

Reicht eine Abarbeitung von Checklisten aus?

Orientierungshilfe



Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

Werden Sie Teil unseres starken Netzwerks!



Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

Ihre Vorteile:

- Erfahrungsaustausch in bundesweit 12 Regionalgruppen
- 9 BvD-Arbeitskreise zu Fachthemen
- Kongresse und Workshops mit namhaften Referenten
- anerkannte Weiterbildungsmodulare zum Nachweis der Fachkunde
- Listung im Verzeichnis der externen Datenschutzbeauftragten
- Arbeitshilfen & Materialien für den Berufsalltag
- Fachmagazin BvD-News
- Politischer Dialog in Gesetzgebungsverfahren
- Rabatte & Vergünstigungen bei zahlreichen Kooperationspartnern

Seit über 30 Jahren vernetzt der BvD Politik, Wirtschaft, Aufsichtsbehörden und Datenschutzbeauftragte – auf regionaler, nationaler und europäischer Ebene. Wir fördern die beruflichen Interessen unserer fast 2.000 Mitglieder und setzen uns aktiv für die weitere Akzeptanz des Berufsbildes „Datenschutzbeauftragter“ ein – als einziger Verband in Deutschland.

Wir bieten Mitgliedschaften für interne und externe Datenschutzbeauftragte sowie für Unternehmen an.

Jetzt beitreten unter:
www.bvdnet.de/mitgliedschaft

BVD-AUSSCHUSS „PRÜFAUFGABEN DES DATENSCHUTZBEAUFTRAGTEN“

Der Datenschutzbeauftragte hat neben vielen anderen Aufgaben vor allem die Prüfaufgabe und deren Dokumentation in Richtung der Unternehmens- bzw. Behördenleitung zu gewährleisten. Der Ausschuss befasst sich mit der Planung, dem Ablauf und der Dokumen-

tation der Prüfungen des benannten Datenschutzbeauftragten. Ganz pragmatisch geht es um das How-to und die dazu erforderlichen Dokumente, die der BvD als Berufsverband empfiehlt.

IMPRESSUM:

Herausgeber:

Berufsverband der Datenschutz-
beauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Tel: 030 26 36 77 60
Fax: 030 26 36 77 63
E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de



[www.xing.com/companies/
berufsverbandderdatenschutz
beauftragtendeutschlands](http://www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands)



www.twitter.com/bvd_datenschutz



www.bvdnet.de/feed/

Diese Umfrage wurde unter
der Mitwirkung von

Christian Nawroth

Stephan Rehfeld

Michael Weinmann

erstellt und ausgewertet.

Der Nachdruck und die Vervielfältigung
sind nur mit schriftlicher Genehmigung des
BvD e.V. zulässig.

DIE PRÜFAUFGABEN DES DATENSCHUTZBEAUFTRAGTEN NACH DSGVO

Reicht eine Abarbeitung von Checklisten aus?

Christian Nawroth, Patrick Grihn

Mit Einführung der Datenschutz-Grundverordnung (DSGVO) hat sich das Anforderungsprofil an Datenschutzbeauftragte (DSB) und den für die Verarbeitung von personenbezogenen Daten Verantwortlichen verändert. Gemäß Artikel 39 „obliegen dem Datenschutzbeauftragten...

- Unterrichtung und Beratung des Verantwortlichen, Auftragsverarbeiter und der Beschäftigten...
- Überwachung der Einhaltung dieser Verordnung...
- Überprüfung der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter,
- Beratung ... im Zusammenhang mit der Datenschutz-Folgeabschätzung und Überwachung ihrer Durchführung...
- Zusammenarbeit mit den Aufsichtsbehörden...“

Außerdem wird dem Datenschutzbeauftragten die Pflicht zur risikoorientierten Tätigkeit auferlegt.

Im Gegensatz dazu hat der Verantwortliche nach der DSGVO sicherzustellen, dass die Einhaltung der Datenschutz-Grundverordnung gewährleistet ist, und er muss dies auch nachweisen können. Darüber hinaus hat der Verantwortliche diese Sicherstellung zu kontrollieren. Wie eingangs schon erwähnt, berät der Datenschutzbeauftragte den Verantwortlichen bei all diesen Tätigkeiten, sofern der Verantwortliche einen solchen benannt hat.

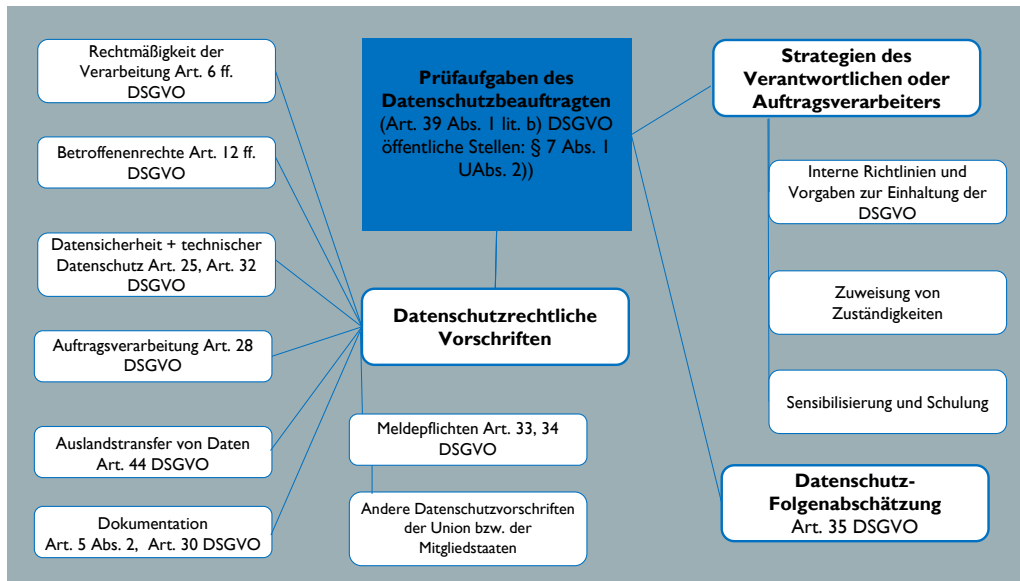
Nachfolgend wollen wir uns diese Anforderungen aus der DSGVO näher ansehen und aufzeigen, welche Auswirkungen diese Anforderungen auf die Arbeit des Datenschutzbeauftragten haben, insbesondere auf Kontrollen und Überprüfungen. Darüber hinaus wollen wir erste Hilfestellungen geben, welche Möglichkeiten sich dadurch auch für den DSB ergeben können.

Prüfaufgaben DSB - Regelmäßige Kontrollen

Für Datenschutzbeauftragte ergeben sich eine Reihe von Prüfaufgaben auf der Basis von gesetzlichen Anforderungen. Diese ergeben sich vor allem aus Art. 39 Abs. 1 lit. b. DSGVO und § 7 Abs. 1 Nr. 2 BDSG.

Zudem berät der Datenschutzbeauftragte den Verantwortlichen, die Auftragsverarbeiter und die Beschäftigten (Art. 39 Abs. 1 lit. a). Um dieser Beratungsverpflichtung nachkommen zu können ist es wichtig zu wissen, dass dem Verantwortlichen durch die DSGVO zusätzliche Prüfpflichten auferlegt werden. Diese ergeben sich aus den Grundsätzen für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. a.-f.) und der Nachweispflicht, für deren Einhaltung diese auch nachzuweisen sind (Art. 5 Abs. 2 und Art. 24 Abs. 1). Außerdem wird dem Verantwortlichen die Pflicht auferlegt, Maßnahmen zu ergreifen und diese Maßnahmen „erforderlichenfalls zu überprüfen und zu aktualisieren“ (Art. 24 Abs. 1). Eine weitere Prüfanforderung stellt der Art. 32 Abs. 1 lit. d an Verantwortliche, die auch für den Auftragsverarbeiter gilt (Art. 28 Abs. 3 lit. c). Es soll „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ etabliert werden. Warum sind diese Anforderungen an den Verantwortlichen und Auftragsbearbeiter auch wichtig für den Datenschutzbeauftragten?

Im Erwägungsgrund 97 wird der Datenschutzbeauftragte als eine Person beschrieben, die den Verantwortlichen oder den Auftragsverarbeiter „bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung“ mit seinem „Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren“ unterstützten soll. Darüber hinaus gibt es noch eine Reihe von weiteren Prüfanforderungen, bei der ein Datenschutzbeauftragter selbst tätig wird oder beratend unterstützt. Wir



Übersicht der Prüfaufgaben des DSB (© AK Prüfaufgaben des BvD)

können festhalten, es gibt neben der generischen Forderung aus Art. 39 die Einhaltung der DSGVO zu überwachen, keine weitere inhaltliche oder operative Anforderung an den DSB. Leider geht die DSGVO oder das Bundesdatenschutzgesetz nicht weiter darauf ein, wie Datenschutzbeauftragte diese doch sehr unspezifisch gehaltenen Prüfanforderungen explizit operativ umsetzen sollen. Wesentlich konkreter wird die DSGVO da schon bei den Verantwortlichen und Auftragsverarbeitern. In den nachfolgenden Artikeln (Art.) und Erwägungsgründen (ErwG) werden teilweise sehr dedizierte Maßnahmen benannt, die eine regelmäßige Überprüfung nach Wirksamkeit der etablierten Prozesse fordern.

- Art. 24 DSGVO – Verantwortung des für die Verarbeitung Verantwortlichen
- Art. 25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art. 32 DSGVO – Sicherheit der Verarbeitung
- ErwG 76 DSGVO – Risikobewertung
- ErwG 78 DSGVO – Geeignete technische und organisatorische Maßnahmen
- ErwG 79 DSGVO – Zuteilung der Verantwortlichkeiten
- ErwG 83 DSGVO – Sicherheit der Verarbeitung

Nicht zuletzt sei noch erwähnt, dass sich die Etablierung von geeigneten Prüfverfahren auch auf

die Bemessung von Bußgeldern auswirkt. Gemäß Art. 83 Abs. 2 lit. d ist der Grad der Verantwortung davon abhängig, welche Maßnahmen gemäß Art. 25 und 32 der Verantwortliche getroffen hat. Hierfür müssen Verarbeiter Nachweise erbringen. Ganz konkret wird gemäß Art. 32 Abs. 1 lit. d ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit gefordert.

So fordert das berufliche Leitbild des BvD e. V., welchem sich seine Mitglieder unterwerfen, dass der Datenschutzbeauftragte regelmäßige Kontrollen durchführt und sich hierbei an die Vorgaben der DSGVO sowie an angrenzende etablierte Managementsysteme hält. Hierbei werden gängige Zyklen wie der PDCA implizit angeführt und auf die o. g. Grundsätze referenziert.

Insbesondere die vielfältigen Aufgaben- und Prüfbereiche des Datenschutzbeauftragten erfordern ein strukturiertes Management der jeweiligen Segmente (vgl. 2.2. Berufliches Leitbild der Datenschutzbeauftragten, 4. Auflage). So werden die offensichtlichen Bereiche ebenso angeführt wie eine strukturierte Kommunikation mit der Aufsichtsbehörde sowie die regelmäßige systematische Überwachung und Verbesserung des Schulungskonzepts.

Durchführung von Kontrollen – Systemischer Ansatz

Auch wenn in den Gesetzestexten nicht explizit

beschrieben ist, welche spezifischen Prüfaufgaben den Datenschutzbeauftragten auferlegt werden und was im Detail überprüft bzw. kontrolliert werden muss, damit die Anforderungen aus der DSGVO eingehalten werden, lässt sich doch aus der Datenschutz-Grundverordnung ableiten, welche Anforderungen sich an die Überwachungsaufgaben des DSB ergeben, insbesondere auch durch die Aufgaben des Verantwortlichen und des Auftragsverarbeiters, da deren regelmäßige Überprüfungen Teil der Überwachungsaufgabe der Datenschutzbeauftragten sein können.

Zusammenfassend ergeben sich fünf allgemeine Anforderungen an die Prüfaufgaben eines Datenschutzbeauftragten:

1. Es muss ein Verfahren etabliert werden. Verfahren bedeutet geregelt, in Verfahrensschritte zerlegbar, nachvollziehbar und hat einen „wiederholbaren Ablauf“.¹

2. Diese Verfahren müssen regelmäßig durchgeführt werden. Eine einmalige Überprüfung ist also nicht ausreichend.

3. Es muss in Form einer Überprüfung stattfinden. Mit Überprüfung ist gemeint, dass eine Untersuchung/Analyse durchgeführt wird, die prüft, ob Anforderungen erfüllt sind. In diesem Fall, ob die gesetzlichen Anforderungen eingehalten sind.

4. Es muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden. Hierunter ist neben einer vollständigen Umsetzung der Maßnahmen auch deren mittel- und langfristige Auswirkung zu bewerten, da nicht jede Maßnahme sofort Wirkung zeigt. Außerdem muss die Maßnahme bewertet werden. Mit Evaluierung ist eine sach- und fachgerechte Untersuchung/Bewertung gemeint.²

5. Es muss ein risikobasierter Ansatz adressiert werden. Bei den Prüfaufgaben ist sicherzustellen, dass die eingerichteten Kontrollen zur Vermeidung von Risiken in allen Bereichen einer Organisation adäquat berücksichtigt und entsprechend etabliert wurden.³

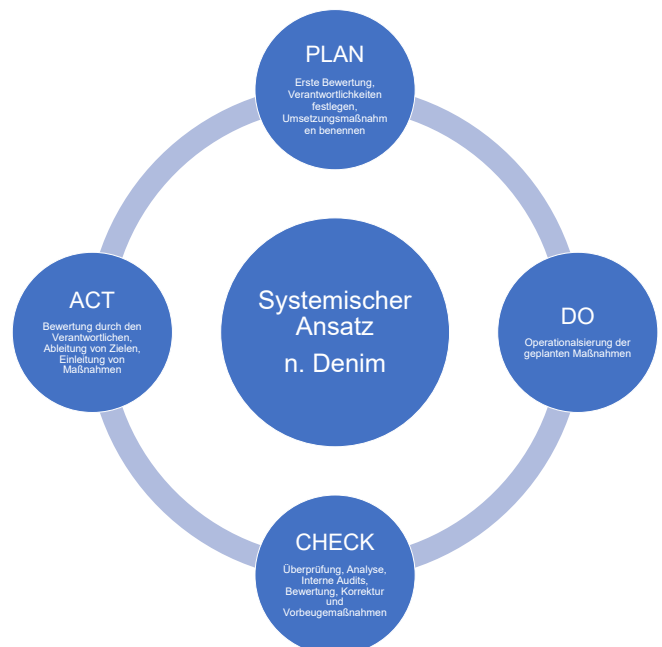
Die größte Herausforderung bei der Umsetzung dieser fünf Anforderungen stellt zweifelsfrei der Punkt 3 dar. Bei den zu überprüfenden Anforderungen handelt es sich nicht um eine Norm mit festgelegten Controls, sondern um gesetzliche Anforderungen. Gesetzliche Anforderungen sind aber von

Rechtsprechungen abhängig und diese beeinflussen möglicherweise die Validierungsregeln⁴. Das bedeutet für den Datenschutzbeauftragten, dass sich Anforderungen gegebenenfalls im Laufe der Zeit ändern können und er die aktuelle Rechtsprechung im Auge behalten muss.

Generell ergeben sich unterschiedliche Ansätze, wie man die Einhaltung von Anforderungen überwachen kann. Neben dem klassischen Kontrollieren durch das Beobachten, Messen und Befragen mittels Checkliste, Anforderungskatalog oder Inspektionen und Überprüfungen von Aufzeichnungen, kann man Monitoringsysteme etablieren. Darüber hinaus können Tests und Analysen durchgeführt werden. Letztendlich dienen alle genannten Maßnahmen nur der Überprüfung der Anforderungen. Eine Bewertung der Wirksamkeit der Maßnahmen hat damit noch nicht stattgefunden.

Deshalb kann es für den Datenschutzbeauftragten sehr hilfreich sein sich mit systemischen Ansätzen zu beschäftigen, wie man in einer strukturierten Vorgehensweise Anforderungen validiert und wie man konkret die Wirksamkeit von Maßnahmen überprüft. Denn wenn man die Wirksamkeit von Maßnahmen überprüfen will, wird einem schnell klar, dass es sich nicht um eine einmalige Überprüfung handeln kann. Denn Maßnahmen, Verfahren, Prozesse entwickeln sich weiter. Diese Weiterentwicklung kann positiv, aber auch negativ sein. Es ist nicht ausreichend Prozesse zu etablieren, sondern die etablierten Prozesse müssen gelebt werden!

Auch für den Verantwortlichen und Auftragsverarbeiter stellt sich die Frage nach der Wirksamkeit und damit auch für den DSB als Beratenden.



¹ „Wikipedia: Verfahren“, <https://de.wikipedia.org/wiki/Verfahren>, 07.06.2021

² „Wikipedia: Evaluation“, <https://de.wikipedia.org/wiki/Evaluation>, 07.06.2021

³ ISACA: „Audit and Assurance - How to audit GDPR“, 2018, Seite 6.

⁴ ISACA: „Audit and Assurance - How to audit GDPR“, 2018, Seite 5.

Für eine nachhaltige Etablierung des Datenschutzes wird optimalerweise ein systemischer Ansatz („under control“) gewählt. Diese Kombination setzt man mit einem Datenschutz-Managementsystem um. Denn nur mit einem Datenschutz-Managementsystem ist man in der Lage der Einhaltung von gesetzlichen Anforderungen adäquat gerecht zu werden.

Optimalerweise wird der Datenschutz in die vorhandenen Prozesse des Verantwortlichen integriert. Als wirksames Instrument hat sich hier der kontinuierliche Verbesserungsprozess nach Deming etabliert. Dieses Verfahren bildet die Basis für alle Managementsysteme der ISO/IEC-Normen und gewährleistet durch den Ansatz der kontinuierlichen Verbesserung auch eine langfristige Bewertung der Wirksamkeit.

Systemischer Ansatz nach Deming

Für die Überprüfung von Datenschutzmanagementsystemen (DSMS) ist ebenfalls eine systemische Vorgehensweise zu empfehlen. Für die Untersuchung von Prozessen, Richtlinien, Anforderungen hat sich die Durchführung von Audits als erprobte, praktische Maßnahme etabliert. Nachfolgende Standards der Internationalen Organisation für Normung (ISO), dem globalen Berufsverband für IT-Revisionen, Wirtschaftsprüfer sowie Experten der Informationssicherheit und IT-Governance (ISACA) und dem Institut der Wirtschaftsprüfer in Deutschland (IDW) können als Leitfaden für die Durchführung von Audits dienen. Im Detail geht es um die Standards:

- **ISO 19011** – Leitfaden zur Auditierung von Managementsystemen
- **ISACA – Auditing-Standards – Auditing-Guidelines – Auditing-Procedures & Code of Professional Ethics** General (1000 series) - Performance (1200 series) - Reporting (1400 series)
- **IDW PS 860** – Prüfungsstandard für alle Sonderprüfungen im IT-Umfeld

Alle anderen genannten Standards legen Prinzipien für die Durchführung der Prüfung/Audits fest. Diese Prinzipien sind die Grundlage für die Audits und müssen natürlich vom Auditor eingehalten werden.

DIN EN ISO 19011	ISACA-IT-Prüfungsstandard	Prüfungsstandard IDW PS 860
<ul style="list-style-type: none"> • Integrität • Sachliche Darstellung • Angemessene berufliche Sorgfaltspflicht • Vertraulichkeit • Unabhängigkeit • Faktenbasierter Ansatz (Vorgehensweise, die auf Nachweisen beruht) • Risikobasierter Ansatz 	<ul style="list-style-type: none"> • Formale Beauftragung • Unabhängigkeit • Rechtschaffenheit & Vertraulichkeit • Fachkompetenz • Nachweis & Nachvollziehbarkeit • Objektivität & Sorgfalt • Sachliche Darstellung 	<ul style="list-style-type: none"> • Relevanz • Vollständigkeit • Verlässlichkeit • Neutralität • Verständlichkeit <p>Ergänzende berufliche Grundsätze der Wirtschaftsprüfer:</p> <ul style="list-style-type: none"> • Unabhängigkeit, Unparteilichkeit und Vermeidung der Besorgnis der Befangenen • Gewissenhaftigkeit einschl. beruflicher Kompetenz und der berufstüblichen Sorgfalt • Verschwiegenheit • Eigenverantwortlichkeit • Berufswürdiges Verhalten, einschließlich Verantwortung gegenüber dem Berufsstand

Kriterien der Durchführung von Audits

Darüber hinaus gibt es Kriterien an den Auditor selbst. Zusammenfassend sollten Auditoren, die Datenschutzprüfaufgaben wahrnehmen, befähigt sein, Audits durchzuführen. Kranig/Sachs/Gierschmann nennen in „Datenschutzcompliance nach DS-GVO“ zusammenfassend die nachfolgenden Anforderungen:⁵

- Fach- und Methodenwissen besitzen
- Soziale Kompetenz haben
- Von den Auditierten als Kompetenz akzeptiert werden
- Sachliche, zielgerichtete und objektive Arbeitsweise haben
- Standhafte Konfliktfähigkeit haben
- Rechtliche Kenntnisse besitzen
- Kenntnisse in der Informationssicherheit haben
- Tiefgreifende Kenntnisse des technischen Datenschutzes haben
- Bei Cloud-Architekturen ein vertieftes Wissen zum internationalen Datentransfer und cloudspezifischer Bedrohungslagen haben

Als BluePrint für die Durchführung von Audits kann die ISO 19011 gut herangezogen werden. Sie beschreibt und regelt das Thema Audits in Form eines „Leitfadens zur Auditierung von Managementsystemen“⁶. Neben der Steuerung eines Auditprogramms wird die Durchführung von Audits sowie die Kompetenz und Bewertung von Audi-

⁵ Kranig, Sachs, Gierschmann: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2017, S.148

⁶ „ISO 19011“, https://de.wikipedia.org/wiki/ISO_19011, 15.06.2021

toren geregelt. Außerdem gibt es im Anhang A eine Anleitung für Auditoren zum Planen und Durchführen von Audits (informativ). Dort wird in 18 Unterkapiteln ausführlich operative Hilfestellung gegeben.⁷ Diese Norm kann dem Datenschutzbeauftragten als allgemeine Grundlage dienen, wie er seine Prüfaufgaben organisiert und welche Rahmenparameter er wählt, um seine Audits in einer strukturierten Form ablaufen zu lassen. Da die ISO 19011 ein allgemeiner Standard für die Durchführung von Audits ist, bietet sie dem Datenschutzbeauftragten keine inhaltliche Hilfe an, was die Datenschutz-Grundverordnung und das BDSG in Bezug auf die Einhaltung des Datenschutzes explizit fordert.

Speziell für die Prüfung der Organisation des Datenschutzes hat sich mit „IDW PH 9.860.1 für Prüfungen nach der DSGVO und dem BDSG“ ein dediziertes Rahmenwerk etabliert. Hier wird neben dem Umfeld die Aufbauorganisation und die Ablauforganisation auditiert. Im Detail sind das die Bereiche:

- Tätigkeit des DSB
- Risikomanagement
- Rechtmäßigkeit der Verarbeitung
- Verzeichnis der Verarbeitungstätigkeiten
- Privacy by Design / Privacy by Default
- Übermittlung in Drittländer
- Auftragsverarbeitung
- Datenschutzverletzung
- Betroffenenrechte
- Löschmanagement
- Sicherheit der Verarbeitung

Als Alternative dazu kann auch das Audit-Programm der ISACA (GDPR – Audit) hilfreich sein. Es basiert auf Durchführungskontrollen (Implementation Controls) und Erhaltungskontrollen (Maintenance Controls).⁸ Im Audit werden 9 Datenschutzcluster (DPP) untersucht.⁹

- DPP1 - Betreiben eines Datenschutz-Management-System
- DPP2 - Erfassen, Identifizieren und Klassifizieren persönlicher Daten
- DPP3 - Umgang mit Datenschutz Risiken
- DPP4 - Umgang mit Datensicherheit
- DPP5 - Lieferketten und Auftragsverarbeiter
- DPP6 - Management von Verstößen und Vorfällen
- DPP7 - Bewusstsein schaffen und aufrechterhalten
- DPP8 - Organisation Datenschutz und DSB

- DPP9 - Betrieb von interne Kontrollen

Auch die gerade verabschiedete DIN EN ISO/IEC 27701:2021 („Deutsche Fassung der Sicherheitstechniken - Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz - Anforderungen und Leitlinien (ISO/IEC 27701:2019)“) kann hier für den Datenschutzbeauftragten hilfreich sein. Die dort beschriebenen spezifischen Anforderungen an ein Privacy Information Managementsystem (PIMS) stellen eine übersichtliche Ergänzung dar.

Empfehlung und Fazit

Es zeigt sich, dass nur ein systemischer Ansatz und eine strukturierte Vorgehensweise bei der Überprüfung (Audit) der Einhaltung der Anforderungen aus der DSGVO und des BDSG ausreichend und geeignet sein kann. Hierfür muss ein Verfahren etabliert werden. Dieses Verfahren muss regelmäßig durchgeführt werden. Optimalerweise wird diese Überprüfung als strukturiertes Audit durchgeführt und es wird der risikobasierte Ansatz berücksichtigt. Vor allem aber muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden. Diese Forderung legt die Messlatte für die Prüfungen durch den Datenschutzbeauftragten und den Verantwortlichen hoch. Dadurch wird auch bei den Prüfaufgaben eine nachhaltige Sicht auf die Verfahren, Prozesse und Maßnahmen des Datenschutz erforderlich. Dies lässt sich mit einer Momentaufnahme mittels Checkliste nicht umsetzen.

Über die Autoren

Christian Nawroth

Seit 1991 als technischer Consultant im Enterprise Umfeld tätig und seit 2002 Inhaber des Beratungsunternehmens SIGU-CONSULT. Außerdem ist er Mitglied des BvD Ausschuss Prüfaufgaben Datenschutzbeauftragter.



Patrick Grihn

Als Geschäftsführer der nextindex GmbH & Co. KG betreut er mit seinem Team KMUs in den Bereichen IT-Infrastruktur, IT-Sicherheit und Datenschutz.



Über den BvD-Ausschuss

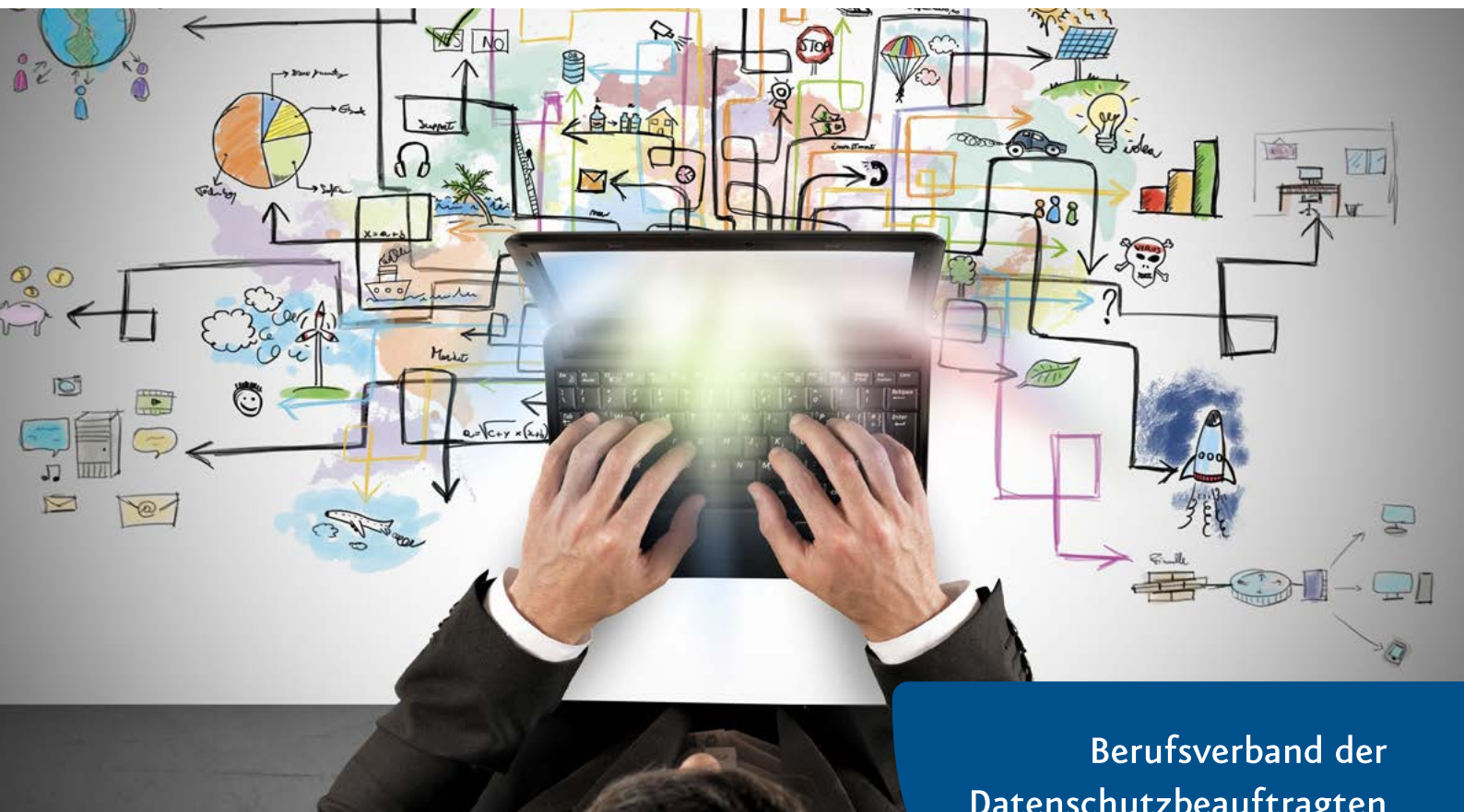
Beide Autoren sind Mitglied im Ausschuss Prüfaufgaben Datenschutzbeauftragter des BvD, der einen einheitlichen Prüfkatalog als Arbeitshilfe für den Datenschutzbeauftragten bei Audits erarbeitet.

⁷ Beuth-Verlag: „Inhaltsverzeichnis DIN EN ISO 19011:2018-10“, <https://www.beuth.de/de/norm/din-en-iso-19011/287794262>, 15.06.2021

⁸ ISACA: „Audit Program Narrativ - GDPR Audit Program“, 2018, Seite 5.

⁹ ISACA Auditcheckliste GDPR_Audit_Program_Enterprise.xlsx

BvD-Webinare & Online-Seminare



Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

WIR BIETEN SEMINARE UNTER ANDEREM ZU:

- Grundlagen- und Intensivseminare zur DSGVO
- Datenschutz & Datensicherheit
- Mitarbeiterdatenschutz
- Die rechtskonforme Einwilligung
- Verzeichnisverfahren und Dokumentationspflicht
- Überblick über die aktuellen Anforderungen in Deutschland, der EU und im transnationalen Datenaustausch

VORTEILE:

- Namhafte Referenten und Praktiker aus dem Datenschutz
- Als Fachwissen anerkannte Bildungsangebote
- Wertvolle Tipps für die Umsetzung im Arbeitsalltag
- Gezielte Beantwortung Ihrer Fragen
- Günstige Konditionen für BvD-Mitglieder / ZD-Abonnenten

PREISE:

Webinare	95,00 € [*] BvD-Mitglieder / ZD-Abonnenten
	145,00 € [*] Nichtmitglieder
Online-Seminare	295,00 € [*] BvD-Mitglieder / ZD-Abonnenten
	395,00 € [*] Nichtmitglieder

(*Alle Preise zzgl. gesetzl. MwSt.)

JETZT ANMELDEN:

www.bvdnet.de/termine

DER BvD: DIE INTERESSENVERTRETUNG DER DATENSCHUTZBEAUFTRAGTEN

Mit mehr als 30 Jahren Erfahrung ist der BvD die älteste Interessenvertretung für betriebliche und behördliche Datenschutzbeauftragte und -berater. BvD-Mitglieder sind in allen Branchen vertreten, insbesondere IT und IKT, Industrie/Produktion, Handel/Vertrieb, Beratung und Gesundheits- und Sozialwesen – und dort als konstruktiv-lösungsorientierte Datenschutzexperten ein wichtiger Partner für

die verantwortliche Unternehmensleitung. Alle Vorstände, alle Leiter von Arbeitskreisen, Ausschüssen und Regionalgruppen des BvD bringen ihre praktische Erfahrung unentgeltlich in die Verbandsarbeit ein. Mit der Gründung des Europäischen Dachverbandes EFDPO hat der BvD die Weichen für verstärkte Vernetzung und Kommunikation auf EU-Ebene gestellt.



DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31
10787 Berlin

Tel: 030 . 26 36 77 60
Fax: 030 . 26 36 77 63

E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de