Standard-Datenschutzmodell:

Kernpunkte, Geschichte, Prüfungen – Schwerpunkt DS-GVO

Dipl.-Inform. Julia Stoll
Referatsleiterin Informatik
Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Telefon 0611 / 14 08 - 150
E-Mail: j.stoll@datenschutz.hessen.de

Übersicht

- Anwendung: Standard-Datenschutzmodell
  - Situation mit der DS-GVO
  - Datenschutzberatung und -prüfung
  - Voraussetzung und Abgrenzung
- Gewährleistungsziele
- Modellierung eines Verfahrens
  - Ermittlung des Schutzbedarfs

Übersicht (Fortsetzung)

- Gewährleistungsziele in der DS-GVO
  - Beispiele für Artikel 5, 25 und 32 DS-GVO
  - Generische Maßnahmen
  - Tabelle zu Gewährleistungen
- Maßnahmenkatalog
  - Basis von Bausteinen
  - Beispiele von Bausteinen
- Mögliches Zusammenspiel

Aktuelle Situation

ANWENDUNG – STANDARD-DATENSCHUTZMODELL

Situation mit der DS-GVO?

Einbettung in der DS-GVO – **Abwägung der Risiken**:
hohes Risiko für die Rechte und Freiheiten natürlicher Personen
Risiko und Haftung,
Risiko und Einwilligung,
Risiko und Auskunfts- und Informationspflichten

Tradition der Technik-Folgenabschätzung: **soziale und gesellschaftliche Bedeutung** [aus der Sicht der Anwendung von Technik]

...ung der GVO mit Blick auf technischen und o... nisatorischen ...ahmen

Sprachliche Barrieren

Grenzen der Anwendbarkeit wg. unterschiedlicher Tiefe bzgl. **organisatorischer Maßnahmen** (oft mit Bezug auf **„vertretbare" Kosten**) und Stand der Technik (wenig konkret)

Fehlende Kontexte aus der Nutzung in der Gesellschaft und/oder Folgen durch Gestaltung mit Technik

Standard-Datenschutzmodell:
Datenschutzberatung und -prüfung (Teaser)

Mit dem Standard-Datenschutzmodell (SDM) werden Datenschutzberatung und -prüfung unterstützt.

Im Artikel 5 der Datenschutz-Grundverordnung (DS-GVO) sind wesentliche Grundsätze für die Verarbeitung personenbezogener Daten formuliert.

Auf der Basis von Gewährleistungszielen, wie Dateiminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit, finden sich im SDM geeignete Maßnahmen, um diese rechtlichen Anforderungen in technische und organisatorische Maßnahmen zu überführen.

Quelle:
https://www.datenschutz.hessen.de/ft015.htm#entry4807

Standard-Datenschutzmodell: Voraussetzung und Abgrenzung

- Voraussetzung in allen deutschen Datenschutzgesetzen und DS-GVO
- Prüfung *bevor* das SDM angewendet wird
  - Rechtmäßigkeit für die Verarbeitung von personenbezogenen Daten
  - Erforderlichkeit der Verarbeitung
- „Anleitung“ durch das SDM: Wie wird‘s gemacht?

Elemente des Standard-Datenschutzmodells

Standard-Datenschutzmodell besteht aus

- Handbuch
- Maßnahmenkatalog

- Verbindungsglied für die Praxis:

  Kap. 7: Die generischen Maßnahmen zur Umsetzung der Gewährleistungsziele

Grundlage

GEWÄHRLEISTUNGSZIELE

7 Gewährleistungsziele

- Grundlegendes Gewährleistungsziel: Datenminimierung (früher: Datensparsamkeit oder sogar Datenvermeidung)
- Elementare Gewährleistungsziele:
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
- Datenschutz-Gewährleistungsziele:
  - Nichtverkettung (nah an Zweckgebundenheit, aber nicht gleich)
  - Transparenz
  - Intervenierbarkeit

Grundlegendes Gewährleistungsziel: Datenminimierung (proaktives Element)

Datenminimierung konkretisiert und operationalisiert im Grundsatz der Erforderlichkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist.

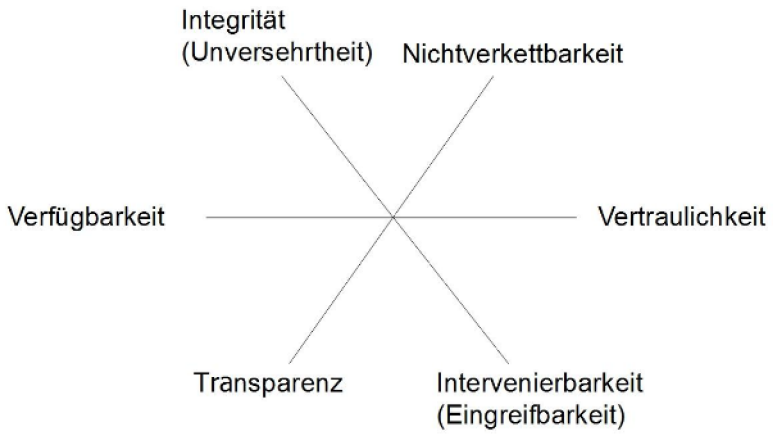
(siehe § 3a BDSG)

Dimensionen der Datenminimierung

Wenn eine vollständige Datenvermeidung nicht möglich ist, so [...] Verarbeitungsschritte bewertet werden:

- nach dem Umfang der verarbeiteten oder offengelegten Informationen,
- nach der Zahl der Stellen und Personen, welchen diese Informationen offenbart werden und
- nach dem Ausmaß der Verfügungsgewalt, den die jeweiligen Stellen und Personen über die Daten erlangen.

Im Abwägungsprozess



Elementare Gewährleistungsziele (auch im IT-Grundschutzkatalog des BSI)

Vertraulichkeit

Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Verfügbarkeit

Den Nutzenden stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Integrität

Die Daten sind vollständig und unverändert.

Datenschutz-Gewährleistungsziel: Transparenz

Transparenz (im allgemeinen Sinn (!))

Den Nutzenden sind die Verfahren bzw. Verwaltungsprozesse [bzgl. der Unternehmens-/Organisationsstruktur und ihre technische Umsetzung; J.S.] offenzulegen, so dass er oder sie in einer zumutbaren Zeit diese nachvollziehen, prüfen und bewerten kann, wie die eigenen personenbezogenen Daten erhoben und verarbeitet werden.

Kommentar

Dieses Gewährleistungsziel geht über die mehrheitlich aus technischer Perspektive beschriebene Prüfbarkeit aktiv genutzter Datenbestände und Dienste hinaus, wie sie bisher im Gewährleistungsziel Verfügbarkeit hinterlegt ist.

Weitere Gewährleistungsziele: Nichtverkettung und Intervenierbarkeit

Nichtverkettung

Die Nutzenden sollen sicher gehen können, dass Verfahren nur zweckgebunden eingesetzt werden und eine klare Zwecktrennung zwischen verwandten Verfahren besteht.

Intervenierbarkeit

Nutzenden sind ein Zugriff auf die Verfahren und Daten bzgl. der eigenen personenbezogenen Daten zu ermöglichen.

Abgeleitete Gewährleistungsziele

Authentizität und Revisionsfähigkeit

Das Gewährleistungsziel der **Authentizität** beschreibt die Anforderung, das personenbezogene Daten ihren Ursprung gesichert zugeordnet werden können;

d.h. um z.B. das Gewährleitungsziel der Transparenz oder der Intervenierbakeit zu unterstützen.

Das Gewährleistungsziel der **Revisionsfähigkeit** beschreibt die Anforderung, dass festgestellt werden kann, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat.

Das Ziel dient der Wahrung der Integrität zwischen der Verknüpfung zwischen Datenbestand und Verarbeitungsnachweis.

Schritte

MODELLIERUNG EINES VERFAHRENS

Modellierung eines Verfahrens: Verfahrenskomponenten

Bei der Modellierung eines Verfahrens [...] sind [...] **drei Komponenten** zu unterscheiden [...]:

- personenbezogenen Daten,
- [...] Systeme (Hardware, Software und Infrastruktur) sowie
- die organisatorischen und personellen Prozesse der Verarbeitung von Daten mit den Systemen.

Modellierung eines Verfahrens: Ermittlung des Schutzbedarfs

- Personenbezogene Daten im Vordergrund
- Ermittlung bzw. Feststellung des Schutzbedarfs durch die verantwortliche Stelle [und/oder den Auftragsverarbeiter; J.S.]
- „“Vererbung“ des ermittelten Schutzbedarfs an Systeme und Prozesse
- Überprüfung des ermittelten Schutzbedarfs anhand des Maßnahmenkatalogs

Modellierung eines Verfahrens: Kernkomponenten

Kernkomponenten sind

- die Eigenschaften von Datenformaten,
- die Betrachtung der (System-)Schnittstellen sowie
- die Klärung der Verantwortlichkeiten für jeden Prozess

Kernkomponente: Eigenschaften der Datenformate

- Speziell die **Eigenschaften der Datenformate** bei der Erhebung beachten
- **Qualität der Daten**
  - frühere Daten, die vermeintlich gelöscht sind
  - Metadaten
  - Ort und Zeit der Graphikdaten
  - verlustbehaftete Daten
- Direkter Einfluss auf die Qualität der Umsetzung der Gewährleistungsziele

Kernkomponente: Schnittstellen

Ziel ist die **Beherrschbarkeit von Datenflüssen**. Dabei sind

- die Systemgrenzen beachten,
- die Schnittstellen zwischen Systemen, die nicht innerhalb der vom Zweck definierten Systemgrenzen zu vermeiden,
- die Existenz von Schnittstellen auszuweisen und
- die Schnittstellen zu dokumentieren

Kernkomponente: Verantwortlichkeiten

- Für jeden Prozess sind Verantwortlichkeiten zu klären, die typischer Weise in Berechtigungen bzw. ein Rollen- und Rechte-Konzept führen (Festlegung *und* Zuweisung)
- Gliederung in
  - organisatorische Maßnahmen (Festlegung)
  - technische Maßnahmen (Zuweisung, ggf. in automatisierten Prozessen)

  ist erforderlich.
- Für Prozess- und Verfahrensverantwortlichkeiten ist zu berücksichtigen,
  - dass Verfahrenskomponenten als des Teile eines organisatorischen Verfahrens oder
  - als eigenständige Teilprozesse eingestuften werden.

Ermittlung des Schutzbedarfs: Perspektiven

- Schutzbedarfsabstufungen zur Bewertung eines Risikos
  - bisher: IT-Grundschutzkataloge des Bundesamts für Informationstechnik (BSI)
  - begrenzte Übertragbarkeit der Informationssicherheit
- [deutlichere] Sichtweise auf Datenschutzaspekte und damit Grundrechtsschutz
  - Datenverarbeitung bedeutet – auch wenn sie datenschutzkonform ist – einen Eingriff in die Grundrechte der Betroffenen darstellt (Art. 7 und 8 der EU-Grundrechtecharta (EUCh)

Schutzbedarf im Standard-Datenschutzmodell

Normal: Es werden personenbezogene Daten verarbeitet, ohne dass Verarbeitungsszenarien mit potentiell erhöhter Eingriffsintensität gegeben sind.

Hoch:

- Es werden personenbezogene Daten verarbeitet, die der Kategorie „besonderer Arten personenbezogener Daten“ zu zuordnen sind und als solche einen hohen Schutzbedarf aufweisen.
- Hoher Schutzbedarf besteht darüber hinaus, wenn Betroffene von Entscheidungen bzw. Leistungen einer Organisation abhängig sind.
- Ein hoher Schutzbedarf besteht auch dann, wenn es nicht möglich ist, dass Konflikte unter realistisch zu bewältigenden Bedingungen für Betroffene vor Gericht geklärt werden können.

Schutzbedarf
im Standard-Datenschutzmodell

Sehr hoch: Von sehr hohem Schutzbedarf ist auszugehen, wenn eine betroffene Person von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existentiell abhängig ist und zusätzliche Risiken für den/die Betroffene/n nicht bemerkbar sind.

- Schutzbedarfsfeststellungen unter Datenschutzaspekten können anders ausfallen, als unter Anwendung der IT-Grundschutzkataloge des BSI
- Beispiel:
  Protokollierung von Zugriffen der Mitarbeiter/innen

Umsetzung von Gewährleistungszielen

- Generische Maßnahmen (im SDM-Handbuch)
- Maßnahmenkatalog (weiteres Dokument)
  - auf der Basis von Bausteinen
  - Möglichkeit zur Beteiligung

Identifikation

GEWÄHRLEISTUNGSZIELE IN DER DS-GVO: ARTIKEL 5, 25 UND 32

Datenminimierung

Art. 5 Abs. 1 lit. c, Art. 5 Abs. 1 lit. e, Art. 25, Art. 32

Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

c) Dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**„Datenminimierung“**)

d) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur solange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und der Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder statistische Zwecke gemäß Art. 89 Abs. 1 verarbeitet werden (**„Speicherbegrenzung“**)

Erwägungsgründe: 28, 29, 30, 39, 78, 156

Datenminimierung

Art. 25: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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 der 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 – trifft, **die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen** und die notwendigen Garantien in der Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Datenminimierung

Art. 25: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für die deren 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 Anzahl von natürlichen Personen zugänglich gemacht werden**.

Datenminimierung
Art.32 Sicherheit der Verarbeitung

4) Der **Verantwortliche** und der **Auftragsverarbeiter unternehmen Schritte, um sicherzustellen**, dass **ihnen unterstellte natürliche Personen**, die Zugang zu personenbezogenen Daten haben, **diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedsstaaten verpflichtet.**

Verfügbarkeit
Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für die deren 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 Anzahl von natürlichen Personen zugänglich gemacht werden.

Erwägungsgründe: 49, 78, 83

Verfügbarkeit

Art. 32 Sicherheit der Verarbeitung

Absatz 1 lit. b)

die Fähigkeit, die Vertraulichkeit, Integrität, **Verfügbarkeit** und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

lit. c)

die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

Integrität

Art. 32 Sicherheit der Verarbeitung

Absatz 1 lit. b)

die Fähigkeit, die Vertraulichkeit, **Integrität**, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Erwägungsgründe: 39, 49, 78, 83

Integrität

Art. 32 Sicherheit der Verarbeitung

2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, **die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung** von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Integrität

Art. 32 Sicherheit der Verarbeitung

4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, **dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten,** es sei denn, sie sind nach dem Recht der Union oder der Mitgliedsstaaten verpflichtet.

Vertraulichkeit

Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für die deren 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 Anzahl von natürlichen Personen zugänglich gemacht werden.

Erwägungsgründe: 49, 78, 83

Vertraulichkeit

Art. 32 Sicherheit der Verarbeitung

Absatz 1 lit. b)

die Fähigkeit, die **Vertraulichkeit**, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Erwägungsgründe: 39, 49, 78, 83

Nichtverkettung

Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellungen grundsätzlich nur personenbezogene Daten, **deren Verarbeitung für die deren 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 Anzahl von natürlichen Personen zugänglich gemacht werden.

Erwägungsgründe: 31, 32, 33, 39, 50, 53, 71, 78

Transparenz und Intervenierbarkeit

Art. 32 Sicherheit in Verarbeitung

2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Erwägungsgründe - Transparenz: 32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100

Erwägungsgründe – Intervenierbarkeit: 39, 59, 65, 66, 67, 68, 69, 70, 79

Auswahl

GENERISCHE MAßNAHMEN

Generische Maßnahmen:
Datenminimierung

- Reduzierung von erfassten Attributen der betroffenen Personen,
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten,
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen,
- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren,
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren

Generische Maßnahmen:
Verfügbarkeit

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u.ä. gemäß eines getesteten Konzepts,
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt),
- Dokumentation der Syntax der Daten,
- Redundanz von Hard-und Software sowie Infrastruktur,
- Umsetzung von Reperaturstrategien und Ausweichprozessen,
- Vertretungsregelunge für abwesende Mitarbeiter

Generische Maßnahmen:
Integrität

- Einschränkung von Schreib- und Änderungsrechten,
- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts,
- Dokumentierte Zuweisung von Berechtigungen und Rollen,
- Prozesse zur Aufrechterhaltung der Aktualität von Daten,
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Test zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen,
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen

Generische Maßnahmen: Vertraulichkeit

- Festlegung eines Rechte- und Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle,
- Implementierung eines sicheren Authentifizierungsverfahrens,
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen,
- Festlegung und Kontrolle zugelassener Ressourcen insbesondere Kommunikationskanäle,

Generische Maßnahmen: Vertraulichkeit (Fortsetzung)

- Spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume),
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptographischen Informationen (Krypokonzept),
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

Generische Maßnahmen: Nichtverkettung

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten,
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten,
- regelnde Maßnahmen zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Software-Entwicklung,
- Trennung nach Organisations-/ Abteilungsgrenzen,

Generische Maßnahmen: Nichtverkettung (Fortsetzung)

- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagement durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens,
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle,
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonyme Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten,
- geregelte Zweckänderungsverfahren

Generische Maßnahmen: Transparenz

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren,
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen geänderten Verfahren,
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen,
- Dokumentation von Einwilligungen und Widersprüchen,

Generische Maßnahmen: Transparenz (Fortsetzung)

- Protokollierung von Zugriffen und Änderungen,
- Nachweis der Quellen von Daten (Authentizität),
- Versionierung,
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts,
- Berücksichtigung der Auskunftsrechte der Betroffenen im Protokollierungs- und Auswertungskonzept

Generische Maßnahmen: Intervenierbarkeit

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten,
- Schaffung notwendiger Datenfelder z.B. Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen,
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen von Verfahren sowie an Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes,
- Deaktivierungsmöglichkeiten einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem,

Generische Maßnahmen: Intervenierbarkeit (Fortsetzung)

- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltungmachung und/oder Durchsetzung von Ansprüchen,
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte,
- Errichtung eines Single-Point-of-Contact (SPoC) für Betroffene,
- operative Möglichkeit zur Zusammenstellung, konsistenten Benachrichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

Standard-Datenschutzmodell - Zusammenfassung

BEZÜGE ZUR DS-GVO

Gewährleistungsziele in der DS-GVO (tabellarische Darstellung)

	Daten-minimierung	**Verfügbarkeit**	**Integrität**	**Vertraulichkeit**
Artikel	Art. 5. Abs. 1 lit. c und lit. e; Art. 25, Art. 32	Art. 5. Abs. lit. e, Art. 13, Art. 15, Art. 20, Art. 25, Art. 32	Art. 5 Abs. 1 lit. f , Art. 25, Art. 32, Art. 33	Art. 5 Abs. 1 lit. f, Art. 25, Art. 28 Abs. 3 lit. b, Art. 29, Art. 32
Erwägungs-gründe	28, 29, 30, 39, 78, 156	49, 78, 83	39, 49, 78, 83	39, 49, 78, 83

Gewährleistungsziele in der DS-GVO (tabellarische Darstellung)

	Nichtverkettung	Transparenz	Intervenierbarkeit
Artikel	Art. 5. Abs. 1 lit. c und lit. e; Art. 17, Art. 22, Art. 25, Art. 40 Abs. 2 lit. d	Art. 5. Abs. lit. a, Art. 13, Art. 14, Art. 15, Art. 19, Art. 25, Art. 30, Art. 32, Art. 33, Art. 40, Art. 42	Art. 5 Abs. 1 lit. d und lit. f , Art. 13 Abs. 2 lit. c, Art. 15 Abs. 1 lit. e, Art. 16, Art. 17, Art. 18, Art. 20, Art. 21, Art. 25, Art. 32
Erwägungs-gründe	31, 32, 33, 39, 50, 53, 71, 78	32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100	39, 59, 65, 66, 67, 68, 69, 70, 78

Referenzen

MAßNAHMENKATALOG

Maßnahmenkatalog (Entwurf)

- Anmerkung – vorweg : Integration des Baustein 1.5 aus dem IT-Grundschutzkatalog des BSI
- Langfristige Planung – möglichst Integration von mehreren Orientierungshilfen
- Fortschreibung von Bausteinen, um die Themen zu erweitern
- Basis von Bausteinen – Themenauswahl (alphabetische Reihenfolge)
  - Anonymisierung & Pseudonymisierung
  - Aspekte eines Datenschutzkonzeptes
  - Aufbewahrung
  - Auskunft
  - Beurteilbarkeit technisch organisatorischer Funktionen

Maßnahmenkatalog (Auswahl): Basis von Bausteinen

- Datensicherung und -wiederherstellung
- Berichtigung
- Datenschutz-Folgenabschätzung
- Datenschutz-Zuständigkeiten (Datenschutzbeauftragter)
- Dokumentation
- Löschen

Maßnahmenkatalog (Auswahl, Fortsetzung): Basis von Bausteinen

- Protokollierung
- Rollen und Berechtigungen
- Single Point of Contact (SPoC)
- Sperren
- Ticketsystem und Administations-Plattform
- Trennung

Baustein: Datensicherung und -wiederherstellung

Ebene Daten

M001	Ermittlung der erforderlichen Daten zur Wiederherstellung eines Verfahrens
M002	Festlegung der Arten der Datensicherung
M003	Erhebung und Dokumentation der Einflussfaktoren auf die Datensicherung

Ebene Systeme

M004	Datensicherungsplan je IT-System und Datenart (Art der Datensicherung, Häufigkeit und Zeitpunkt der Datensicherung, Medien und Aufbewahrungsorte, Rekonstruktionszeiten

Baustein:
Datensicherung und -wiederherstellung

Ebene Prozesse

M005	Randbedingungen (Vertragsgestaltungen, Refresh-Zyklen, Bestandsverzeichnis, Löschen von Daten, Vernichten von Datenträgern)
M006	Datensicherung bei Einsatz von kryptographischen Verfahren
M007	Verpflichtung der Mitarbeiter zur Datensicherung
M008	Restaurierungsübungen
M009	Prüfung von Löschungsmöglichkeiten einzelner Daten aus der Datensicherung

Baustein:
Berichtigung

Ebene Daten

M001	Datenmodell mit geeigneten Datenstrukturen
M002	Datenfelder zur Speicherung von Datenchronologien
M003	Datenfelder zur Speicherung von Zeitangaben oder Zeitstempeln
M004	Datenfelder zur Speicherung identifizierender Daten des Auskunftssuchenden

Baustein:
Berichtigung

Ebene Systeme

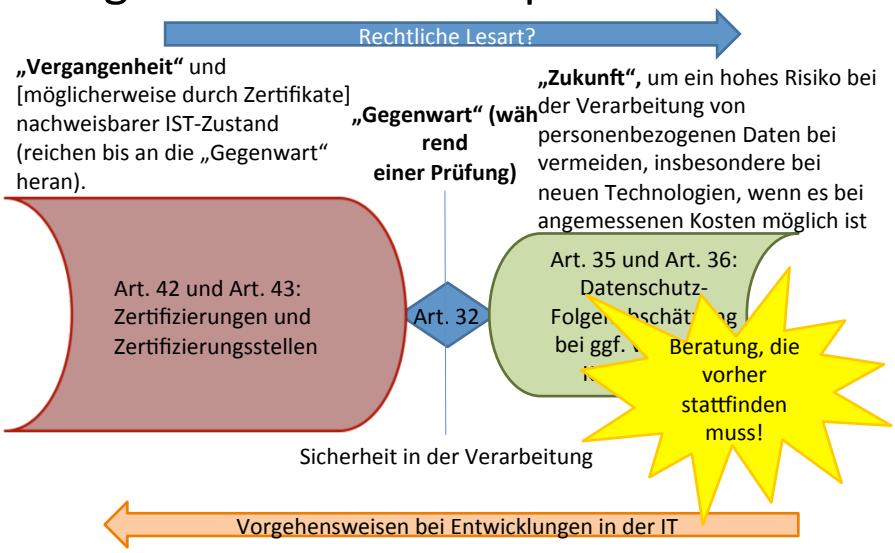
M005	Technische Systeme, die Benachrichtigungsvorgänge zulassen
M006	Trennung von Datenbeständen, um differenziert benachrichtigen zu können
M007	Technische Umsetzung des Rechte- und Rollenkonzepts
M008	System zur Fristenüberwachung
M009	Elektronische Zeitstempelsysteme
M010	Identifizierungssysteme, die Auskunftssuchende sicher identifiziereng können
M011	Identifizierung über die eID-Funktion des Personalausweises
M012	Verfahren zur Sperrung von Datenfeldern bei Zweifelsfällen
M013	Protokollierungssysteme

Baustein:
Berichtigung

Ebene Prozesse

M014	Berichtigungskonzept
M015	Rechte- und Rollenkonzept
M016	Prozess zur Dokumentation aller Datenübermittlungen
M017	Prozess zur Fristenüberwachung
M018	Prozess zu ordnungsgemäßen Ablehnung von Berechtigungsbegehren
M019	Prozess für turnusmäßige „Korrekturläufe“

Mögliches Zusammenspiel ?!



Referenzen (Auswahl)

Bundesamt für Sicherheit in der Informationstechnik -Schutzbedarfskategorien: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/Schutzbedarfskategorien/Definitionen/definitionen_node.html (letzter Aufruf: 06.05.2013)

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK): Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele (V.1.0 – Erprobungsfassung) 9. und 10. November 2016

Das Standard-Datenschutzmodell: Entwurf Maßnahmenkatalog (in private communication)

EU - Veröffentlichung der **EU-DSVGO im Web (dt. Fassung)**: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN

Forum Privatheit und selbstbestimmtes Leben in der digitalen Gesellschaft: Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz (White Paper) unter: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, veröffentlicht 17.03.2016 (letzter Aufruf: 21.03.2017)

M. Rost; K. Bock: Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen. In: DuD - Datenschutz und Datensicherheit. Nr. 1 (2011). S.30-35

Anhang

AUSWAHL VON ARTIKELN IN DER DS-GVO

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten in Bezug auf das Standard-Datenschutzmodell

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

c) Dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)

d) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur solange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und der Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder statistische Zwecke gemäß Art. 89 Abs. 1 verarbeitet werden („Speicherbegrenzung“)

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Personen gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Zwecke oder für wissenschaftliche und historische Forschungszwecke oder statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherabgrenzung“)

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)

Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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 der 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 – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen und die notwendigen Garantien in der Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für die deren 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 Anzahl von natürlichen Personen zugänglich gemacht werden.

Art. 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

3) Ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Art. 32 Sicherheit der Verarbeitung

Art. 32 Sicherheit der Verarbeitung

1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

Art. 32 Sicherheit der Verarbeitung

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Art. 32 Sicherheit in Verarbeitung

2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Art.32 Sicherheit der Verarbeitung

3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder der genehmigten Zertifizierungen gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Anforderungen nachzuweisen.
4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedsstaaten verpflichtet.

Art. 35 Datenschutz-Folgenabschätzung

Art. 35 Datenschutz-Folgenabschätzung

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. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.
2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde ein.

Art. 35 Datenschutz-Folgenabschätzung

3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:
   a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatische Verarbeitung einschließlich Profiling gründet ihrerseits ls Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
   b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
   c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Art. 35 Datenschutz-Folgenabschätzung

4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.
5) 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 dann dem Ausschuss.

Art. 35 Datenschutz-Folgenabschätzung

6) Vor der Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren und Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedsstaaten im Zusammenhang stehen oder die den freien Verkehr von personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

Art. 35 Datenschutz-Folgenabschätzung

7) Die Folgenabschätzung enthält zumindest Folgendes:
   a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von den 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 gemäß Absatz 1 und
   d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich der 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.

Art. 35 Datenschutz-Folgenabschätzung

8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgängen, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.
9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Person oder ihrer Vertreter zu der berechtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

Art. 35 Datenschutz-Folgenabschätzung

10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c und e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedsstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

Art. 35 Datenschutz-Folgenabschätzung

11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerben, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.