Checkliste DS-GVO

Eine Ausarbeitung der

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Version 1.0

Stand der Bearbeitung: 12.06.2017

Autoren (alphabetisch)

Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Hinweis: Die Checkliste kann in keinster Weise die notwendige Sachkunde ersetzen, die zur Umsetzung der Anforderungen der EU Datenschutz-Grundverordnung (DS-GVO) benötigt wird. Daher ist entsprechend geschultes Personal oder auch extern eingekaufte Beratungsleistung zur Umsetzung der Anforderungen der DS-GVO unabdingbar. Einen guten Überblick über die Anforderungen der DS-GVO bietet das Buch

> Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung, Verlag Fachmedien Recht und Wirtschaft, ISBN 978-3-8005-1623-0.

Die vorliegende Checkliste dient nur der Unterstützung der Anforderungsumsetzung durch einen entsprechend kompetenten Datenschutzbeauftragten.

1 Analyse des Soll-Zustandes

Aufarbeitung der neuen gesetzlichen Anforderungen, die das eigene Unternehmen betreffen

2 Analyse des Ist-Zustandes

2.1 Welche Daten werden verarbeitet?

- Welche personenbezogene Daten werden verarbeitet?
- Welche besonderen Kategorien personenbezogener Daten (Art. 9) werden verarbeitet?
- Werden Kindern Dienste der Informationsgesellschaft angeboten?

2.2 Wozu werden Daten verarbeitet?

- Was sind die Zwecke meiner Datenverarbeitungen?

2.2.1 Arbeitnehmerdaten

- Besonderheiten Arbeitnehmerdatenschutz
  - Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc.
  - Rechtzeitige Kommunikation mit dem Betriebsrat, insbesondere Prüfung bestehende Betriebsvereinbarungen auf Konformität zur DS-GVO

2.3 Wie werden Daten verarbeitet?

- Welche Datenanwendungen bestehen?
  - Welche Standardanwendungen liegen derzeit vor?
  - Welche Datenanwendungen sind derzeit im Verarbeitungsverzeichnis gelistet? Welche fehlen?
- Erfolgt Profiling?
- Besteht für meine Datenverarbeitungen Dokumentationspflicht?
  - Wie wird die Dokumentationspflicht erfüllt?

2.3.1 Findet eine Verarbeitung im Ausland statt?

- Welcher Datenverkehr mit dem EU-Ausland besteht und auf welcher Rechtsgrundlage?
- Werden die Anforderungen an die Transparenz (z. B. Art. 13 Absatz 1 Buchstabe f und Art. 14 Absatz 1 Buchstabe f) und Dokumentation (Art. 30) erfüllt?
- Im Falle einer Auftragsverarbeitung: Ist eine Datenverarbeitungsvereinbarung vorhanden?
- Verwenden Sie in Ihrem Unternehmen Binding Corporate Rules (BCR)?

Falls ja

- Besteht in Ihrem Unternehmen ein Meldeverfahren zur Unterrichtung der Aufsichtsbehörde über etwaige rechtliche Bestimmungen in Ihrem Land, welche die Garantien der BCR beeinträchtigen könnten (Art. 47 Abs. 2 lit. m)?
- Bietet Ihr Unternehmen geeignete Datenschutzschulungen für Beschäftigte mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten an (Art. 47 Abs. 2 lit. b)?
- Informiert Ihr Unternehmen die Aufsichtsbehörde und die betroffene Person über Struktur und Kontaktdaten des Konzerns und seiner Unternehmen (Art. 47 Abs. 2 lit. a)?
- Bestehen Verfahren für die Erfassung von Änderungen der BCR und Ihre Meldung an die Aufsichtsbehörde (Art. 47 Abs. 2 lit. k)?
- Werden die Maßnahmen und Verfahren, auf die in Art. 47 Absatz 2 Buchstabe l und j verwiesen wird, dokumentiert (Art. 47 Abs. 2 lit. l, j)?

2.3.2 Auftragsverarbeitung

- Werden Auftragsverarbeiter (derzeit „Dienstleister“) herangezogen?
- Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?
- Gibt es schriftliche Vereinbarungen für die Auftragsverarbeitung?
  - Sind alle Anforderungen aus Art. 28 DS-GVO an den Vertrag berücksichtigt?
- Werden Auftragsverarbeiter in die Verantwortung für den Schutz personenbezogener Daten einbezogen?

2.4 Rechtsgrundlage

- Was ist die Rechtsgrundlage der Datenverarbeitung?
  - Liegt eine Einwilligung vor?
- Überprüfen Sie Ihre AGBs, Datenschutzerklärungen, Impressum, laufende Verträge, Website-Einstellungen, usw.

2.5 Umgang mit Betroffenenrechten

- Wie werden die Informationspflichten (nach der DSGVO) erfüllt?
  - Kontaktdaten
  - Zwecke/Rechtsgrundlage der Verarbeitung
  - Wenn vorhanden: berechtigte Interessen der verarbeitenden Stelle
  - Empfänger der Daten
  - Übermittlung in Drittländer
  - Dauer der Speicherung
  - Betroffenenrechte
  - Hintergründe der Bereitstellung
  - Automatisierte Entscheidungsfindung
  - Zweckänderung
- Wie werden die Betroffenenrechte (nach der DSGVO) erfüllt?
  - An wen in meinem Unternehmen können sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden?
  - Darstellung der Umsetzung
    - Auskunft
    - Berichtigung
    - Datenübertragbarkeit

        - Löschung
        - Einschränkung der Verarbeitung
        - Widerspruch gegen Verarbeitung
        - Beschwerde bei Aufsichtsbehörden
        - Widerruf der Einwilligung
- Gibt es ein betriebsfähiges Konzept zur unternehmensweiten Löschung von Daten über alle Funktionsbereiche und IT-Systeme hinweg?
- Können personenbezogene Daten auf Anforderung des Betroffenen an Dritte in einem strukturierten, gängigen und maschinenlesbaren Format weitergegeben werden?
- Werden Schutzverletzungen über entsprechende unternehmensinterne Prozesse systematisch zuverlässig und nachvollziehbar dokumentiert?
- Existieren Prozesse, welche eine erforderliche Meldung von Schutzverletzungen an Aufsichtsbehörden und betroffenen Personen gewährleisten?

2.6 Sicherheit der Datenverarbeitung

- Gewährleisten die IT-Systeme und die mit ihnen verbundenen Prozesse einen hohen Schutz der Daten?
  Zu beachten: Die Sicherheit muss aus Sicht des Betroffenen betrachtet werden, sodass ggf. auch vor Zugriffe aus dem Unternehmen zu schützen ist, die zwar aus Sicht des Unternehmens wünschenswert, aus Sicht des Betroffenen jedoch nicht oder auch vermutlich nicht gewünscht ist.
- Welche Datensicherheitsmaßnahmen sind vorhanden?
- Ist ein Informationssicherheits-Management-System (ISMS) im Einsatz?
- Wie ist privacy by design/privacy by default implementiert?
- Welche Vorkehrungen gegen Datenschutzverletzungen existieren schon in meinem Unternehmen?
    - Gibt es eine Risikoanalyse bezogen auf die Risiken für die betroffenen Personen?
    - Gibt es eine Risikobewertung bezogen auf die Risiken für die betroffenen Personen?
    - Werden bei der Risikoanalyse und –bewertung insbesondere die durch unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung/unbefugtem Zugriff entstehen?
    - Existieren Maßnahmen, um die Risiken für die betroffenen Personen zu minimieren?
- Sind die in der DS-GVO genannten TOMs berücksichtigt?
    - Pseudonymisierung eingesetzt?
    - Verschlüsselung durchgeführt? Ende-zu-Ende?
    - Kann die Verfügbarkeit der personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden?
    - Kann der Zugang zu den personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden?
    - Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung?
- Besteht im Unternehmen ein Prozess zur Datenschutz-Folgenabschätzung?
    - Ist gewährleistet, dass für Datenverarbeitungen bei Erfordernis immer eine Datenschutz-Folgenabschätzung durchgeführt wird?

        - Welche Risiken aus der Datenverarbeitung ergeben sich für die Rechte und Freiheiten der Betroffenen?
        - Wie kann ich den Risikoeintritt verhindern oder zumindest minimieren?
    - Ist, falls erforderlich, gewährleistet, dass eine vorherige Konsultation bei der Aufsichtsbehörde erfolgt?

2.7 Datenschutzbeauftragter

- Brauche ich einen Datenschutzbeauftragten?
- Hat der Datenschutzbeauftragte die notwendige fachliche Kompetenz?
    - Ist ein ausreichendes Fachwissen auf dem Gebiet des Datenschutzrechts vorhanden?
    - Ist ein ausreichendes Fachwissen auf dem Gebiet der Datenschutzpraxis vorhanden?
    - Ist ein ausreichendes Fachwissen auf dem Gebiet der Informationstechnik insbesondere auf dem Gebiet der IT-Sicherheit vorhanden?
    - Ist ein ausreichendes Fachwissen in betriebswirtschaftlichen Fragen vorhanden, sodass betriebswirtschaftliche Abwägungen hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten beurteilt werden können?
    - Ist ein ausreichendes Fachwissen aus dem Tätigkeitsumfeld (z. B. medizinische Versorgung oder Bankgeschäfte) vorhanden, sodass die Notwendigkeit der Verarbeitung personenbezogener Daten beurteilt werden können?
- Stehen dem Datenschutzbeauftragten die benötigten Ressourcen zur Verfügung?
- Berichtet der Datenschutzbeauftragte unmittelbar an die Unternehmens- bzw. Geschäftsleitung?

2.8 Weitergehende rechtliche Anforderungen

- Wie weise ich nach, dass meine Datenverarbeitungen DS-GVO-konform erfolgen? Z. B.
    - Dokumentation der Einwilligungserklärungen
    - Verarbeitungsverzeichnis,
    - Dokumentation der ergriffenen Sicherheitsmaßnahmen,
    - Dokumentation der Risikoabschätzung,
    - …
- Rechtsdurchsetzung und Strafen: Rechtsbehelfe, Haftungen und Sanktionen

3 Abgleich Ist- mit Soll-Zustand

Überprüfung, wo Handlungsbedarf besteht; erfolgt idealerweise ergänzend zu den einzelnen Abschnitten bei der Erhebung des Ist-Zustandes

4 Umsetzungsplanung

4.1 Zeitliche und budgetäre Planung (Priorisierung der Ziele)

- Budgetplanung bzgl. Anpassung Workflow/Prozesse
    - Prozesse müssen umgestaltet, Mitarbeiter entsprechend geschult werden.
    - Anpassung der eingesetzten IT-Systeme beauftragen, insbesondere:
        - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
        - Recht auf Datenübertragbarkeit
        - Recht auf Löschung / „Vergessenwerden“

        - Einwilligung mit Symbolen: ggfs. Maschinenlesbarkeit notwendig
        - …
    - Ggf. müssen IT-Systeme sogar ausgetauscht werden
- Budgetplanung beim Datenschutzbeauftragter anpassen
    - Der Datenschutzbeauftragte muss Fortbildungen besuchen, um sich einen Überblick zu verschaffen und das Wissen anzueignen, was konkret an Umsetzungen im Unternehmen ansteht
    - Es muss neue Literatur zur Datenschutz-Grundverordnung angeschafft werden
- Ggfs. ist externe Beratung/Dienstleistung erforderlich
- Vorschlag Vorgehen bzgl. Priorisierung
    - Zunächst Sanktionsgefahr für Unternehmen minimieren
    - Tatbestände bzgl. Art. 83 DS-GVO im Unternehmen nach Möglichkeit beseitigen, von „teuer“ nach „billig“
        - Art. 83. Abs. 5,6: Geldbußen bis zu 20 Mill Euro (bzw. 2% Umsatz)
          Verstöße bzgl.
            - Artt. 5, 6, 7, 9 (fehlende oder fehlerhaft eingeholte Einwilligung)
            - Artt. 12-22 (Verstoß gegen die Rechte der/des Betroffenen)
            - Artt. 44 bis 49 (Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation)
            - Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde

          beseitigen. D.h.
            - Einwilligungsformulare sowie Prozess Einholung Einwilligung wie auch Widerspruch Einwilligung anpassen
            - Prozesse zur Wahrung Betroffenenrechte etablieren (z.B. Archivierungs- und Löschkonzept)
            - Prüfen, ob und wie Daten in ein Drittland übermittelt werden (z.B. Wartung)
        - Art. 83. Abs. 4: Geldbußen bis zu 10 Mill Euro (bzw. 2% Umsatz)
          Verstöße bzgl.
            - Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
            - Art. 28 (Auftragsverarbeiter)
            - Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters)
            - Art. 30 (Verzeichnis von Verarbeitungstätigkeiten)
            - Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde)
            - Art. 32 (Sicherheit der Verarbeitung)
            - Artt. 33 u. 34 (Meldung von Datenpannen an Aufsichtsbehörde und Betroffenen)
            - Art. 35 (Datenschutzfolgenabschätzung)
            - Artt. 36 bis 39 (Datenschutzbeauftragter)

          beseitigen.

4.2 Maßnahmen festlegen

4.2.1 Datenschutzrichtlinie erstellen

- Verantwortung Management klarstellen (analog QM)
- Darstellung, dass die umfassenden Nachweispflichten erkannt wurden und wie man ihnen im Unternehmen gerecht wird
- Einbindung Datenschutzbeauftragter in Unternehmensprozesse beschreiben
    - Wie können Mitarbeiter/Kunden/,,, DSB ansprechen?
    - Wie wird DSB bei der Änderung bestehender oder Implementierung neuer Verarbeitungsverfahren eingebunden?
    - Besteht eine Freigabe-Verpflichtung seitens Datenschutz, wenn personenbezogene Daten verarbeitet werden?
- Je nach Unternehmensgröße: zusätzlich zum Datenschutzbeauftragten (in diesem Fall eher Koordinierungsaufgabe) zusätzliche Verantwortliche benennen und entsprechende Ressourcen bereitstellen

4.2.2 Prozesse gestalten

- Personal schulen (Art. 39 Abs. 1 lit. b. DS-GVO)
- Dokumentation ergänzen
    - Verarbeitungsverzeichnis zu Tätigkeitsverzeichnis migrieren
    - Datenschutz-Folgenabschätzung
        - Erforderlichkeitsprüfung, Festhaltung Ergebnis und wie man dazu kam
        - Ggf. Vorgaben Aufsichtsbehörden prüfen
        - Prozessbeschreibung
        - Festlegen, wann eine Hinzuziehung der Aufsichtsbehörde („Vorherige Konsultation“) erforderlich ist
    - Vertragsmanagement anpassen (z. B. hinsichtlich ADV)
    - Nachweis Datenschutzschulungen gewährleistet? Ist ein Datenschutz Schulungskonzept vorhanden?
    - Nachweis Datensicherheit
    - Rechenschaftspflicht bzgl. Dokumentation erfüllt? D. h.
        - Schrift- oder elektronischer Form
        - Jederzeit auffindbar
        - Ergebnis eines klaren Dokumentationsprozesses einschließlich eindeutiger Zuweisung von Verantwortlichkeiten für die Dokumentation
        - Klare Beschreibung der aktuellen Situation und der Umstände
        - Verweis auf die Rechtsgrundlage
        - Angabe des Verfassers und der Änderungshistorie
- IT-Sicherheit prüfen
    - Steht eine dem „Stand der Technik“ entsprechende IT-Landschaft zur Verfügung?
- Meldepflichten bei Datenpannen: entsprechenden Workflow implementieren
  Cave:
    - Ausnahmslos alle - d. h. insbesondere ohne Abwägung von Risiken für den Betroffenen – Datenschutzverletzungen sind gemäß Art. 33 Abs. 5 DS-GVO zu dokumentieren; hierzu zählt beispielsweise auch, wenn sich interne Mitarbeiter unberechtigten Zugriff verschafften oder es diesen aufgrund fehlerhaft konfigurierter Berechtigungen möglich war, ein Nachweis aufgrund fehlender Protokollierung aber nicht möglich ist

- Neu im Vergleich zur jetzigen Rechtslage ist, dass nicht mehr bestimmte Datenarten abhandenkommen müssen, sondern nun jedes personenbezogene Datum zählt.

- Datenschutzbeauftragter
  - Konzerndatenschutzbeauftragter sinnvoll?
  - Interner oder externer Datenschutzbeauftragter?
  - Mindestpflichten beschreiben
    - Information und Beratung
      - Inkl. Mitarbeiterschulungen
    - Überwachung der Einhaltung der Vorgaben der DSGVO sowie der Datenschutzstrategien im Unternehmen
      - Entsprechend Einbindung im Unternehmen erforderlich, d. h. Zuweisung von Zuständigkeiten und Legitimierung entsprechender Kontrollmöglichkeiten
      - „Überwachung der Einhaltung“ (Art. 39 Abs. 1 lit b DS-GVO) ggf. mit einer strafrechtlichen oder ordnungswidrigkeitsrechtlichen Verantwortlichkeit aufgrund einer Garantenstellung verbunden
    - Beratung bei der Datenschutz-Folgenabschätzung sowie Überwachung von deren Durchführung
      - Cave: Überwachen impliziert einen Interessenkonflikt bzgl. der Durchführung durch den DSB: Der DSB kann eine DSFA nicht durchführen, da er sich dann selbst überwachen müsste
    - Zusammenarbeit mit Aufsichtsbehörden
    - Risikobeurteilung (Art. 39 Abs. 2 DS-GVO)
  - Unterstützung DSB durch Unternehmen gewährleisten
    - Zurverfügungstellung erforderlicher Ressourcen (inkl. Weiterbildungsmöglichkeiten)
    - Zugang zu Verarbeitungsvorgängen und personenbezogenen Daten
    - Weisungsfreiheit
  - Direkte Berichterstattung an Verantwortlichen, d. h. (oberste) Unternehmensleitung
  - Beachtung Geheimhaltungspflicht, d. h. Aussageverweigerungsrecht bzgl. Leitungsorganen implementieren
  - Veröffentlichung von Kontaktdaten

- Abbildung Betroffenenrechte
  - Abbildung der Informationspflichten im Workflow, insbesondere muss bei Auskunftsanfragen Betroffener berücksichtigt werden
    - Verarbeitungszwecke müssen angegeben werden
    - Rechtsgrundlage, aufgrund welcher die Verarbeitung erfolgt, muss angegeben werden
    - Speicherfristen müssen angegeben werden, d. h.
      - Eine Mitteilung an den Betroffenen, wann seine Daten gelöscht werden, muss enthalten sein
      - Ggf. in Form von für den Betroffenen nachvollziehbaren Kriterien zur Speicherbegrenzung
    - Insbesondere Benachrichtigung Betroffener bei Aufhebung einer Sperrung

  Hinweis: ErwGr 63 sieht vor, dass Betroffenen nach Möglichkeit ein Fernzugang zur Verfügung gestellt wird, welcher ihnen einen direkten Zugang zu ihren Daten ermöglicht

- Implementierung von Korrektur/Sperrung/Löschung

- Umgang mit Beschäftigtendaten
  - Werden Beschäftigtendaten extern verarbeitet?
  - Verpflichtung Beschäftigte auf Wahrung des Datengeheimnisses
    - Verpflichtung nur noch in Art. 28 Abs. 3 lit. b DS-GVO vorgesehen
    - § 53 BDSG neu gilt nicht für Verarbeitungen, welche unter die Regelungen der DS-GVO fallen!
    - Aber
      - Verbot der Weitergabe von während einer Tätigkeit erhaltener Informationen nach Beendigung der Tätigkeit ist in Art. 6 Abs. 1 bzw. Art. 9 Abs. 1 DS-GVO, enthalten (Erlaubnistatbestand zur Verarbeitung der Daten nur während der Tätigkeit, Weitergabe nach Beendigung der Tätigkeit mangels Verarbeitungserlaubnis demnach verboten)
      - Verantwortlicher hat umfassende Nachweispflichten bzgl. der datenschutzgerechten Verarbeitung (insbesondere Artt. 5, 24 DS-GVO)
      - Daher Verpflichtung Beschäftigte auch weiterhin unumgänglich
  - Überprüfung/Anpassung Betriebsvereinbarungen
    Hinweis: Betriebsvereinbarungen können grundsätzlich Rechtsgrundlagen für die Verarbeitung personenbezogener Daten bilden (§ 26 Abs. 4 BDSG neu), müssen dabei die Anforderungen der DS-GVO hinreichend genug entsprechen, damit sie rechtsgültig sind. D.h. insbesondere Übereinstimmung mit Art. 5 DS-GVo sowie die Wahrnehmung der Betroffenenrechte prüfen

- Auftragsverarbeitung
  - Verträge anpassen
  - TOMs dokumentieren (lassen) und bewerten,
  - Wirksamkeit der TOMs prüfen, Penetrationstests und Informationssicherheitsmanagement planen
  - Auftragnehmer: Eigene Pflichten beachten

- Formulare und Einwilligungen anpassen, inkl. Internetauftritt
  - Information des Betroffenen an neue Anforderungen anpassen (z. B. Symbole ergänzen)
  - Insbesondere Einwilligung anpassen
    - Cave: Nur eine Einwilligung, welche den Anforderungen der DS-GVO genügt, kann nach Eintreten der Geltung der DS-GVO weiterhin als Legitimationsgrundlage für eine Datenverarbeitung im Sinne von Art. 4 Abs. 2 DS-GVO gelten.

- Datenschutzerklärung anpassen, ggf. Webtracking anpassen
  (Cave: IP-Adresse personenbezogenes Datum, BGH Urt. v. 16.05.2017, Az. VI ZR 135/13)

4.3 Maßnahmen umsetzen

Hier steht, was sie bisher umsetzten…

5 Sanktionsübersicht

5.1 Datenschutz-Grundverordnung

5.1.1 Art. 83. Abs. 4: Geldbußen bis zu 10 Mill Euro (bzw. 2% Umsatz)

Verstöße bzgl.

- Art. 8 (Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft)
- Art. 11 (Identifizierung der betroffenen Person für Verarbeitung erfolgt, aber nicht erforderlich)
- Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
- Art. 28 (Auftragsverarbeiter)
- Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters)
- Art. 30 (Verzeichnis von Verarbeitungstätigkeiten)
- Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde)
- Art. 32 (Sicherheit der Verarbeitung)
- Artt. 33 u. 34 (Meldung von Datenpannen an Aufsichtsbehörde und Betroffenen)
- Art. 35 (Datenschutzfolgenabschätzung)
- Artt. 36 bis 39 (Datenschutzbeauftragter)
- Art. 41 Abs. 4 (keine Maßnahmen ergriffen für Verstoß gegen Verhaltensregeln)
- Artt. 42, 43 (Verstoß gegen Anforderungen bzgl. Zertifizierung)

5.1.2 Art. 83. Abs. 5,6: Geldbußen bis zu 20 Mill Euro (bzw. 4% Umsatz)

Verstöße bzgl.

- Art. 5 (grundlegende Anforderungen nicht eingehalten)
- Art. 7 (fehlende oder fehlerhaft eingeholte Einwilligung bzw.
- Artt. 6,9 (Verarbeitung ohne Erlaubnistatbestand)
- Artt. 12-22 (Verstoß gegen die Rechte der/des Betroffenen)
- Artt. 44 bis 49 (Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation)
- Art. 58 Abs. 1, 2 (fehlende Unterstützung von Aufsichtsbehörden, Verstoß gegen Vorgaben Aufsichtsbehörde)
- Artt. 85-31 (Verstoß gegen Rechtsvorschriften eines Mitgliedstaates)
- Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde

5.2 Bundesdatenschutzgesetz (gültig ab 25. Mai 2018)

5.2.1 § 42 Strafvorschriften

- Freiheitsstrafe bis zu 3 Jahren: nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne Rechtsgrundlage
    a) einem Dritten übermitteln oder
    b) auf andere Art und Weise zugänglich machen und hierbei gewerblich handeln
- Freiheitsstrafe bis zu 2 Jahren: nicht allgemein zugängliche personenbezogene Daten
    a) ohne Rechtsgrundlage verarbeiten oder
    b) durch unrichtige Angaben erschleicht und
        1. hierbei gegen Entgelthandeln oder

2. in der Absicht handeln, sich oder einen anderen zu bereichern oder einen anderen zu schädigen

Hinweis:

1. Verfolgung nur auf Antrag. Antragsberechtigt sind: betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde (§ 42 Abs. 3 BDSG)
2. Eine Meldung nach Art. 33 DS-GVO darf in einem Strafverfahren nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden (§ 42 Abs. 4 BDSG)

5.2.2 § 43 Bußgeldvorschriften

Geldbuße bis zu 50.000 Euro, wer vorsätzlich oder fahrlässig

a) entgegen § 30 Abs. 1(Bewertung Kreditwürdigkeit bzgl. Verbraucherkredite) ein Auskunftsverlangen nicht richtig behandeln oder
b) entgegen § 30 Abs. 2 S. 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichten

Hinweis: Gegen Behörden und sonstige öffentliche Stellen werden keine Geldbußen verhängt (§ 43 Abs. 3 BDSG)