KPMG

Datenschutz im Fokus der Internen Revision

Handlungsempfehlungen für die Interne Revision

Inhalt

KPMG

Datenschutz-Grundverordnung – Hintergrund und Auswirkungen

Mit Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) zum 25. Mai 2018 sind weitreichende Auswirkungen auf eine Vielzahl von Unternehmensbereichen verbunden, darunter auch auf die Interne Revision.

Bereits bestehende Datenschutzbestimmungen zur Verarbeitung von personenbezogenen Daten wurden hierdurch weiter verschärft und das mögliche Strafmaß bei Missachtung angehoben. So können Bußgelder von bis zu 20 Millionen Euro oder – ab einem Umsatz von 500 Millionen Euro – 4 Prozent des weltweiten Jahresumsatzes verhängt werden. Die wesentlichen Anforderungen und Auswirkungen der DSGVO sind in Abbildung 01 zusammenfassend dargestellt.

Personenbezogen sind Daten, die direkt oder indirekt Rückschlüsse auf die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität einer natürlichen Person erlauben. Darunter fallen insbesondere Informationen wie Namen, Kennnummern, Standortdaten, Onlinekennungen oder besondere Merkmale, die betroffenen Personen zugeordnet werden können.[1]

Bei der Mehrzahl der Geschäftsprozesse fallen personenbezogene Daten an, sodass die von der Internen Revision durchgeführten Prüfungshandlungen regelmäßig eine Verarbeitung von personenbezogenen Daten, entweder von Beschäftigten oder von Dritten, beinhalten.

01 **Überblick EU-Datenschutz-Grundverordnung (DSGVO)**
Wesentliche Anforderungen und Auswirkungen

1	**Bußgelder:** Bei Verstößen gegen die DSGVO sind Bußgelder von bis zu 20 Millionen Euro oder 4 Prozent des gesamten weltweiten Vorjahresumsatzes vorgesehen.
2	**Datenschutz-Managementsystem:** Die DSGVO setzt hohe Governance-Maßstäbe, die für alle Unternehmen und in allen Branchen gelten und die Etablierung eines Datenschutz-Managementsystems erfordern.
3	**Rechenschaftspflichten:** Die Dokumentationspflichten wurden deutlich ausgeweitet. Die Compliance-Verantwortung liegt beim Datenverarbeiter, der nun die Einhaltung der DSGVO nachweisen muss (faktische Beweislastumkehr).
4	**Sanktionierungsansatz:** Sanktioniert wird insbesondere das Nicht-Vorhalten DSGVO-konformer Prozesse und Maßnahmen – nicht erst der Datenschutzverstoß als solcher.
5	**Risikoanalyse und -folgenabschätzung:** Unternehmen müssen das Risiko zukünftiger Datenverarbeitungen und ihre Folgewirkungen auf den Datenschutz abschätzen und gegebenenfalls mit der Aufsichtsbehörde abstimmen.
6	**Informations- und Auskunftspflichten:** Personen, deren Daten verarbeitet werden, erhalten neue Rechte (zum Beispiel Recht auf Vergessenwerden). Es gelten erweiterte, fristgebundene Informationspflichten für Unternehmen.
7	**Auftragsverarbeitung:** Die Anforderungen an die Auftragsverarbeitung wurden verschärft, wodurch eine Vielzahl von Dienstleisterverträgen angepasst werden müssen.
8	**Meldepflichten:** Die Meldepflichten für Datenschutzverstöße wurde erweitert. Eine Anzeige bei der Aussichtsbehörde muss innerhalb von 72 Stunden nach Bekanntwerden erfolgen.
9	**Technische und organisatorische Maßnahmen:** Um die Betroffenenrechte zu stärken, wurden erweiterte Pflichten wie Privacy by Design und Privacy by Default eingeführt.
10	**Marktortprinzip:** Die DSGVO gilt auch für Unternehmen mit Sitz außerhalb der EU, wenn die Datenverarbeitung einen Bezug zu europäischen Betroffenen hat.

Quelle: KPMG in Deutschland, 2019

1 Artikel 4 Ziffer 1 DSGVO

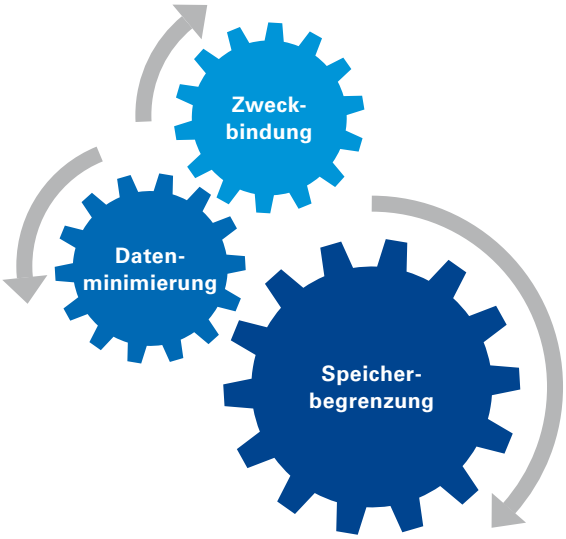
Berücksichtigung des Datenschutzes im Rahmen der Revisionsprozesse

Im Hinblick auf die Interne Revision sind bei der Verarbeitung von personenbezogenen Daten die folgenden Bestimmungen der DSGVO besonders hervorzuheben (Abbildung 02):

- **Zweckbindung:** Die Verarbeitung muss auf der Grundlage eines festgelegten, eindeutigen und legitimierten Zwecks erfolgen.
- **Datenminimierung:** Die Verarbeitung ist auf ein für die Zwecke notwendiges Maß zu beschränken.
- **Speicherbegrenzung:** Die Speicherung von personenbezogenen Daten darf nur so lange erfolgen, wie es für den Verarbeitungszweck erforderlich ist.

Da die Interne Revision funktional für die Durchführung von Prüfungen zuständig ist und grundsätzlich ein uneingeschränktes Informationsrecht[2] besitzt, lässt sich die Notwendigkeit, personenbezogene Daten zu verarbeiten, als legitimer Zweck ableiten.

02 **Aspekte bei der Verarbeitung von personenbezogenen Daten**



Quelle: KPMG in Deutschland, 2019

Im Rahmen der Prüfungsvorbereitung, -durchführung und -dokumentation sind jedoch einige Datenschutzvorgaben zu beachten.

Bereits während der Prüfungsvorbereitung sollte im Prüfungsauftrag genau beschrieben werden, welche personenbezogenen Daten in die Prüfung einbezogen und mit welchem Prüfungsziel sie verwendet werden. Darüber hinaus ist festzuhalten, ob der geplante Zweck der Prüfungshandlungen nur genau mit den zu verwendenden personenbezogenen Daten erfüllbar ist oder welche alternativen Vorgehensweisen gegebenenfalls möglich sind, durch die die Betroffenen in ihren Persönlichkeitsrechten weniger belastet werden.

Im Rahmen der Prüfungsdurchführung, deren Umfang sich aus dem Prüfungsauftrag ergibt, ist dem bereits erwähnten Prinzip der Datenminimierung zu folgen. Wenn es der Verwendungszweck zulässt und dadurch kein unverhältnismäßig hoher Aufwand entsteht, sollten personenbezogene Daten pseudonymisiert oder anonymisiert verarbeitet werden.

Bei der Prüfungsdokumentation ist darauf zu achten, dass die in den Prüfungsdokumenten bzw. -berichten festgehaltenen Ergebnisse keine personenbezogenen Daten enthalten. Sind personenbezogene Daten im Einzelfall selbst Teil der Untersuchungsergebnisse oder sind aufgrund der Unternehmensgröße aus Abteilungen oder Bereichen Rückschlüsse auf einzelne Personen möglich, sind besondere Schutzmaßnahmen zu etablieren und insbesondere ein besonderer Vertraulichkeitsgrad zu definieren.

Bestehen keine gesetzlichen Aufbewahrungsfristen oder sind diese Fristen abgelaufen, sollten personenbezogene Daten gelöscht oder anonymisiert werden. Hierzu ist das Vorhalten eines Löschkonzepts erforderlich. Besondere Vorsicht ist bei sensiblen und schutzbedürftigen personenbezogenen Daten wie Angaben über die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder die sexuelle Orientierung geboten. Die Zulässigkeit einer Erhebung, Verarbeitung und Nutzung solcher Daten richtet sich allein nach § 28 Abs. 5 bis 9 Bundesdatenschutzgesetz (BDSG).

2 DIIR Revisionsstandard Nr. 3, Mindeststandard 2; IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW PS 983), Mindeststandard 2

Datenschutz als Prüfungsthema für die Interne Revision

Datenschutz als wesentlicher Risikobereich im Audit Universe der Internen Revision

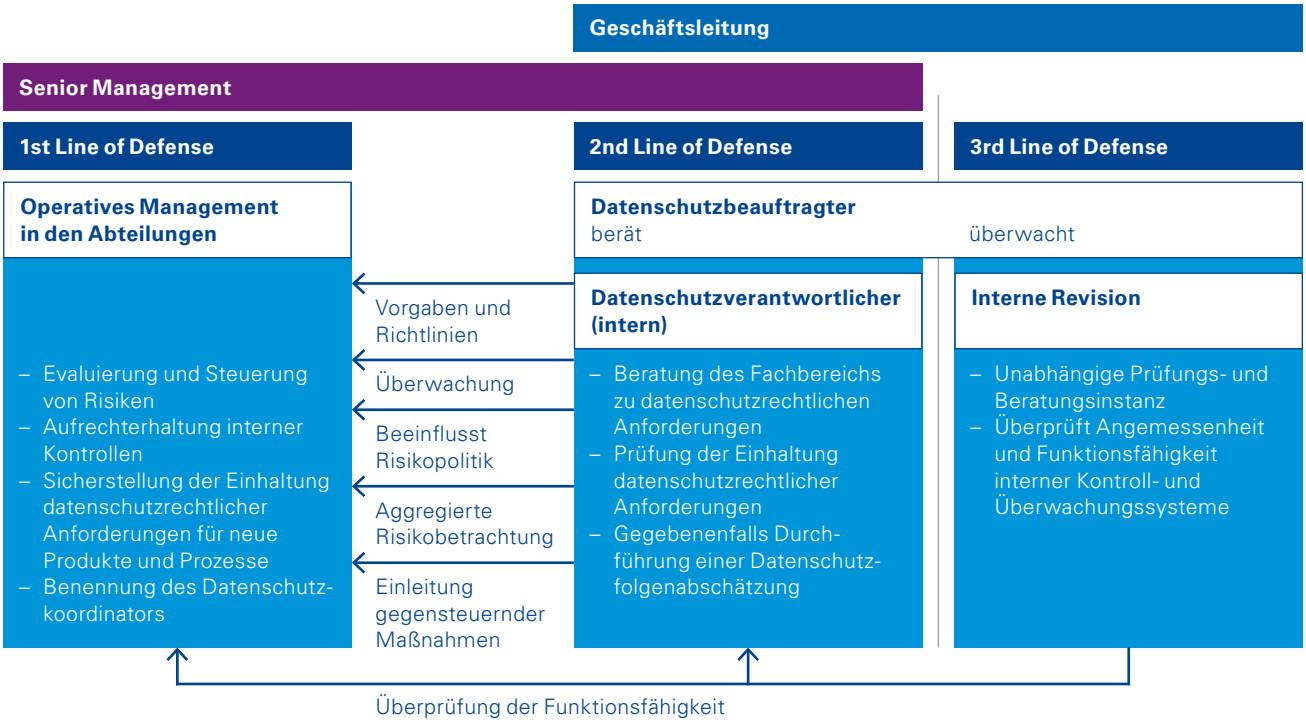
Entsprechend den neuen Risiken steigen nicht nur die Anforderungen an das Management, sondern ebenso die Anforderungen an die Interne Revision, denn sie erfüllt eine wichtige Kontroll- und Transparenzfunktion im Unternehmen. Daher sollte das Thema Datenschutz auch auf der Agenda der Internen Revision stehen, in das Audit Universe einfließen und bei der Prüfungsplanung Berücksichtigung finden. Hierbei sollte nicht nur die Ausgestaltung des Datenschutz-Managementsystems geprüft werden, sondern insbesondere auch die konkrete Umsetzung der Datenschutzmaßnahmen in den Geschäftsprozessen (Abbildung 03).

Um Effektivität und Effizienz der Prüfungstätigkeiten in der Internen Revision zu steigern, ist eine risikoorientierte Prüfungsplanung in den Unternehmen unabdingbar.[3] Die risikoorientierte, im eigenen Ermessen der Internen Revision durchzuführende Planung umfasst das gesamte Prüfumfeld eines Unternehmens, also alle Geschäftsprozesse, und kann anhand folgender Schritte vorgenommen werden:[4]

Identifikation

Es gilt im ersten Schritt die Gesamtheit aller Prüfungsobjekte (Projekte, Prozesse, Gesellschaften) im Audit Universe zu erfassen, um die Existenz revisionsfreier Räume auszuschließen. Die Strukturierung kann sich hierbei auf Organisationseinheiten und Prozesse beziehen und ist in einer Risikomatrix festzuhalten. Ein weiterer Aspekt der Strukturierung sollte die datenschutzrechtlichen Risiken umfassen. Demnach können unter Berücksichtigung der Organisationseinheiten und -prozesse, die mit datenschutzrechtlichen Fragestellungen konfrontiert sind, neue zusätzliche Prüfungsobjekte identifiziert werden. Die Identifikation der Prüfungsobjekte kann beispielsweise auf der Analyse des Verarbeitungsverzeichnisses basieren. Daraus lässt sich zum Beispiel ableiten, in welchen Geschäftsprozessen besonders schutzbedürftige, personenbezogene Daten verarbeitet werden.

03 **Zusammenarbeit zwischen Datenschutzbeauftragtem und Interner Revision – Three Lines of Defense**



Quelle: KPMG in Deutschland, 2019, in Anlehnung an das Three-Lines-of-Defense-Modell (ECIIA und Prof. Dr. Marc Eulerich)

3 DIIR Revisionsstandard Nr. 3, Mindeststandard 4; IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW PS 983), Mindeststandard 4

4 Empfehlung des DIIR „Risikoorientierte Prüfung – Best Practice"

Bewertung

Anhand definierter Kriterien sind je nach Prüfungsobjekt möglichst objektive Risikobewertungen vorzunehmen, zum Beispiel durch Festlegung des Schadensausmaßes. Hierbei müssen nun auch datenschutzrelevante Kriterien wie beispielsweise die Häufigkeit der Verstöße in einer Organisationseinheit, Beschwerden, bereits aufgedeckte Verfehlungen oder Ähnliches als Risikokriterien berücksichtigt werden. Zudem können die Ergebnisse der Risikoanalyse im Rahmen des Datenschutz-Managementsystems (bis hin zur Datenschutzfolgenabschätzung) als Risikokriterien herangezogen werden, um für das Unternehmen und den jeweiligen Geschäftsprozess besonders kritische Verarbeitungen zu identifizieren und zu bewerten.

Priorisierung

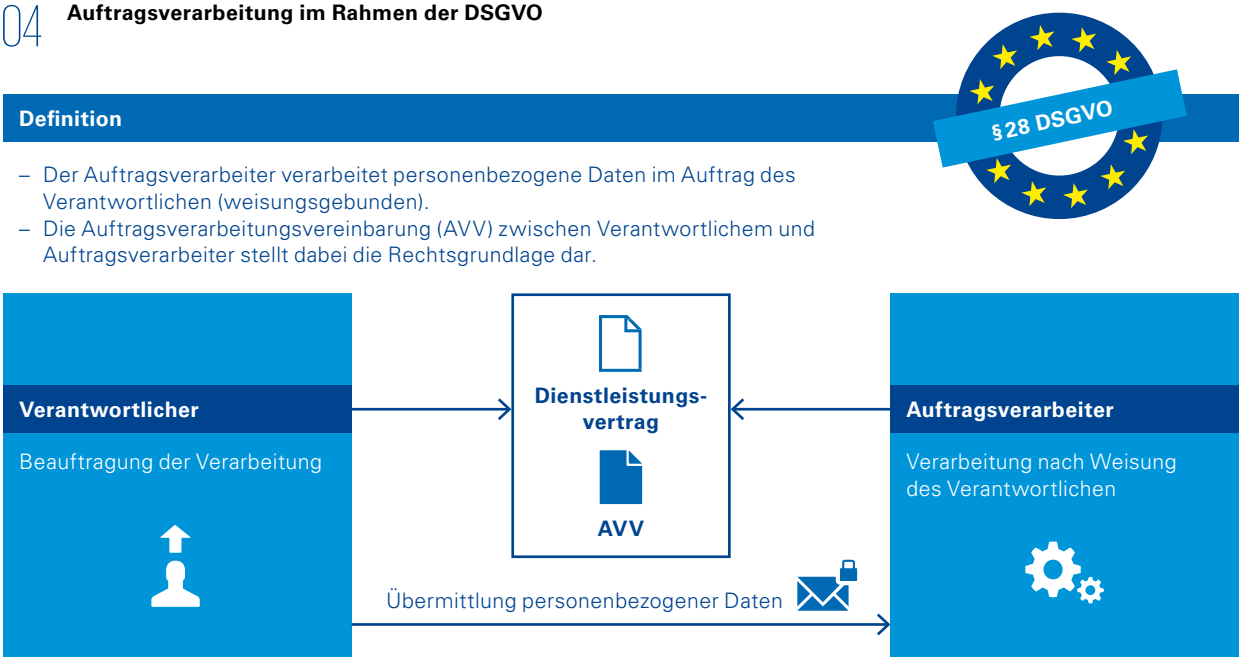
Ziel der Bewertung der Risiken ist eine Priorisierung der Prüfobjekte, um die durchzuführenden Prüfungen risikoorientiert und unter Berücksichtigung der verfügbaren Ressourcen planen zu können. So kann sich die Priorisierung unter Heranziehung der datenschutzrelevanten Bewertungskriterien verschieben und den Prüfungsplan der Internen Revision beeinflussen.

Prüfungsplan

Ergebnis der Priorisierung der Prüfungsobjekte ist der Prüfungsplan (zum Beispiel auf Jahresebene), der nun auch die Datenschutzrisiken berücksichtigt.

Datenschutzrechtliche Aspekte sind nicht nur im eigenen Unternehmen zu beachten. Auch der Aspekt der Auftragsverarbeitung sollte nicht außer Acht gelassen werden (Abbildung 04). Hierbei verarbeitet ein externer Dienstleister für das Unternehmen weisungsgebunden personenbezogene Daten. Die Verantwortung für die ordnungsgemäße Datenverarbeitung obliegt dabei weiterhin dem Unternehmen, das hauptverantwortlich für den Datenschutz bleibt. Der externe Dienstleister wird bei der Auftragsverarbeitung nur unterstützend tätig. Werden dabei Datenschutzverstöße begangen, so sind sie dem auftraggebenden Unternehmen zuzurechnen. Denn die Haftung des Auftragsverarbeiters beschränkt sich auf Verstöße gegen Pflichten, die ihm speziell in seiner Funktion als externem Dienstleister auferlegt sind. Daher sollte die Interne Revision auch mögliche Verstöße solcher Dienstleister bei der Prüfung datenschutzrechtlicher Themen berücksichtigen. Je nach Ergebnis der Bewertung und Priorisierung des Risikos von Verarbeitungsfehlern durch externe Auftragsverarbeiter kann die Interne Revision abwägen, ob sie sie in ihre Prüfung einbezieht.

04 **Auftragsverarbeitung im Rahmen der DSGVO**



Quelle: KPMG in Deutschland, 2019

Berücksichtigung von Datenschutzaspekten im Rahmen von Prozessprüfungen

Das obligatorische Verarbeitungsverzeichnis, das die Datenverarbeitung personenbezogener Daten in sämtlichen Geschäftsbereichen und -prozessen des Unternehmens darstellt, bietet bei Vollständigkeit eine valide Grundlage zur Berücksichtigung neuer datenschutzrelevanter Risiken in der Planung und in den Prüfprogrammen der Internen Revision.

Das Verarbeitungsverzeichnis gewährt der Internen Revision Informationen darüber, welche personenbezogenen Daten je Prozess (beispielsweise Einkauf, Personal) verarbeitet werden. Anhand dieser Informationen kann die Interne Revision die geplanten Prüfungshandlungen auf datenschutzrechtliche Gesichtspunkte ausweiten oder anhand des Verarbeitungsverzeichnisses neue Prüffelder mit hohem Risikopotenzial identifizieren.

Da im Verarbeitungsverzeichnis unter anderem auch aufgeführt wird, wie die Verarbeitung von personenbezogenen Daten stattfinden soll, kann die Interne Revision anhand des Verzeichnisses einen einfachen Abgleich der Soll- und Ist-Situation und der damit verbundenen Datenverarbeitungsschritte in den darunterliegenden Prozessen vornehmen.

Des Weiteren kann die Interne Revision datenschutzrechtliche Aspekte einbeziehen, die sich an den Verarbeitungsgrundsätzen des Artikel 5 DSGVO orientieren. Artikel 5 lit. e DSGVO nennt beispielsweise den Grundsatz der Speicherbegrenzung. Demnach sind Unternehmen verpflichtet, personenbezogene Daten zu löschen, wenn sie nicht mehr erforderlich sind und keine gesetzlichen Aufbewahrungspflichten bestehen. Denn die DSGVO sieht klare Löschpflichten vor (unter anderem in Artikel 17 DSGVO „Recht auf Vergessenwerden“).

Die Prüfungshandlung der Internen Revision kann auch in der Überprüfung des prozessspezifischen Löschkonzepts selbst bestehen und kontrollieren, ob es richtig angewandt wurde. Fragestellungen, mit der sich die Interne Revision typischerweise beschäftigen wird, sind:

- Welche Datenart wurde verarbeitet? Beispiele für eine Datenart sind Stammdaten (Mitarbeiter, Kunden, Lieferanten), Vertragsdaten, Abrechnungsdaten, Buchhaltungsdaten (zum Beispiel Buchungsbelege, Zahlungsläufe) etc.

- Wo befinden sich die personenbezogenen Daten, wer hat Zugriff und an wen werden sie weitergegeben?

- Wann sind gemäß den gesetzlichen Vorgaben Daten zu löschen?

- Welche Löschfristen sind für die einzelnen Datenarten, unter Berücksichtigung der vertraglichen und rechtlichen Aufbewahrungsfristen, implementiert?

Des Weiteren muss die Verarbeitung von personenbezogenen Daten durch technische und organisatorische Maßnahmen (TOM) geschützt werden. Die DSGVO verpflichtet Unternehmen in Artikel 32 dazu, „geeignete technische und organisatorische Maßnahmen [zu treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“[5] (Abbildung 05):

05 **Schutzziele für die Verarbeitung von personenbezogenen Daten**

Quelle: KPMG in Deutschland, 2019

Daher sollte die Interne Revision auch die Einhaltung und die Existenz der technischen und organisatorischen Maßnahmen im Unternehmen und innerhalb eines jeden zu prüfenden Prozesses überwachen und ihre Kontrolle als festen Bestandteil in die Prüfung inkludieren.

Ein Beispiel für eine solche Prozessprüfung könnte im Personalwesen der Prozess des Bewerbermanagements sein. Hier kann die Interne Revision sich an folgenden beispielhaften Prüfungsfragen orientieren:

- Wie werden die Daten erhoben und verarbeitet (wird beispielsweise ein Bewerbermanagement-Tool eingesetzt)?

- Ist das Berechtigungskonzept der genutzten Tools und Systeme angemessen?
  - Wie sehen die Zugriffsrechte von Mitarbeitern auf das System, inklusive der Lese- und Schreibrechte, sowie die Systemmodule aus?
  - Ist das Berechtigungskonzept angemessen hinsichtlich des Need-to-Know-Prinzips?

- Welchen Personen werden die Daten offengelegt und wie sind die Daten vor unberechtigtem Zugriff geschützt?
  - Sind geeignete TOMs implementiert und ordnungsgemäß dokumentiert?
  - Wie sehen die Sicherungsmaßnahmen hinsichtlich unberechtigter Zugriffe auf ausgedruckte Daten, Daten auf Speichermedien oder Daten, die zur Vernichtung bereitgestellt werden, aus?

- Gibt es eine Information an den Bewerber über die Verarbeitung personenbezogener Daten (vergleiche hierzu Informationspflichten nach Artikel 12 bis 14 EU-DSGVO)?

- Werden die Daten gemäß den Aufbewahrungsfristen gelöscht und wie ist die Löschung organisiert?
  - Sind spezifische Lösch- und Sperrkonzepte je Verarbeitungstätigkeit vorhanden, die den Grundsätzen der Zweckbindung, Datenminimierung und Speicherbegrenzung entsprechen?
  - Soweit sich Zweckänderungen ergeben, werden die Löschkonzeptionen entsprechend überprüft?
  - Wird die Einschätzung der Aufbewahrungsfristen sowie der Lösch- und Sperrfristen regelmäßig aktualisiert?

- Ist der Verarbeitungsprozess gemäß den gesetzlichen Vorgaben korrekt im Verzeichnis der Verarbeitungstätigkeiten abgebildet?

- Wenn Auftragsverarbeiter eingesetzt werden, ist mit ihnen eine entsprechende Vereinbarung getroffen, die die gesetzlichen Vorgaben erfüllt?

5 DIIR-Arbeitskreis Interne Revision & Datenschutz, Leitfaden Interne Revision und Datenschutz, veröffentlicht im Oktober 2017 auf www.diir.de

Prüfung des Datenschutz-Management-systems durch die Interne Revision

Nach Artikel 5 Abs. 2 der DSGVO müssen Unternehmen über die Einhaltung der Datenverarbeitungsgrundsätze Rechenschaft ablegen. Das legt die Einführung eines Datenschutz-Managementsystems nahe, das die Einhaltung der Schutzziele der DSGVO (zum Beispiel Artikel 25 und 32) gewährleistet. Somit muss die Interne Revision nicht nur im Rahmen von Prozessprüfungen überwachen, ob die Anforderungen der EU-DSGVO umgesetzt werden, sie muss auch das Datenschutz-Managementsystem an sich in regelmäßigen Abständen überprüfen und entsprechende Kontrollen in der Prüfungsplanung berücksichtigen.

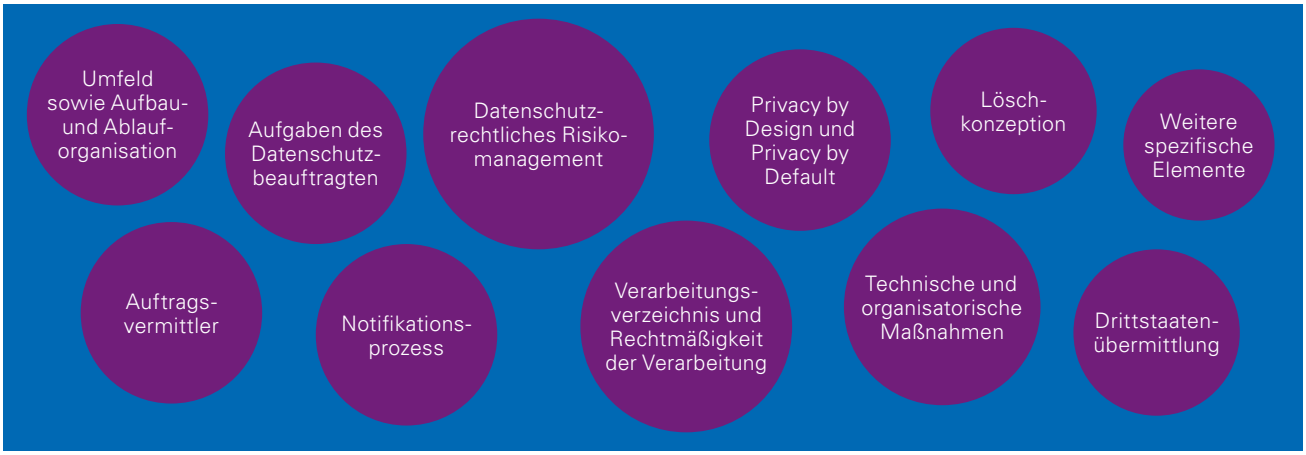
Im Mittelpunkt einer Prüfung des Datenschutz-Managementsystems durch die Interne Revision sollten die zentral implementierten Prozesse und Richtlinien stehen.

Bei der Erstellung des Prüfprogramms kann zur Orientierung die vom DIIR – Deutsches Institut für Interne Revision e. V. (DIIR) herausgegebene „Checkliste zur Prüfung der Datenschutzorganisation“[6] herangezogen werden.

Hierbei wird auf folgende Prüfungsschwerpunkte eingegangen:
- Datenschutzstrategie
- Vorgaben und Anforderungen
- Organisation
- Kommunikation und Prozesse
- Reporting

Zusätzlich zu der bereits erwähnten DIIR-Checkliste kann der Prüfungshinweis IDW PH 9.860.1 „Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz“[7] als weitere Grundlage herangezogen werden. Der Leitfaden schlägt Prüfungshandlungen für Grundsätze, Verfahren und Maßnahmen eines Unternehmens vor, die auf die Einhaltung der Anforderungen der DSGVO und des BDSG bei der Verarbeitung personenbezogener Daten gerichtet sind. Abbildung 06 zeigt dazu einen Überblick, auf welche Prüfungselemente der IDW PH 9.860.1 hierbei besonders eingeht.

06 **Prüfungselemente des IDW PH 9.860.1**



Quelle: KPMG in Deutschland, 2019

6 DIIR-Arbeitskreis Interne Revision & Datenschutz, Checkliste zur Prüfung der Datenschutzorganisation, veröffentlicht im Oktober 2017 auf www.diir.de
7 Fachausschuss für Informationstechnologie (FAIT), Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz, verabschiedet am 17.05.2018, billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 19.06.2018, veröffentlicht im IDW-Life-Heft 8/2018

Für jedes der Prüfungselemente werden beispielhaft Prüfungshandlungen aufgezeigt, anhand derer ein Datenschutz-Managementsystem geprüft werden kann. Jedoch ist zu beachten, dass diese Beispiele nur ergänzend zu den Anforderungen des IDW PS 980 sowie IDW PS 860 gelten (Abbildung 07).

Bei der Prüfung eines Datenschutz-Managementsystems kann sich die Interne Revision an folgenden beispielhaften Prüfungsfragen orientieren:

- Wurden Datenschutzziele festgelegt, die sich nachvollziehbar aus der Unternehmensstrategie ableiten, besondere datenschutzrechtliche Faktoren berücksichtigen, die sich aus dem Geschäftsmodell ergeben, und die dokumentiert sind?

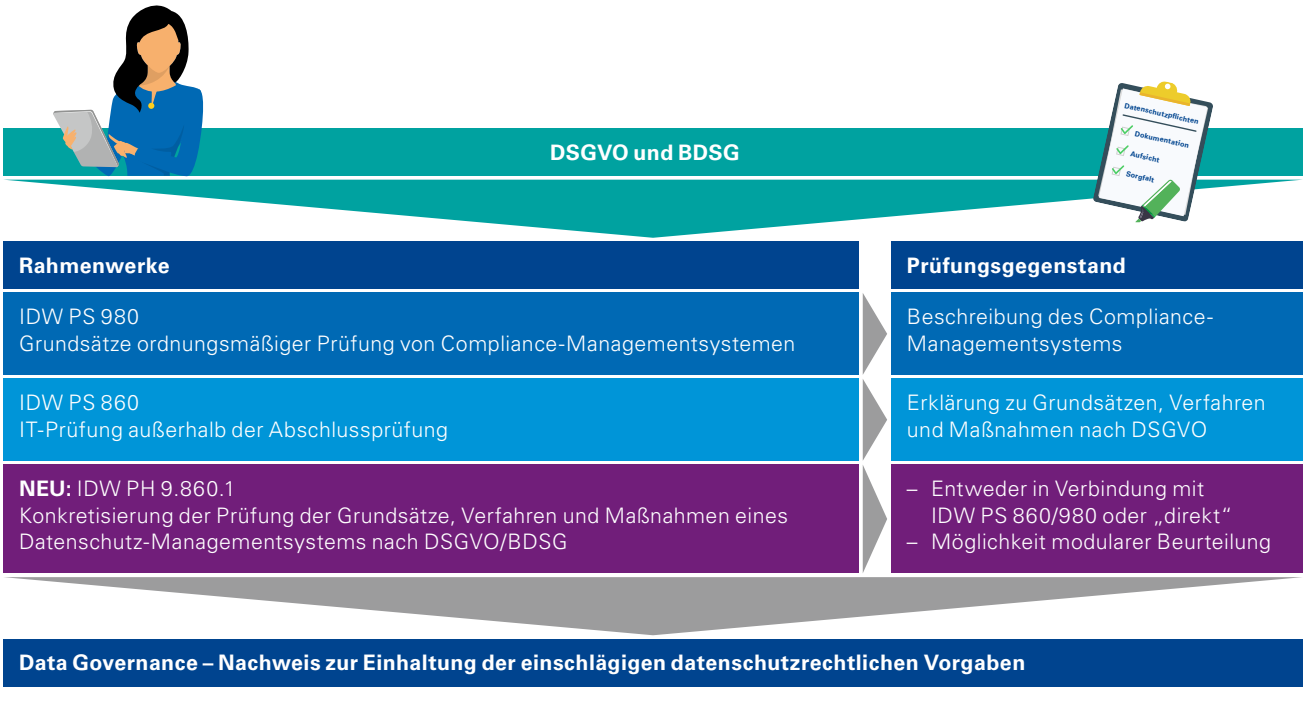
- Existiert eine Datenschutzorganisation, die Rollen und Verantwortlichkeiten klar festlegt?

- Sind Richtlinien und Anweisungen zum Datenschutz vorhanden, die die gesetzlichen und unternehmensinternen Anforderungen berücksichtigen?

- Ist ein Prozess implementiert, wie das Verzeichnis der Verarbeitungstätigkeiten zu erstellen und in welchen Abständen es zu überprüfen ist?

- Gibt es ein schriftlich dokumentiertes und geeignetes Löschkonzept und ist es implementiert?
  - Existiert eine übergreifende Richtlinie zur Löschung und Sperrung personenbezogener Daten?
  - Wurden bei der Erstellung der anwendungsbezogenen Löschkonzepte die IT-Abteilung und die Fachbereiche eingebunden?

07 **Rahmenwerke für Datenschutz-Audits**



Quelle: KPMG in Deutschland, 2019

Unsere Leistungen

KPMG steht Ihnen bei allen Fragen rund um die Prüfung von Datenschutz-Managementsystemen und Unternehmensprozessen mit umfangreicher Erfahrung aus zahlreichen Projekten und breitem Know-how zur Seite.

Auf Basis einer projektbegleitenden Prüfung in Form eines Readiness-Checks bewerten wir den Umsetzungsstand des Datenschutz-Managementsystems und unterstützen bei der Identifikation noch umzusetzender Handlungsfelder oder Kerndatenschutzprozesse, damit Sie für eine nachgelagerte Revisionsprüfung gewappnet sind.

Bei bereits implementierten Datenschutz-Managementsystemen führen wir Prüfungen der Internen Revision durch. Hierbei verifizieren wir unter anderem, ob alle datenschutzrechtlichen Vorgaben und Datenschutzanforderungen erfüllt werden. So sind Sie für eine mögliche nachgelagerte Prüfung (zum Beispiel IDW PS 980, IDW PS 860 mit IDW PH 9.860.1) durch unsere Experten gut gerüstet. Aufgrund der Wichtigkeit des Datenschutzes im Unternehmen und der damit einhergehenden Risiken, empfehlen wir alle zwei bis drei Jahre eine Berücksichtigung der Prüfung der Datenschutzorganisation in der Revisionsplanung und unterstützen Sie gerne bei der Planung und Durchführung.

Darüber hinaus beraten beziehungsweise unterstützen wir die Interne Revision
- in allen Fragestellungen zur Prüfung eines Datenschutz-Managementsystems,
- zur Re-Organisation der Revisionsfunktion, um den datenschutzrechtlichen Anforderungen zu genügen,
- bei der Erstellung von Prüfprogrammen, inklusive der Berücksichtigung von datenschutzrechtlichen Prüfungsfragen,
- bei der Durchführung von Prüfungen im Rahmen von Cosourcing- und Outsourcing-Projekten,
- durch Schulungen der internen Revisoren, zum Beispiel zum Thema:
  - Revisionsprüfungen zum Datenschutz-Managementsystem oder von Teilbereichen,
  - Datenschutz und welche Besonderheiten von den Revisoren bei Prüfungen zu berücksichtigen sind.

Bestens für Sie aufgestellt

Der Bereich Internal Audit arbeitet eng mit Branchen- und IT-Experten zusammen. Wir verfügen über umfassende Erfahrung und Praxisorientierung auf dem Gebiet der Prüfung von Datenschutz-Managementsystemen sowie -prozessen und sind mit datenschutzrechtlichen Fragestellungen sowie allen regulatorischen Anforderungen und Standards vertraut. Unsere Spezialisten stehen Ihnen deutschlandweit zur Verfügung. Zudem können wir aufgrund unserer Einbindung in das weltweite KPMG-Netzwerk auf das Know-how weiterer Experten zurückgreifen, die bei internationalen Fragestellungen und Sachverhalten kompetent unterstützen. So profitieren Sie von unserem profunden Verständnis für Märkte, Branchen und Unternehmen.

Gerne stehen wir für Ihre Fragen oder ein erstes Gespräch zur Verfügung. Sprechen Sie uns an.

Kontakt

KPMG AG Wirtschaftsprüfungsgesellschaft
Ganghoferstraße 29
80339 München

Albina Kladusak
Partner, Governance & Assurance Services
T +49 89 9282-3157
akladusak@kpmg.com

Oliver Schnell
Senior Manager, Governance & Assurance Services
T +49 40 32015-5104
oschnell@kpmg.com

Timo Herold
Senior Manager, Governance & Assurance Services
T +49 711 9060-41928
timoherold@kpmg.com

Monika Antoni
Manager, Governance & Assurance Services
T +49 89 9282-1665
mantoni@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia