzung

- Möglichkeit der Vorwegnahme der Datenschutzfolgeabschätzung (Art. 35 Abs 10 DSGVO) im Rahmen legistischer Maßnahmen.
- Rechtsvorschriften müssen den konkreten Verarbeitungsvorgang regeln und im Rahmen der Folgenabschätzung der Gesetzwerdung wird auch eine Datenschutzfolgeabschätzung durchgeführt

White/ Black List

- „Blacklist“ (auch Positivliste genannt) – Liste von Datenverarbeitungssystemen, die jedenfalls einer Datenschutzfolgeabschätzung bedürfen – sind dem Datenschutzausschuss zu übermitteln
- Art 29 DS Gruppe hat guidelines dazu erarbeitet, Beschluss erfolgte am 4.10.2017, auch auf Website der DSB veröffentlicht
- DSB kann gem Art 35 Abs 5 auch White List (Negativliste) erstellen (siehe Standard VO derzeit)

White/ Black List

- „Standard“ tritt außer Kraft mit 24.5.2018
- DSB hat im DSG Verordnungsermächtigung erhalten (§ 21 Abs 2 DSG)
- DSB arbeitet an Erstellung einer „White List“
- Absicht: Begutachtungsbeginn noch 2017

Abschnitt 4:

- „Datenschutzbeauftragter“
- Benennung eines Datenschutzbeauftragten (Art. 37)
- Stellung des Datenschutzbeauftragten (Art. 38)
- Aufgaben des Datenschutzbeauftragten (Art. 39)

Benennung eines Datenschutzbeauftragten

Republik Österreich
Datenschutz behörde

- Zwingend für Behörden und öffentliche Stellen (Ausnahme Gerichte im Rahmen ihrer justiziellen Tätigkeit), oder
  - wenn Kerntätigkeit systematische Überwachung von Personen
  - wenn Kerntätigkeit die Verarbeitung von sensiblen Daten, oder Strafdaten
- Sonst optional; Kontaktdaten des Beauftragten sind zu veröffentlichen und der DSB mitzuteilen

Datenschutzbeauftragter

- Art 37 ff und § 5 DSG
- Weisungsfrei bezüglicher der Ausübung dieser Tätigkeit
- Kommuniziert mit DSB
- Berichtet unmittelbar oberster Managementebene
- Wird in technische Entwicklungsmaß-nahmen eingebunden……

Republik Österreich
Datenschutzbehörde

Rechtsschutz und Sanktionen nach der DSVGO

Rechtsschutz nach der DSVGO

- Recht auf Beschwerde bei einer Aufsichtsbehörde

- Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde: Bescheidbeschwerde (gegen verbindliche Entscheidungen der Aufsichtsbehörde) sowie Säumnisbeschwerde

- Recht auf gerichtlichen Rechtsbehelf gegen Verantwortlichen oder Auftragsverarbeiter

Geldbußen

- wirksam, verhältnismäßig und abschreckend
- Geldbußen zusätzlich oder anstelle von Abhilfemaßnahmen nach Art. 58 Abs. 2
- Art. 83 Abs. 7 DSGVO: Mitgliedstaat kann festlegen, ob und in welchem Umfang gegen Behörden/öffentliche Stellen Geldbußen verhängt werden können
  - § 30 Abs. 5 DS-Anpassungsgesetz 2018: keine Geldbußen gegen Behörden/öffentliche Stellen verhängen
- „angemessene Verfahrensgarantien“: gerichtliche Rechtsbehelfe

Recht auf Schadenersatz

- Jede Person, der wegen Verstoß gegen DSGVO Schaden entstanden ist
- Haftung: „jeder an einer Verarbeitung beteiligte Verantwortliche“, der Schaden verursacht
- Haftungsbefreiung: „keinerlei“ Verantwortung für Schadenseintritt
- solidarische Gesamthaftung - interner Regress möglich

Weiterführende Informationen

- Website der DSB: www.dsb.gv.at

  → Rubrik – Europa & Internationales: Art-29-Gruppe

  → Aktuelle **Guidelines**!!!

  http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Newsletter der DSB: online bestellen

- Datenschutzbericht 2016: abrufbar auf der Website der DSB

- Leitfaden zur DSVGO auf der Website der DSB

Literaturauswahl zur DSGVO

(Stand: September 2017, kein Anspruch auf Vollständigkeit)

- *Feiler/Forgó*, EU-Datenschutz-Grundverordnung (Kommentar)
- *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg.), Kommentar zur Datenschutz-Grundverordnung
- *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (Praxishandbuch)
- *Paal/Pauly* (Hrsg.), Datenschutz-Grundverordnung (Kommentar)
- *Pollirer/Weiss/Knyrim/Haidinger*, DSGVO (Textausgabe)
- *Sydow* (Hrsg.), Europäische Datenschutzgrundverordnung (Kommentar)