Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO III

To-Dos für die Übergangsfrist bis zur Geltung der DS-GVO

INHALT

1. Phase – Kommunikationsplan 5

2. Phase – Aktionsplan 5

3. Phase – Umsetzung 5

3.1 Anpassung Prozesse 5

3.2 Ggf. Anpassung IT-Systeme / Datensicherheit 8

3.3 Datenschutz in Produkten 8

3.4 Transparenzpflichten & Betroffenenkommunikation 8

3.5 Vertragsmanagement 9

To-Dos für die Übergangsfrist bis zur Geltung der DS-GVO

Bis zur Geltung der DS-GVO ab 25. Mai 2018 verbleibt den Unternehmen in der EU nicht viel Zeit, ihre Datenschutzorganisation an die neuen Anforderungen der DS-GVO anzupassen. Dabei setzt die DS-GVO auf ein Datenschutzmanagementsystem, das unabhängig von der Bestellung eines Datenschutzbeauftragten in der eigenen Verantwortung des Unternehmens wirksam sein muss. Im Hinblick auf die vielfachen Dokumentations- und Nachweisanforderungen unter dem Stichwort Rechenschaftspflicht (Accountability) der DS-GVO bietet es sich an, das Datenschutzmanagementsystem stark mit anderen, bereits im Unternehmen bestehenden Management- und Kontrollsystemen zu verknüpfen. Die DS-GVO setzt zum Beispiel das Vorhandensein eines IT-Sicherheitsmanagements voraus. Auch verweist sie immer wieder auf Aspekte des Risikomanagements. Durch Einbeziehung solcher etablierter Systeme können Synergien geschaffen und ausschließlich für den Datenschutz getroffene Maßnahmen vermieden bzw. verringert werden.

Als Schwierigkeit zur Etablierung eines Datenschutzmanagements nach DS-GVO vor deren Gültigkeit könnte gesehen werden, dass den nationalen Gesetzgebern eine Reihe von Regelungsspielräumen verbleiben, die bislang nicht ausgefüllt sind. Unter diesem Gesichtspunkt die Anpassung zu verschieben ist hinsichtlich der zu erwartenden Aufgaben nicht anzuraten.

Ein Aufschieben ist auch nicht erforderlich: Die organisatorischen Maßnahmen sind in der DS-GVO weitgehend abschließend geregelt. Im nichtöffentlichen Bereich eröffnet die DS-GVO dem nationalen Gesetzgeber kaum Regelungsspielräume, auf deren Ausfüllung im Hinblick auf die Überführung der Organisation vom BDSG zur DS-GVO gewartet werden müsste.

Das nachfolgend beschriebene Modell zur Etablierung eines Datenschutzmanagements nach DS-GVO fokussiert sich auf die Ausgangssituation in Deutschland nach dem BDSG. Die Besonderheit in Deutschland besteht darin, dass das BDSG die verpflichtende Bestellung von Datenschutzbeauftragten vorsieht. Voraussichtlich wird es in Deutschland bei den bekannten Voraussetzungen für die Bestellpflicht von Datenschutzbeauftragten bleiben, da von einem entsprechenden Regelungsspielraum in der DS-GVO Gebrauch gemacht werden soll. In anderen Mitgliedstaaten der EU wird die Bestellung eines Datenschutzbeauftragten entweder von der jeweiligen nationalen Regelung oder von der Erfüllung der Voraussetzungen des Art. 37 Abs. 1 DS-GVO abhängig sein[1]. Dennoch kann das beschriebene Modell auch im europäischen Umfeld genutzt werden, da das Datenschutzmanagement nach DS-GVO als eigene Aufgabe der Organisation auch unabhängig von der Bestellung eines Datenschutzbeauftragten vorhanden sein muss. Soweit der Datenschutz bereits nach BDSG organisiert ist, kann in weiten Bereichen hierauf aufgebaut werden. An vielen Stellen wird sich hierdurch der Aufwand zur Umsetzung der DS-GVO reduzieren.

Während das Vorgehensmodell unter Berücksichtigung nationaler Besonderheiten, etwa zum Beschäftigtendatenschutz oder zur wettbewerbsrechtlichen Zulässigkeit werblicher Ansprache, grundsätzlich EU-weit genutzt werden kann, werden im Folgenden die besonderen Aspekte des internationalen Datenaustauschs mit Drittländern nicht besonders betrachtet. Die Behandlung dieser komplexen Themen bleibt dem GDD-Arbeitskreis Internationales vorbehalten.

Die Einstellung des Unternehmens auf die DS-GVO sollte als Projekt organisiert werden. Dabei kann und sollte dieses Projekt durch den jeweiligen Datenschutzbeauftragten angestoßen und koordiniert werden. Die Umsetzung des Datenschutzes ist jedoch eine unternehmensweite Aufgabe, bei der der Datenschutzbeauftragte zwar sein Fachwissen einbringen soll, aber die er nicht selbst stemmen kann und – nach BDSG wie nach DS-GVO – auch nicht in eigener Verantwortung stemmen soll.

Ab 25. Mai 2018 wird das Funktionieren des Datenschutzmanagements nach DS-GVO ohne weitere Übergangsfrist erwartet. Mit diesem Datum erlangen auch die umfangreichen und verschärften Haftungs- und Bußgeldnormen Gültigkeit. Damit steigt allein im Hinblick auf organisatorische Verfehlungen das Bußgeldrisiko auf bis zu 10 Millionen € oder bis zu 2 % des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist.

Daher gilt: Es ist viel zu tun und der Countdown läuft!

1 Siehe auch WP 243 „Guidelines on Data Protection Officers“ der Artikel-29-Gruppe, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

1. Phase – Kommunikationsplan

>> **Analyse der neuen Anforderungen und Kommunikation des Änderungsbedarfs**
- > Identifizierung von Adressaten
- > **Gewährleistung einer effizienten, zielgruppengerechten Information** durch allgemeine und spezielle Informationsmodule nach folgender Gliederung:
  - Allgemeingültige Informationen zum Thema, z.B. Geltungszeitpunkt, unmittelbare Geltung in Deutschland, Anwendungsbereich
  - Wichtige Themen zur DS-GVO, z.B. erhöhte Risiken durch immens gestiegene Bußgeldrahmen, Accountability-Ansatz, Zuständigkeiten und Verantwortlichkeiten nach der DS-GVO
  - Konsequenzen für den Adressatenkreis
  - Diskussion und Erarbeitung von Handlungsempfehlungen

2. Phase – Aktionsplan

>> **Bestimmung des konkreten Handlungsbedarfs mittels Gap-Analyse**/Soll-Ist-Abgleich; es bietet sich ein Modell an, das folgende Faktoren berücksichtigt:
- > Feststellung der neuen gesetzlichen Anforderungen (Soll-Zustand)
- > Bestandsaufnahme des betrieblichen Ist-Zustands
- > Bestimmung des Handlungs- und Umsetzungsbedarfs
- > Risikoanalyse und Accountability

>> **Beschaffung erforderlicher Ressourcen/** Deckung des erhöhten Bedarfs zur Umsetzung der DS-GVO

3. Phase – Umsetzung

Die Umsetzungsphase bezieht sich auf verschiedene Aspekte. So bedarf es einer Anpassung der bestehenden unternehmensinternen Prozesse und ggf. der IT-Systeme an die Vorgaben der DS-GVO. Deren Anforderungen wirken sich darüber hinaus im Bereich der Produktentwicklung sowie der Kommunikation mit Kunden, Vertragspartnern und Beschäftigten aus. Einer Anpassung bedarf schließlich auch das Vertragsmanagement, soweit im Rahmen der Verarbeitung personenbezogener Daten Dienstleister eingeschaltet bzw. entsprechende Dienstleistungen erbracht werden.

3.1 Anpassung Prozesse

>> **Prüfung der DS-Organisationsstruktur; Anpassung unternehmensinterner Regularien/ Richtlinien/Policies/Handbücher,**
- > Bestandsaufnahme: Welche Richtlinien, Handbücher etc. gibt es?
  - Compliance Handbuch
  - Datenschutzrichtlinie
  - ITK-Sicherheitshandbuch
  - Richtlinien zur Vertragserstellung (ADV-Verträge), vgl. auch Anpassung des Vertragsmanagements
  - Datenschutzrelevante Prozesse, Produkte und Services ? – Sicherstellung der Privacy-by-Design bzw. Privacy-by-Default-Vorgaben?
- > Welche Prozesse gibt es?
  - Formulare zur Verfahrensmeldung und Vorabprüfung kritischer Datenverarbeitungen?
  - Datenschutzunterweisung und -verpflichtung der mit der Datenverarbeitung Beschäftigten?

- Risikomanagementprozess?
- Meldung von Datenpannen

> Was fehlt, sollte ergänzt werden

> Was vorhanden ist, sollte auf Anpassungsbedarf geprüft werden

>> **Überprüfung und ggf. Anpassung von Betriebsvereinbarungen**

> Vereinbarung der Betriebsparteien zum gemeinsamen Vorgehen
  - Priorisierung der zu prüfenden Betriebsvereinbarungen, z.B.
  - Zentrale Personaldatenverarbeitung
  - Nutzung IT- und TK-Anlagen
  - Zentrale kaufmännische Systeme

> Betriebsvereinbarungen müssen **Anforderungen der DS-GVO hinreichend umsetzen**. Unklar ist bislang noch, wie mit bestehenden Betriebsvereinbarungen umgegangen werden soll. Bei einer Prüfung bestehender und neuer Regelungen gilt:
  - Besonderes Augenmerk auf Transparenz und Grundrechtsschutz (Art. 88 Abs. 2 DS-GVO)
  - Vereinbarkeit mit Grundsätzen des Art. 5 DS-GVO
  - Umgang mit besonderen Datenkategorien (Art. 9 DS-GVO) ist zu prüfen
  - Erfüllung der Informationspflichten nach Art. 12 ff. DS-GVO; Hinweis auf Betroffenenrechte
  - Datenschutz-Folgenabschätzung

>> **Nachweis-/Dokumentationspflichten aufgrund der Accountability (Rechenschaftspflicht) bzw. spezifischer Vorgaben der DS-GVO, insbesondere bzgl.**

> Datenschutzmanagement/-organisation und Sicherstellung entsprechender Dokumentationen

> Datenschutzpolicies (einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen)

> durchgeführter Verarbeitungstätigkeiten (Art. 30 DS-GVO)

> durchgeführter Risikobewertungen/Datenschutz-Folgenabschätzungen

> Datenschutzverstößen/-vorfällen

>> **Nachfolgeregelung zu § 5 BDSG (Verpflichtung auf das Datengeheimnis)/Schulung**

> BDSG: Leitung der verantwortlichen Stelle muss die mit der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis verpflichten (§ 5 BDSG)

> BDSG: Enger Zusammenhang mit Schulungspflicht des DSB (§ 4g Abs. 1 S. 4 Nr. 2 BDSG), da Inhalt von § 5 BDSG regelmäßig erst nach Schulung vollumfänglich nachvollzogen werden kann.

> Ausdrücklich ist die Verpflichtung nur noch vorgesehen in Art. 28 Abs. 3 Buchst. b) DS-GVO (Auftragsverarbeiter). Aber: Umfassende Nachweispflicht der ordnungsgemäßen Datenschutzorganisation (Art. 24 DS-GVO). Damit bleiben Verpflichtung und Schulung auch künftig wichtiger Bestandteil eines Datenschutzmanagementsystems.

> Verpflichtung wie Schulung nach DS-GVO Aufgabe der Leitung der öffentlichen bzw. privaten Stelle; Schulungsaufgabe kann aber dem Datenschutzbeauftragten übertragen werden

> Keine „Nachverpflichtung“ aufgrund der Gel-

tung der DS-GVO erforderlich, wenn zurückliegend auf BDSG-Basis ordnungsgemäß verpflichtet wurde
- > Empfehlung: regelmäßige Auffrischung, z.B. bei Aufgabenwechsel oder wesentlichen neuen Funktionen

>> **Datenschutz-Folgenabschätzung (DS-FA) durch Fachabteilung**
- > Gewährleistung der Umsetzung der Vorgaben zur DS-FA (Art. 35 DS-GVO)
  - **Prüfung des Erfordernisses einer DS-FA:** Jedes Verfahren personenbezogener Datenverarbeitung ist vor Beginn darauf zu prüfen, ob es voraussichtlich hohe Risiken für die betroffenen Personen birgt und daher eine DS-FA durchzuführen ist (Hilfestellung durch gesetzliche Regelbeispiele sowie Black- bzw. Whitelist der Datenschutzaufsicht)
  - **Durchführung der DS-FA** (sofern vorhanden, ist Rat des Datenschutzbeauftragten einzuholen); bei mehreren ähnlichen Verarbeitungsvorgängen mit ähnlich hohen Risiken reicht eine (gemeinsame) Abschätzung
  - **Dokumentation**, Überwachung und Fortschreibung der DS-FA
  - Verbleibt nach der DS-FA trotz Abhilfemaßnahmen ein hohes Risiko, ist vor der Verarbeitung die **Aufsichtsbehörde** zu **konsultieren** (Art. 36 Abs. 1 DS-GVO)

>> **„Datenpannen“**
- > Vorhandensein eines Krisenreaktionsplans für Datenpannen?

> Zu den Details eines solchen Plans vgl. GDD-Ratgeber „Datenpannen“, 2. Aufl. 2015, online unter https://www.gdd.de/downloads/praxishilfen/GDD-Ratgeber_Datenpannen_2._Aufl._2015.pdf

- > Wenn ja, Prüfung auf Anpassungsbedarf, insbes. bzgl.
  - Voraussetzungen der Melde-/Benachrichtigungspflicht
  - Zeitliche Vorgaben für die Meldung
  - Inhalt von Meldungen/Benachrichtigungen
  - Pflicht zur Dokumentation von Datenpannen
- > Wenn nein, Entwicklung eines entsprechenden Plans
- > **Prävention**, d.h. Vermeidung von Datenschutzverletzungen bzw. des Entstehens diesbezüglicher Informationspflichten durch ausreichende Sicherheitsmechanismen und **Verschlüsselung nach dem Stand der Technik**

>> **Umsetzung der (antragsunabhängigen) Verpflichtung zur Löschung (Löschkonzept)**
- > Verpflichtung zur Angabe der Speicherdauer bei Datenerhebung (Art. 13 Abs. 2, 14 Abs. 2 DS-GVO)

>> **Gewährleistung der Betroffenenrechte**
- > Prozesse entwickeln für die Rechte auf Auskunft, Löschung, Berichtigung, Vergessenwerden, Datenportabilität und Widerspruch
- > Verpflichtung zur Information über ein Löschungsverlangen, wenn die zu löschenden personenbezogenen Daten öffentlich gemacht wurden (Art. 17 Abs. 2 DS-GVO)

>> **Ggf. Anpassung stattfindender Datenverarbeitungen** an geänderte Zulässigkeitsregeln durch die DS-GVO

3.2 Ggf. Anpassung IT-Systeme / Datensicherheit

>> **Art. 32 DS-GVO:** Vertraulichkeit, Integrität und Verfügbarkeit (klassische Schutzziele der IT-Sicherheit) **plus Belastbarkeit („resilience") der Systeme und Dienste als neues Schutzziel**

>> **Sicherheit nach DS-GVO**[2]
- > Schutzbedarf personenbezogener Daten feststellen
- > Risikobewertung mit Fokus Betroffener
- > Maßnahmen treffen unter Berücksichtigung von Stand der Technik und Implementierungskosten (Verhältnismäßigkeit)
- > **Nachweise für Konformität** (Art. 5, 24 DS-GVO), z.B. durch Zertifizierung

3.3 Datenschutz in Produkten

>> **Berücksichtigung von Privacy-by-Design und Privacy-by-Default bei der Produktentwicklung**
- > Geeignete technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze bereits zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung
- > Geeignete technische und organisatorische Maßnahmen, um durch Voreinstellung sicherzustellen, dass nur zweckbestimmte, personenbezogene Daten verarbeitet werden

>> **Datenportabilität**
- > Bereitgestellte Daten sind grundsätzlich in einem Format zu erhalten, die eine direkte Übertragung von einem Verantwortlichen auf einen anderen Verantwortlichen technisch ermöglichen

>> **Elektronische Zugänge**
- > ErwGr 63 sieht vor, dass Betroffenen nach Möglichkeit der Fernzugang zu einem sicheren System bereitgestellt werden soll, der direkten Zugang zu ihren personenbezogenen Daten ermöglicht.

3.4 Transparenzpflichten & Betroffenenkommunikation

>> **Erweiterte Transparenz- und Informationspflichten bei Datenerhebung**
- > Differenzierung zwischen Datenerhebung beim Betroffenen (Art. 13 DS-GVO) und Erhebung aus anderer Quelle (Art. 14 DS-GVO)
- > **Problem: Verhältnis von Art. 13 Abs. 1 zu Art. 13 Abs. 2 DS-GVO** (und Art. 14 Abs. 1 zu Art. 14 Abs. 2 DS-GVO)?
  Informationen nach den Absätzen 2 müssen wohl nur gegeben werden, soweit diese „notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten".

2 Vgl. BayLDA, https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf.

Ein Maßstab für die Beurteilung, wann dies der Fall ist, fehlt jedoch. Aus Gründen der Rechtssicherheit und praktischen Handhabung kann es sich daher empfehlen, alle ggf. notwendigen Informationen zu geben.

- **Art und Weise der Information:** leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst; ggf. zusätzlich visuelle Elemente (delegierter Rechtsakt)
- **Medienbrüche** durch DS-GVO nicht ausdrücklich ausgeschlossen. Gemäß ErwG 58 können Informationen auch in elektronischer Form zur Verfügung gestellt werden.
- **Gestuftes Informationsverfahren**[3] wohl auch in Zukunft statthaft und sinnvoll

>> Einwilligungsmanagement

Während nach dem BDSG eine Einwilligung grundsätzlich in Schriftform erfolgen muss, gewährt die DS-GVO eine Formfreiheit. Der Betroffene kann die Einwilligung in jeglicher Form erteilen. Es kommt nur darauf an, dass aus dem Handeln des Betroffenen unmissverständlich erkennbar wird und belegt werden kann, in welche konkrete Datenverarbeitung er einwilligt.

- **Neu einzuholende Einwilligungen** sollten bereits vor Anwendbarkeit der DS-GVO den Vorgaben der DS-GVO genügen
  Bzgl. **Alteinwilligungen** Prüfung, inwiefern diese auch nach Geltung der DS-GVO eine belastbare Rechtsgrundlage darstellen

> Vgl. in diesem Zusammenhang den Beschluss des Düsseldorfer Kreises vom 13./14. September 2016 zur Fortgeltung bisher erteilter Einwilligungen unter der DS-GVO. Nach Erwägungsgrund 171 S. 3 DS-GVO sollen bisher erteilte Einwilligungen fortgelten, sofern sie der Art nach den Bedingungen der DS-GVO entsprechen. Bisher rechtswirksame Einwilligungen erfüllten grundsätzlich diese Bedingungen, so der Düsseldorfer Kreis.

3.5 Vertragsmanagement

- Überprüfung bereits geltender bzw. noch abzuschließender Verträge mit Datenschutzrelevanz dahingehend, ob die Anforderungen der DS-GVO eingehalten sind; zu überprüfen sind
  - insbes. **vertragliche Regelungen im Zusammenhang mit Outsourcingverhältnissen**
  - Verträge über die Übermittlung personenbezogener Daten
  - sonstige Verträge, welche die Verarbeitung personenbezogener Daten betreffen
- Ab 25. Mai 2018 müssen die Verträge den DS-GVO-Vorgaben genügen
- **Anpassungsverträge für „Alt"-Verträge**
- Für die Übergangszeit bis zur Geltung der DS-GVO ggf. Abschluss von „Hybrid"-Verträgen, die den Vorgaben von BDSG und DS-GVO genügen

3 Vgl. Art. 29-Datenschutzgruppe, WP 100 vom 25.11.2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt.

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (Dezember 2016)