DATENSCHUTZ-GRUNDVERORDNUNG

Kapitel 4

Verantwortlicher und Auftragsverarbeiter

Kapitel 4 - Verantwortlicher und Auftragsverarbeiter

- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Gemeinsam Verantwortliche
- Auftragsverarbeiter
- Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
- Verzeichnis von Verarbeitungstätigkeiten
- Sicherheit der Verarbeitung
- Meldung von Verletzungen des Schutzes pDaten an die Aufsichtsbehörde
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
- Datenschutz-Folgenabschätzung
- Vorherige Konsultation
- Benennung eines Datenschutzbeauftragten
- Stellung des Datenschutzbeauftragten
- Aufgaben des Datenschutzbeauftragten
- Verhaltensregeln
- Überwachung der genehmigten Verhaltensregeln
- Zertifizierung
- Zertifizierungsstellen

Allgemeine Pflichten

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 25 (1): *„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.“*

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Verantwortlicher

legt fest

geeignete technische und organisatorische Maßnahmen

sind ausgelegt auf

Datenschutzgrundsätze:

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

+

Garantien

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

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 25 (2): *„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****.“*

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der genannten Anforderungen nachzuweisen.

Gemeinsam Verantwortliche

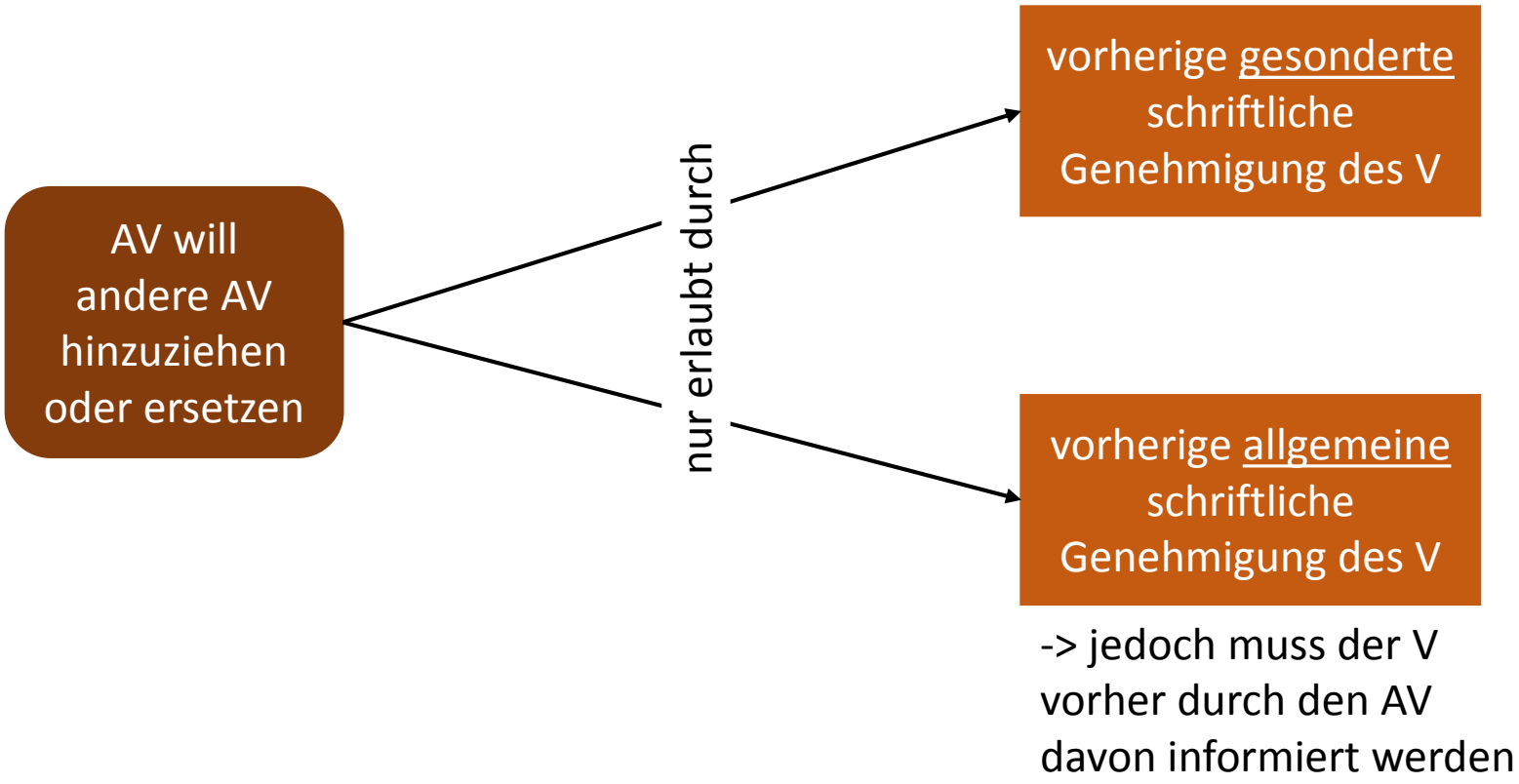
- Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**.
- Sie legen **in einer Vereinbarung** in transparenter Form fest, **wer von ihnen welche Verpflichtung** gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt.
- In der Vereinbarung kann eine **Anlaufstelle** für die betroffenen Personen angegeben werden.

Gemeinsam Verantwortliche

- Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. **Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt**.
- **Ungeachtet der Einzelheiten der Vereinbarung** kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung **bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen**.

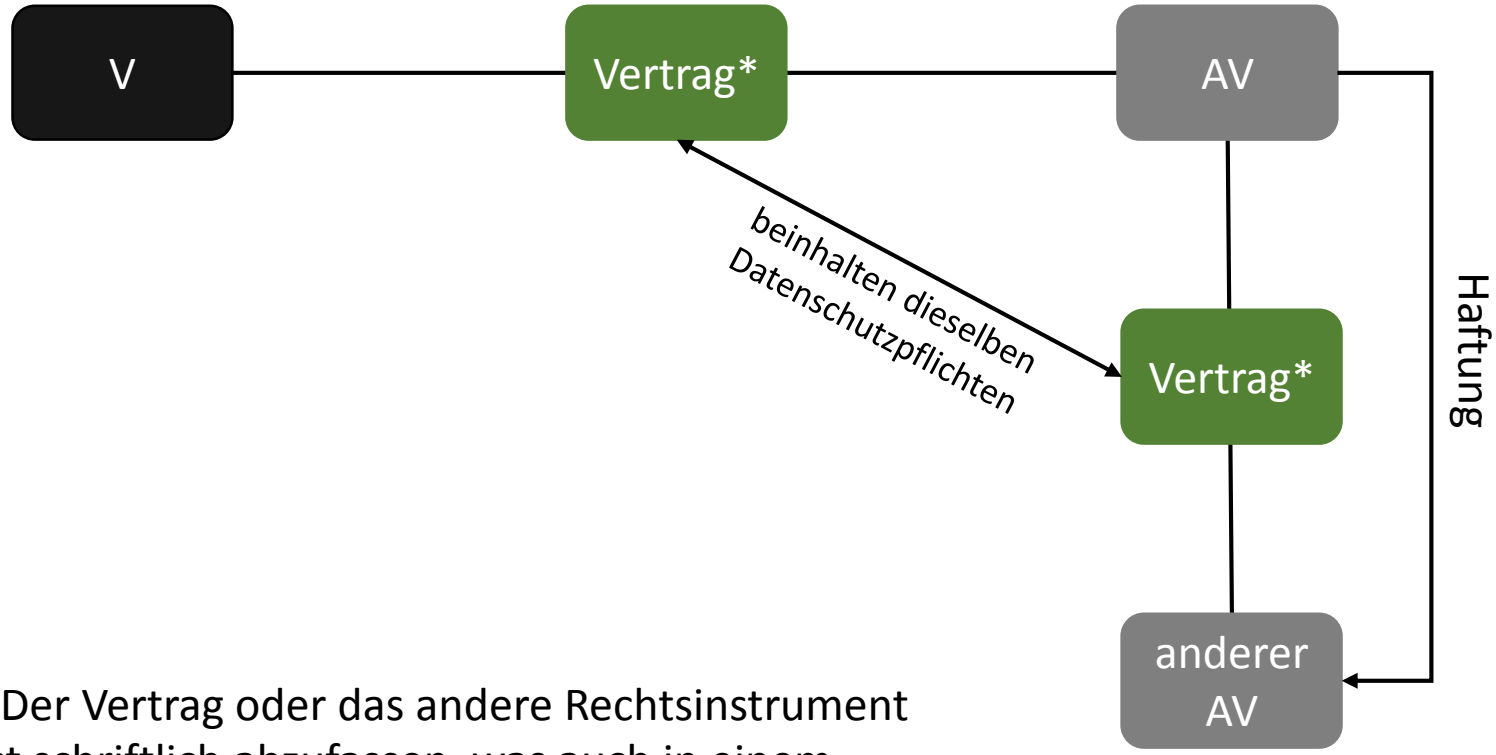
Auftragsverarbeiter

Ein anderer/weiterer AV soll in Anspruch genommen werden:



Auftragsverarbeiter

Ein anderer/weiterer AV soll in Anspruch genommen werden:



*Der Vertrag oder das andere Rechtsinstrument ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

Auftragsverarbeiter

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das

- den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und
- in dem Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen
- und die Pflichten und Rechte des Verantwortlichen

festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter:

Auftragsverarbeiter

- die pDaten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung pDaten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- alle gemäß Artikel 32 („Sicherheit der Verarbeitung) erforderlichen Maßnahmen ergreift
- die in den vorigen Folien genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält

Auftragsverarbeiter

- angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen
- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
- nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der **Auftragsverarbeiter** und jede dem Verantwortlichen oder dem Auftragsverarbeiter **unterstellte Person**, **die Zugang zu personenbezogenen Daten hat**, dürfen diese Daten **ausschließlich auf Weisung des Verantwortlichen verarbeiten**, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Verzeichnis von Verarbeitungstätigkeiten

Jeder **Verantwortliche** und ggf. sein Vertreter führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält **sämtliche folgenden Angaben**:

Verzeichnis von Verarbeitungstätigkeiten

- **den Namen und die Kontaktdaten**
  - des Verantwortlichen
  - ggf. 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**
- ggf. Übermittlungen von pDaten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie die Dokumentierung geeigneter Garantien zu den Datenübermittlungen (s. Art. 49 (1) Unterabsatz 2)
- 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

Jeder **Auftragsverarbeiter** und ggf. sein Vertreter führen ein **Verzeichnis** zu allen Kategorien von *im Auftrag eines Verantwortlichen* durchgeführten Tätigkeiten der Verarbeitung, die **Folgendes** enthält:

Verzeichnis von Verarbeitungstätigkeiten

- **den Namen und die Kontaktdaten**
  - des Auftragsverarbeiters oder der Auftragsverarbeiter
  - jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist
  - ggf. des Vertreters des Verantwortlichen oder des Auftragsverarbeiters
  - sowie eines etwaigen Datenschutzbeauftragten
- die **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden
- ggf. Übermittlungen von pDaten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie die Dokumentierung geeigneter Garantien zu den Datenübermittlungen (s. Art. 49 (1) Unterabsatz 2)
- 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

- das Verzeichnis ist **schriftlich** zu führen, was auch in einem **elektronischen** Format erfolgen kann
- das Verzeichnis wird **auf Anfrage der Aufsichtsbehörde dieser zur Verfügung gestellt**
- die genannten Pflichten aus dem Verzeichnis gelten **nicht** für Unternehmen oder Einrichtungen, die **weniger als 250 Mitarbeiter** beschäftigen, es sei denn
  - die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen
  - die Verarbeitung erfolgt nicht nur gelegentlich
  - es erfolgt eine Verarbeitung besonderer Datenkategorien bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Sicherheit personenbezogener Daten

Sicherheit der Verarbeitung

Der Verantwortliche und der Auftragsverarbeiter treffen **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes **Schutzniveau** zu gewährleisten, diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

Sicherheit der Verarbeitung

- 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

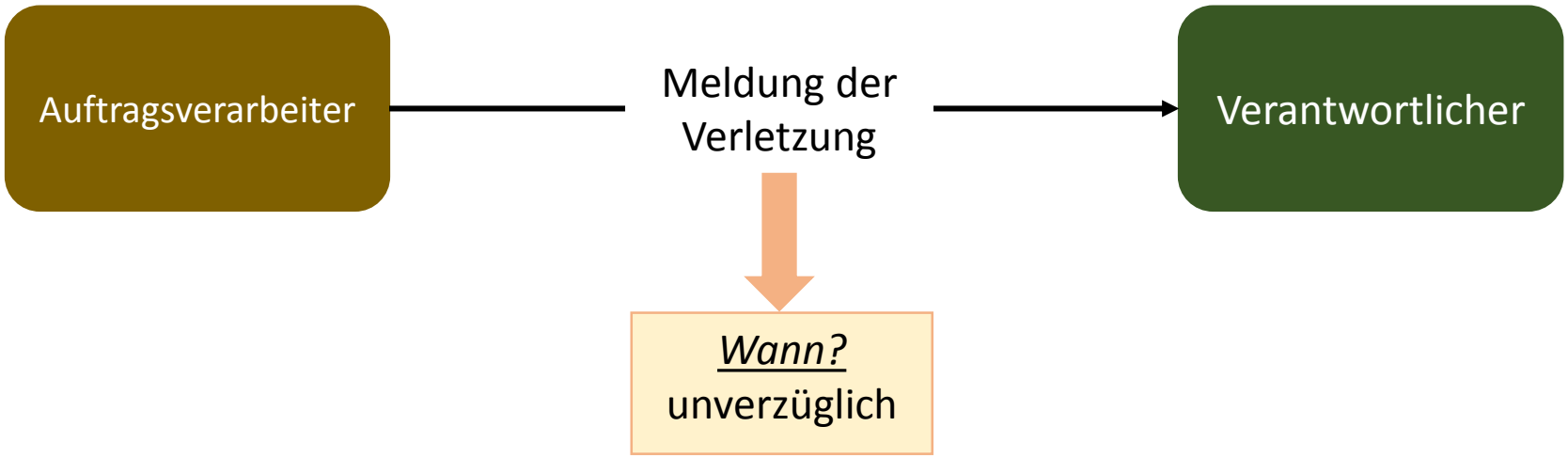
Sicherheit der Verarbeitung

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.

Sicherheit der Verarbeitung

Die Einhaltung genehmigter **Verhaltensregeln** gemäß Artikel 40 oder eines genehmigten **Zertifizierungsverfahrens** gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der genannten Anforderungen nachzuweisen.

Meldung von Verletzungen des Schutzes pDaten an die Aufsichtsbehörde



Meldung von Verletzungen des Schutzes pDaten an die Aufsichtsbehörde

Wann? unverzüglich/binnen 72 Stunden; wenn nicht innerhalb 72 Stunden, dann Begründung für Verzögerung

Wann keine Meldung? Wenn der Verantwortliche nachweisen kann, dass die Verletzung des Schutzes pDaten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Wie? Wenn die Informationen nicht zur gleichen Zeit bereitgestellt werden können, ist schrittweise Bereitstellung dieser erlaubt.

Meldung von Verletzungen des Schutzes pDaten an die Aufsichtsbehörde

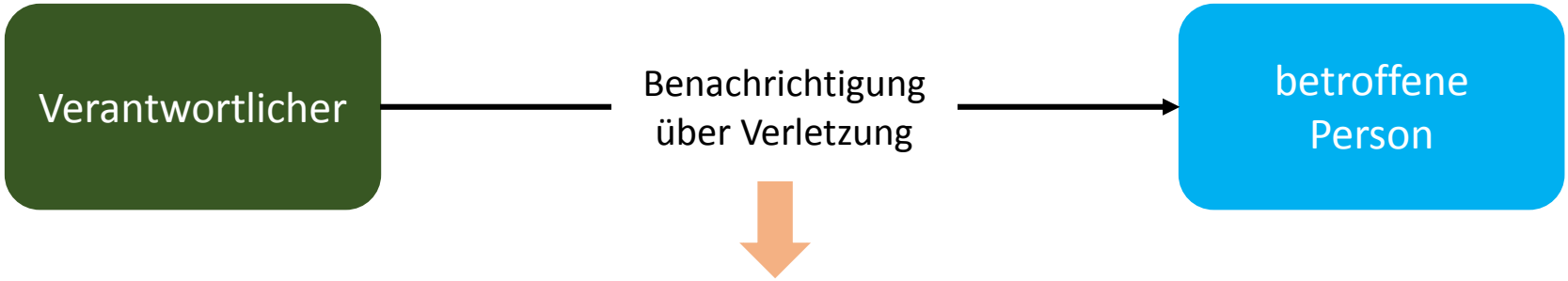
Die Meldung enthält mindestens folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Meldung von Verletzungen des Schutzes pDaten an die Aufsichtsbehörde

Der Verantwortliche dokumentiert Verletzungen des Schutzes pDaten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes pDaten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person



Voraussetzung für die Benachrichtigung: hohes Risiko für die persönlichen Rechte und Freiheiten der Person

Was beinhaltet die Benachrichtigung?

- Art der Verletzung des Schutzes pDaten in einer klaren und einfachen Sprache
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Benachrichtigung ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

1. der Verantwortliche **geeignete technische und organisatorische Sicherheitsvorkehrungen** getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen pDaten angewandt wurden
2. der Verantwortliche durch **nachfolgende Maßnahmen** sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß aller Wahrscheinlichkeit nach **nicht mehr besteht**
3. dies mit einem **unverhältnismäßigen Aufwand** verbunden wäre. In diesem Fall hat stattdessen eine **öffentliche Bekanntmachung** oder eine **ähnliche Maßnahme** zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden

Datenschutz-Folgenabschätzung und vorherige Konsultation

Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung 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.

insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung

Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende 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

b) umfangreiche Verarbeitung **besonderer Kategorien** von pDaten oder von pDaten über **strafrechtliche Verurteilungen und Straftaten**

c) systematische umfangreiche Überwachung **öffentlich zugänglicher Bereiche**

Datenschutz-Folgenabschätzung

Rolle der Aufsichtsbehörde:

- Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese.
- Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die **keine** Datenschutz-Folgenabschätzung erforderlich ist.
- Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

Datenschutz-Folgenabschätzung

Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird

Vorherige Konsultation

Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Vorherige Konsultation

Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation folgende Informationen zur Verfügung:

a) gegebenenfalls Angaben zu den jeweiligen **Zuständigkeiten** des Verantwortlichen, der **gemeinsam Verantwortlichen** und der an der Verarbeitung beteiligten **Auftragsverarbeiter**, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen

b) die **Zwecke und die Mittel** der beabsichtigten Verarbeitung

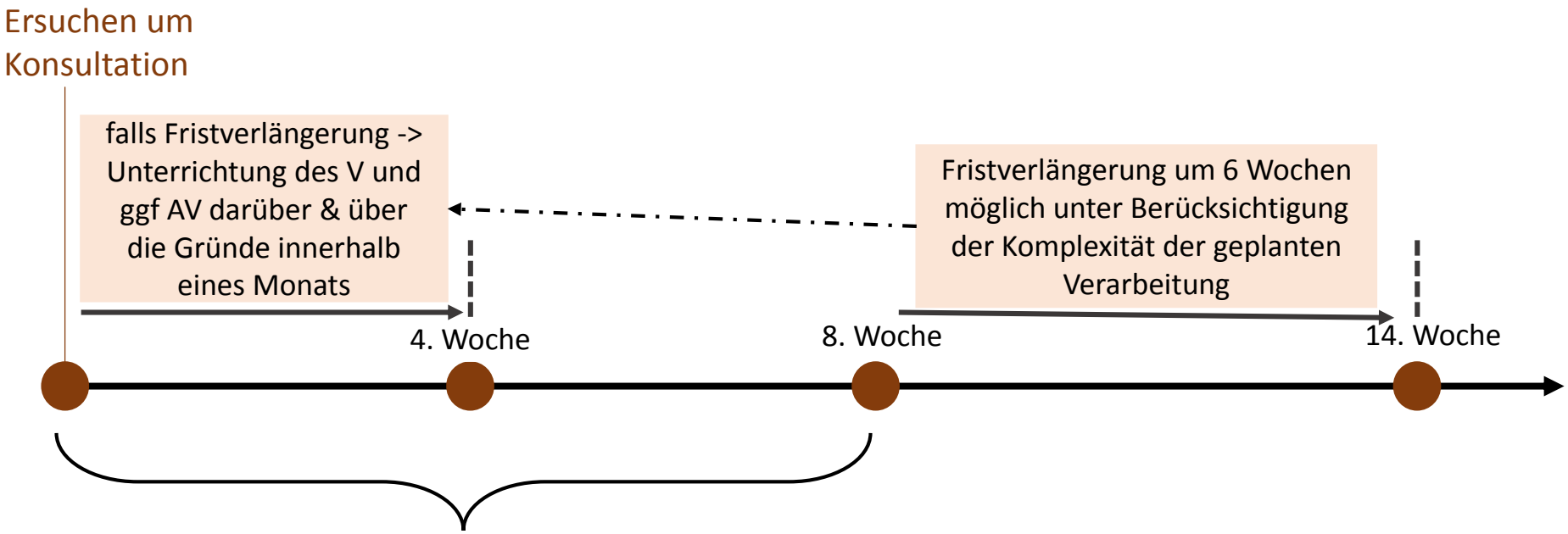
c) die zum **Schutz der Rechte und Freiheiten** der betroffenen Personen gemäß dieser Verordnung vorgesehenen **Maßnahmen und Garantien**

d) gegebenenfalls die **Kontaktdaten des Datenschutzbeauftragten**

e) die **Datenschutz-Folgenabschätzung**

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen

Vorherige Konsultation



innerhalb von 8 Wochen gibt die Aufsichtsbehörde eine schriftliche Empfehlung an V oder AV + kann ihre Befugnisse gemäß Art. 58 ausüben

Datenschutzbeauftragter

Benennung eines Datenschutzbeauftragten

Der Verantwortliche (V) und der Auftragsverarbeiter (AV) benennen auf jeden Fall einen Datenschutzbeauftragten, wenn:

a) die Verarbeitung von einer **Behörde** oder **öffentlichen Stelle** durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,

b) die Kerntätigkeit in der Durchführung von **Verarbeitungsvorgängen** besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen

c) die Kerntätigkeit in der umfangreichen Verarbeitung **besonderer Kategorien** von Daten oder von personenbezogenen Daten über **strafrechtliche Verurteilungen und Straftaten** besteht.

Benennung eines Datenschutzbeauftragten

-> in anderen Fällen gilt das Recht der Union oder der Mitgliedsstaaten;

<u>das BDSG schreibt vor:</u>

- es muss ein Datenschutzbeauftragter benannt werden, soweit der V oder AV in der Regel **mindestens zehn Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen
- nehmen der V oder der AV Verarbeitungen vor, die einer **Datenschutz-Folgenabschätzung** unterliegen oder verarbeiten sie pDaten **geschäftsmäßig zum Zweck der Übermittlung**, der **anonymisierten Übermittlung** oder für **Zwecke der Markt- oder Meinungsforschung**, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen

Benennung eines Datenschutzbeauftragten

nach BDSG:

Pflicht der Benennung des Datenschutzbeauftragten

abhängig von der Anz. der Beschäftigten, die sich mit der automatisierten Verarbeitung pDaten beschäftigen

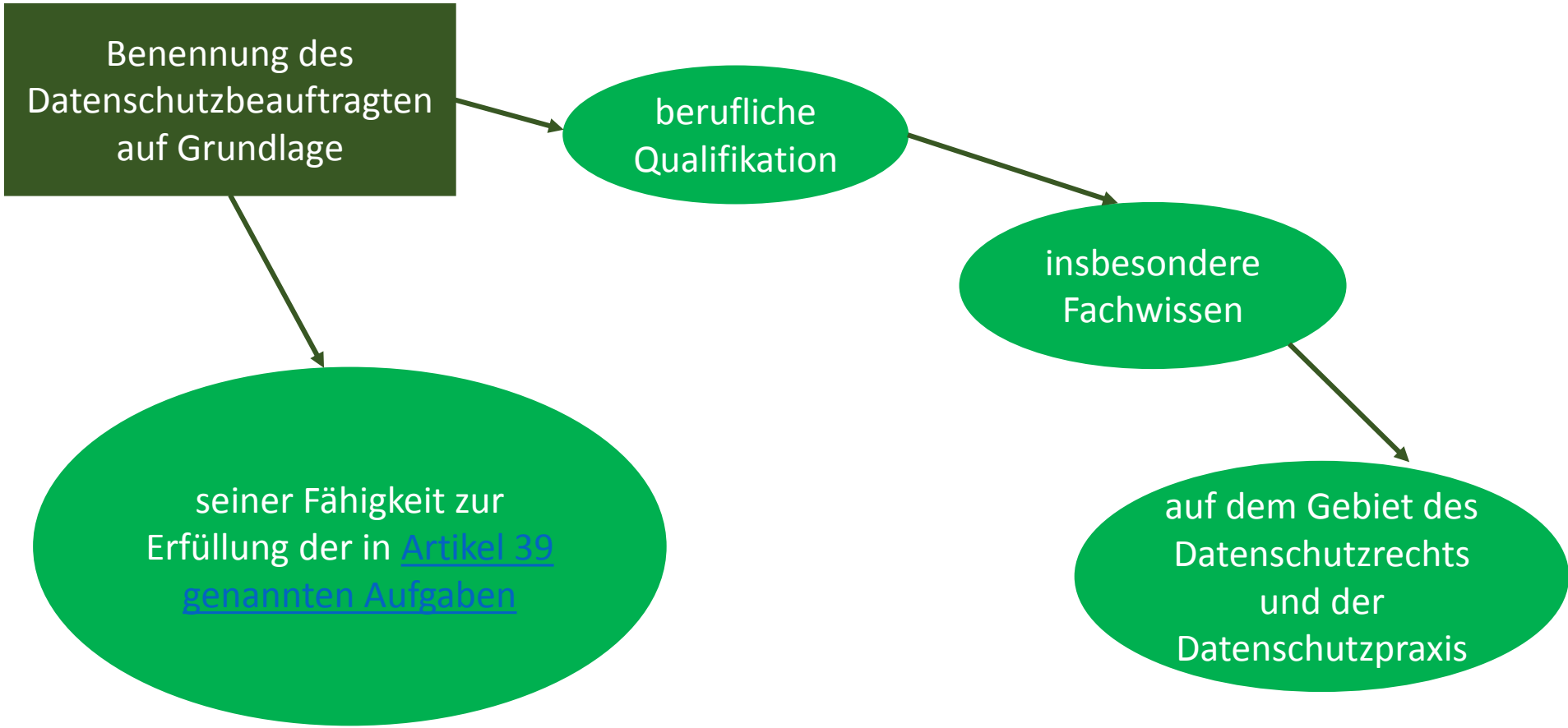
- i.d.R. 10 Personen ständig beschäftigt

unabhängig von der Anzahl der Beschäftigten

V oder AV

- unterliegen einer Datenschutz-Folgeabschätzung
- verarbeiten pDaten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung

Benennung eines Datenschutzbeauftragten



Benennung eines Datenschutzbeauftragten

- Der Datenschutzbeauftragte kann **Beschäftigter** des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines **Dienstleistungsvertrags** erfüllen.

- Der Verantwortliche oder der Auftragsverarbeiter **veröffentlicht die Kontaktdaten** des Datenschutzbeauftragten und **teilt diese Daten der Aufsichtsbehörde mit**.

Stellung des Datenschutzbeauftragten

- Der V und der AV stellen sicher, dass der Datenschutzbeauftragte **ordnungsgemäß und frühzeitig** in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
- Der V und der AV **unterstützen** den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben, indem sie die für die Erfüllung dieser Aufgaben erforderlichen **Ressourcen und den Zugang zu pDaten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen** zur Verfügung stellen.
- Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben **keine Anweisungen** bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter **wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt** werden.

Stellung des Datenschutzbeauftragten

- Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen **zu Rate** ziehen.
- Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die **Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden**.
- Der Datenschutzbeauftragte kann **andere Aufgaben und Pflichten wahrnehmen**. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten **nicht zu einem Interessenkonflikt** führen.

Stellung des Datenschutzbeauftragten

weiterhin laut BDSG:

- Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.
- Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. [2]Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. [3]Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

- **Unterrichtung und Beratung** des **V** oder des **AV** und der **Beschäftigten**, die Verarbeitungen durchführen, hinsichtlich ihrer **Pflichten nach dieser Verordnung** sowie nach **sonstigen Datenschutzvorschriften** der Union bzw. der Mitgliedstaaten

- **Überwachung der Einhaltung**
  - **dieser Verordnung**,
  - **anderer Datenschutzvorschriften** der Union bzw. der Mitgliedstaaten
  - sowie der **Strategien des V oder des AV für den Schutz pDaten**
  - einschließlich **der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen**

- **Beratung – auf Anfrage** – im Zusammenhang mit der **Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung** gemäß Artikel 35

(s. entsprechende Folien)

- **Zusammenarbeit mit der Aufsichtsbehörde**

- Tätigkeit als **Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der **vorherigen Konsultation** gemäß Artikel 36, und gegebenenfalls **Beratung zu allen sonstigen Fragen**

Verhaltensregeln und Zertifizierung

Verhaltensregeln

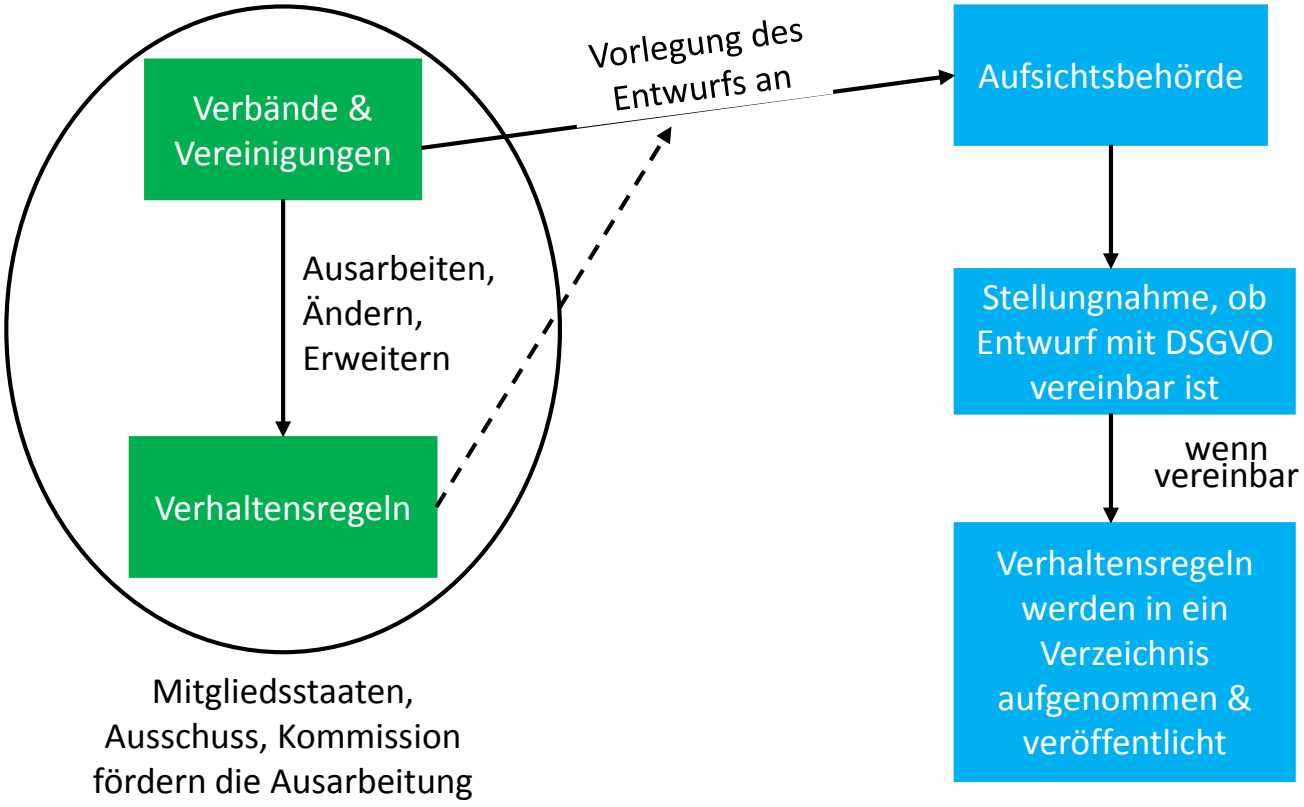
Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern **vertreten**, **können Verhaltensregeln ausarbeiten** oder **ändern** oder **erweitern**, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:

Verhaltensregeln

- faire und transparente Verarbeitung;
- die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;
- Erhebung personenbezogener Daten;
- Pseudonymisierung personenbezogener Daten;
- Unterrichtung der Öffentlichkeit und der betroffenen Personen;
- Ausübung der Rechte betroffener Personen;
- Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
- die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;
- die Meldung von Verletzungen des Schutzes pDaten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes pDaten;
- die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder
- außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln 77 und 79

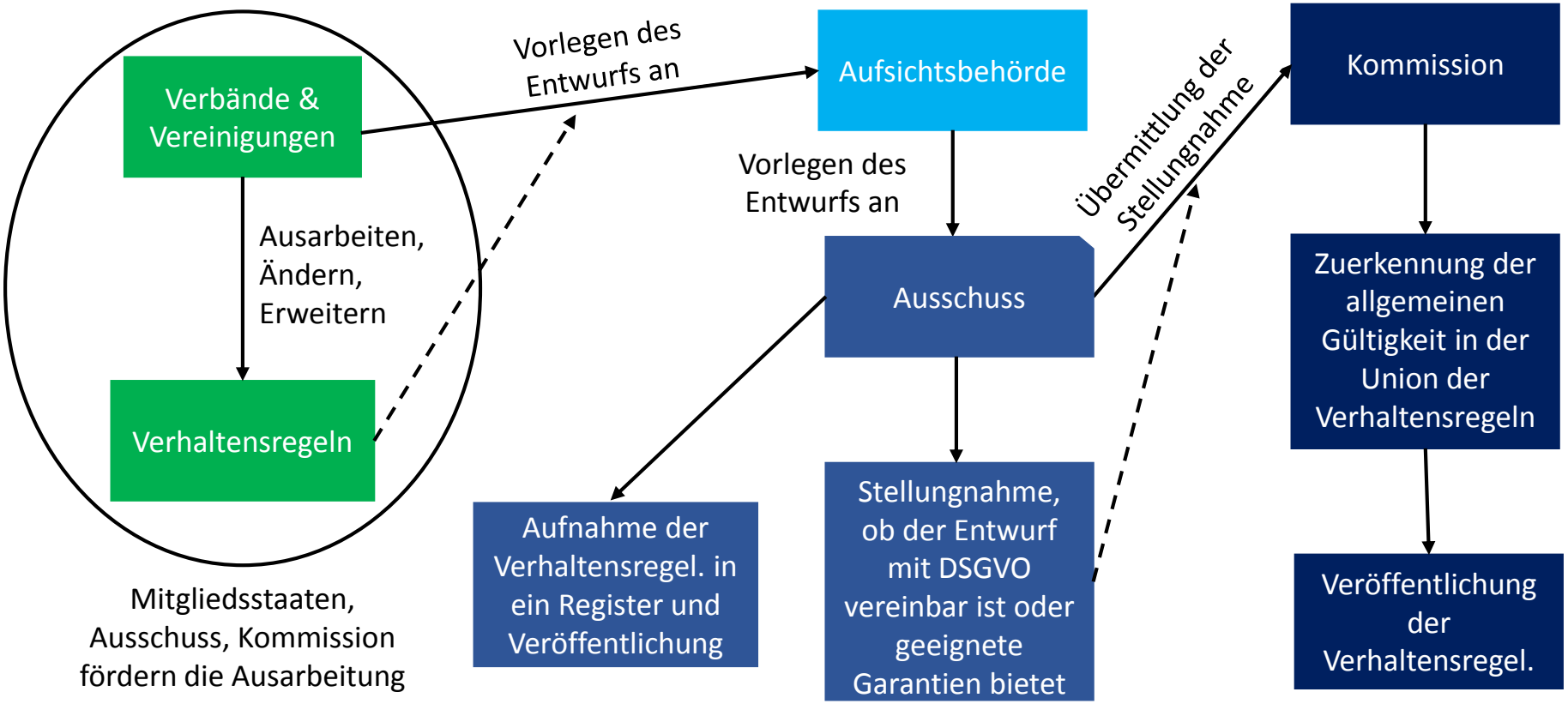
Verhaltensregeln

Verhaltensregeln sollen nur in einem Mitgliedsstaat gelten:



Verhaltensregeln

Verhaltensregeln sollen in mehreren Mitgliedsstaaten gelten:



Überwachung der genehmigten Verhaltensregeln

- Durchführung der Überwachung durch eine Stelle, die über das **geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln** verfügt und die von der **zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert** wurde
- [… https://dsgvo-gesetz.de/art-41-dsgvo/]

Zertifizierung

Grundlegendes: datenschutzspezifischen Zertifizierungsverfahren, Datenschutzsiegel und Datenschutzprüfzeichen werden von Mitgliedstaaten, Aufsichtsbehörden, dem Ausschuss und der Kommission gefördert

Ziel: Nachweis, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird

Bedingung: Zertifizierung muss freiwillig und über transparentes Verfahren zugänglich sein; der V oder AV stellt alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt der Zertifizierungsstelle oder der Aufsichtsbehörde den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten

Wer erteilt die Zertifizierung? Zertifizierungsstellen und zuständige Aufsichtsbehörden

Dauer: Zertifizierung max. für 3 Jahre; Verlängerung möglich, sofern die einschlägigen Kriterien weiterhin erfüllt werden

Widerruf der Zertifizierung: wenn die Kriterien für die Zertifizierung nicht oder nicht mehr erfüllt werden

Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Zertifizierungsstellen

Die Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, erteilen oder verlängern, nach Unterrichtung der Aufsichtsbehörde, die Zertifizierung.

[näheres siehe: https://dsgvo-gesetz.de/art-43-dsgvo/]