ISO 19011 als Grundlage für Datenschutzaudits

Orientierungshilfe

Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

BvD-Ausschuss „Prüfaufgaben des Datenschutzbeauftragten“

BvD e.V.
DATENSCHUTZ GESTALTEN

Werden Sie Teil unseres starken Netzwerks!

BvD e.V.
DATENSCHUTZ GESTALTEN

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 Weiterbildungsmodule 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 Dokumentation 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 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
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.

ISO 19011 ALS GRUNDLAGE FÜR DATENSCHUTZAUDITS

Der systemische Ansatz

Stephan Rehfeld

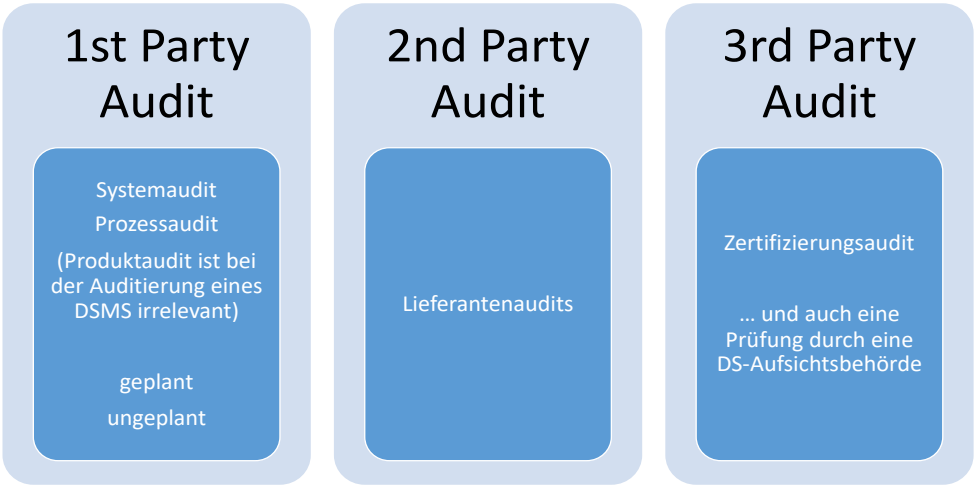
Unter der Ägide der Datenschutz-Grundverordnung (DSGVO) ist eine Aufgabe des Datenschutzbeauftragten die Organisation von Datenschutzaudits. Christian Nawroth und Patrick Grihn haben in ihrem vorangestellten Artikel die gesetzlichen Grundlagen des Datenschutzbeauftragten, des Verantwortlichen und des Auftragsverarbeiters für die Organisation und die Durchführung von Datenschutzaudits herausgearbeitet und begründet, warum nur ein systemischer Ansatz für die Durchführung von DSGVO-konformen Datenschutzaudits geeignet sein kann.

Die Autoren weisen in ihrem Artikel darauf hin, dass „[…] die Datenschutz-Grundverordnung oder das Bundesdatenschutzgesetz nicht weiter darauf [eingehen], wie Datenschutzbeauftragte diese doch sehr unspezifisch gehaltenen Prüfanforderungen explizit operativ umsetzen sollen."

Die Autoren haben herausgearbeitet, dass ein systemischer Ansatz zur Erfüllung der Datenschutzanforderungen der DSGVO an Datenschutzaudits fünf Anforderungen erfüllen muss:

- Es muss ein Verfahren etabliert werden.
- Dieses Verfahren muss regelmäßig durchgeführt werden.
- Es muss in Form einer Überprüfung stattfinden.
- Es muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden.
- Es muss ein risikobasierter Ansatz adressiert werden.

Die Autoren ziehen das Fazit „[…], 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." In diesem Artikel soll untersucht werden, inwieweit mit der ISO 19011:2018[1] ein DSGVO-konformes Vorgehen beschrieben wird, dass den Datenschutzbeauftragten, Verantwortlichen und/oder Auftragsverarbeiter dabei unterstützen kann Datenschutzaudits so zu planen und durchzuführen, dass die Anforderungen an einen systemischen Auditansatz erfüllt werden können.



[1] Im Weiteren wird auf die nationale Norm DIN EN ISO 19011:2018-10 Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018) Bezug genommen, wenn von der ISO 19011:2018 berichtet wird.

Audittypen

In der Praxis können verschiedene Audittypen unterschieden werden:

- Compliance-Audits
- Systemaudits
- Prozessaudits
- Produktaudits

Im Folgenden wird nur auf System- und Prozessaudits weiter eingegangen.

Als **Erstparteienaudit (1st Party Audit)** werden interne Audits bezeichnet. Eigene Mitarbeiter oder Dienstleister überprüfen für den Verantwortlichen die eigene Organisation nach Kriterien, die der Verantwortliche vorgegeben hat. Die Ergebnisse dienen zu eigenen Zwecken, wie der Erfüllung der organisationseigenen Nachweispflichten nach DSGVO.

Solche Erstparteienaudits können geplant oder ungeplant erfolgen. Im Regelfall erfolgen die internen Audits geplant und werden lang- oder mittelfristig im Rahmen eines Auditprogramms terminiert und mit den zu auditierenden Abteilungen terminiert. Ungeplante Audits können zum Beispiel durch Beschwerden oder Datenschutzvorfälle ausgelöst werden. Hier kann es erforderlich sein, dass kurzfristig überprüft wird, ob in Geschäftsprozessen die Datenschutzanforderungen eingehalten werden. Ungeplante Audits sollten der Ausnahmefall sein.

Weiterhin kann zwischen System- und Prozessaudits unterschieden werden. Bei einem Systemaudit wird das gesamte System auf sein generelles Funktionieren überprüft. Dies ist die Vogelperspektive auf ein Datenschutz-Managementsystem (DSMS). Bei einem Prozessaudit hingegen werden die zu untersuchenden Geschäftsprozesse auf Konformität untersucht. In der Praxis ist der Übergang von einem Systemaudit zu einem Prozessaudit fließend. Bei der erstmaligen Aufnahme eines Auditprogramms in einer Organisation wird ein Systemaudit im Vordergrund stehen, da meist erstmal die Frage geklärt werden soll, ob der betriebliche Datenschutz prinzipiell „funktioniert". Mit einer größeren Anzahl an durchgeführten Audits wird die Detailtiefe in den Vordergrund treten und die Prozessaudits werden wichtiger.

Als Zweitparteienaudit (2nd Party Audits) werden Lieferantenaudits bezeichnet. Bei Lieferantenaudits werden im Datenschutz Auftragsverarbeiter durch den Auftraggeber auditiert. Die Audits können durch eigenes Personal des Verantwortlichen durchgeführt werden oder durch beauftragte Dritte. In der DSGVO sind Lieferantenaudits in Art. 28. Abs. 3 lit. h DSGVO explizit vorgesehen.

Als Drittparteienaudits (3rd Party Audits) werden Zertifizierungsaudits bezeichnet. Hier beauftragt der Verantwortlichen einen Zertifizierer damit, ein Audit durchzuführen. Als Auditkriterium dient meistens ein Standard. Anders ist dies bei einer sogenannten Artikel-42-Zertifizierung. Hier wird gegen die DSGVO geprüft. Auch eine anlassfreie Prüfung durch eine Datenschutz-Aufsichtsbehörde kann systematisch als ein 3rd Party Audit aufgefasst werden.

Die ISO 19011:2018 ist ein Leitfaden, in dem allgemein die Auditierung von Managementsystemen beschrieben wird. Das Vorgehensmodell der ISO 19011:2018 kann bei den hier beschriebenen 1st, 2nd und 3rd Party Audits angewendet werden. In der ISO 19011:2018 wird nicht auf Produktaudits eingegangen und sie kann auf beliebige Themen von Managementsystemen angewendet werden, also etwa für Datenschutzaudits, aber auch Audits des Informationssicherheitsmanagements, des Qualitätsmanagements oder des Umweltmanagements. Die Kombination von Audits aus mehreren Management-Normen ist mit der ISO 19011:2018 möglich (auch als integrierte Audits bezeichnet) und durchaus gewollt.

Auditprinzipien

Die Auditprinzipien der ISO 19011:2018 sind die Grundlage der Arbeit der Auditoren bei der Prüfung eines (Datenschutz-) Managementsystems. Beim Auditieren müssen Auditoren die Auditprinzipien einhalten, damit unterschiedliche Auditoren zu identischen oder zumindest ähnlichen Auditergebnissen kommen (würden).
Ferner müssen die Auditprinzipien eingehalten werden, um bei den Personen in der zu auditierenden Organisation ausreichend Vertrauen zu erzeugen, um eine freie und wahrheitsgemäße Beantwortung zu ermöglichen (oder dieser nicht entgegenzuwirken).

In der ISO 19011:2018 werden die folgenden Auditprinzipien genannt:[2]

- Integrität
- sachliche Darstellung
- angemessene beruflich Sorgfalt
- Vertraulichkeit hinsichtlich der Sicherheit von Informationen
- Unabhängigkeit
- faktengestützter Ansatz
- risikobasierter Ansatz

Obwohl alle Auditprinzipien für ein erfolgreiches Audit wichtig sind, sollen drei Prinzipien genauer vorgestellt werden.

Mit dem **faktengestützten Ansatz** ist gemeint, dass Auditschlussfolgerungen auf nachvollziehbaren Fakten (sogenannten Nachweisen) gestützt werden und auf einer angemessenen Stichprobe basieren müssen. In einem engen Zusammenhang mit dem faktengestützten Ansatz steht die **sachliche Darstellung** eines Auditergebnisses.

Die Darstellung von Feststellungen und Auditschlussfolgerungen muss wahrheitsgemäß erfolgen. Sollte über eine Feststellung oder eine Auditschlussfolgerung zwischen der auditierten Organisation und dem Auditor Uneinigkeit bestehen, so muss der Auditor in seinem Bericht auch darüber objektiv und wahrheitsgemäß berichten.

Unter dem **risikobasierten Ansatz** fordert der Standard schwerpunktmäßig die Themen zu auditieren, die einen maßgeblichen Einfluss auf die Ziele des Managementsystems haben. Für den Auditor ergeben sich also die Auditschwerpunkte aus dem Managementsystem selbst.

Auditprogramm

Ein Audit ist in der ISO 19011:2018 keine Tätigkeit, die zufällig passiert. Stattdessen muss **der Auditauftraggeber** einen Auftrag zur Erstellung eines Auditprogramms an den **Auditprogrammleiter** geben. Der Auftraggeber ist typischerweise das Top-Management der zu auditierenden Organisation und der Auditprogrammleiter ist regelmäßig der Managementsystembeauftragte. Dies wird in der Praxis häufig der Datenschutzbeauftragte sein. Ob hier Konflikte mit der gesetzlich definierten Rolle des Datenschutzbeauftragten entstehen können, muss in Zukunft geklärt werden.

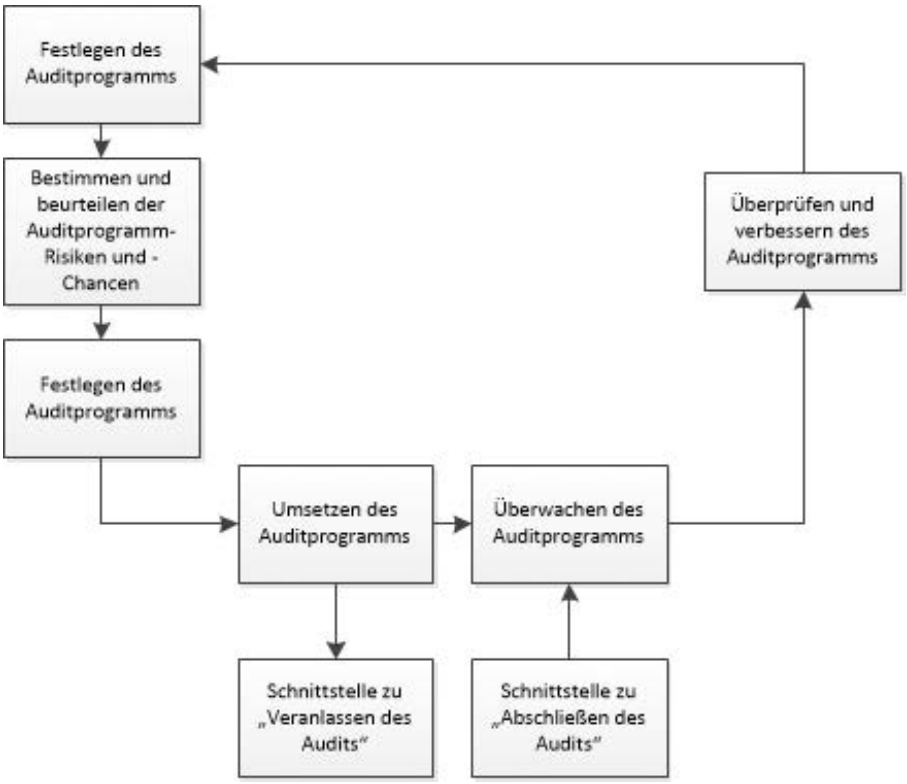


Abbildung 1: Prozessablauf für die Steuerung eines Auditprogramms (Auszug), DIN EN ISO 19011:2018-10, S. 23

Ein **Auditprogramm** ist die Planung und Durchführung von Audittätigkeiten für einen definierten Zeitraum. Der Umfang eines (Datenschutz-) Auditprogramms hängt von verschiedenen Faktoren ab, wie der Kritikalität der zu verarbeitenden personenbezogenen Daten oder der Größe der zu auditierenden Organisation.

In der ISO 19011:2018 wird der folgende Prozess zur Steuerung eines Auditprogramms vorgeschlagen: Bei der Festlegung eines Auditprogramms sollten folgende Informationen erfasst werden (Auszug):[3]

- Ziele für das Auditprogramm
- Risiken und Chancen in Verbindung mit dem Auditprogramm

[2] DIN EN ISO 19011:2018-10, S. 18 ff
[3] DIN EN ISO 19011:2018-10, S. 22

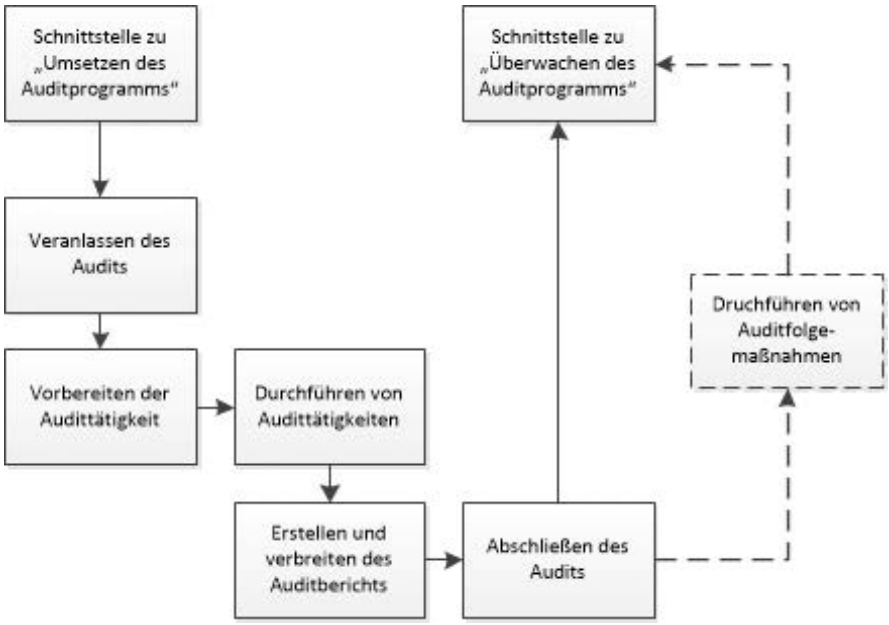


Abbildung 2: Prozessablauf für die Steuerung eines Auditprogramms (Auszug), DIN EN ISO 19011:2018-10, S. 23

- Umfang (Ausmaß, Grenzen, Standorte) jedes Audits des Auditprogramms
- Zeitplan (Anzahl, Dauer, Häufigkeit) der Audits

Hierbei sollte ein besonderes Augenmerk darauf gerichtet werden, dass die Ziele des Auditprogramms und die Auditkriterien klar definiert sind, damit bei den interessierten Parteien keine Enttäuschung über das Ergebnis des Auditprogramms entstehen.

Die Planung, Durchführung, Überwachung und Verbesserung eines Auditprogramms nach ISO 19011:2018 wird in dem Standard sehr ausführlich beschrieben, kann hier aber nicht weiter ausgeführt werden.

Auditdurchführung

Auch die Durchführung eines Audits, die Inhalte eines Auditberichts bis hin zur Durchführung von Auditfolgemaßnahmen werden in der ISO 19011:2018 detailliert beschrieben.

Der leitende Auditor hat die Aufgabe mit dem zu auditierenden Bereich der Organisation Kontakt aufzunehmen und das Audit zu planen. Bei der Vorbereitung der Audittätigkeit wird der Auditplan auf Grundlage des Auditprogramms und der vorab geprüften Dokumentation von dem/den Auditor(en) erstellt. Anschließend wird das eigentliche Audit durchgeführt. Während des Audits sammeln die Auditoren objektive Nachweise, um die Konformität oder die Nichtkonformität des auditierten Bereichs mit den Auditzielen feststellen zu können. Die Auditfeststellungen werden mit dem auditierten Bereich am Ende das Audits besprochen und in einem Auditbericht dokumentiert. Bei Nichtkonformität, also Abweichungen von den Auditzielen oder systematischen Mängeln, werden mit dem auditierten Bereich Korrekturmaßnahmen vereinbart. Diese Korrekturmaßnahmen müssen nach der Umsetzung auf ihre Wirksamkeit überprüft werden. Der Auditbericht wird dem Auditprogrammleiter und auch dem Top-Management zur Auswertung übermittelt. In kleineren Organisationen wird die Aufgabe des Auditprogrammleiters und des Auditors dem Datenschutzbeauftragten zufallen.

Fazit

Die vorstehenden Ausführungen sollen zur Beurteilung dienen, ob die ISO 19011:2018 ein Standard ist, der einen Datenschutzbeauftragten, Verantwortlichen oder Auftragsverarbeiter bei der Erfüllung seiner gesetzlichen Datenschutz-Auditverpflichtung nach DSGVO unterstützt und einen systemischen Ansatz verfolgt. Nach Nawroth/Grihn müssen dazu die folgenden fünf Anforderungen erfüllt werden:

- Es muss ein Verfahren (Prozess) etabliert werden. Der Standard ISO 19011:2018 beschreibt einen Prozess zur Planung, Durchführung, Überwachung und Verbesserung eines Auditprogramms, dass alle Audits innerhalb eines definierten Zeitraums umfasst. Auch die Auditdurchführung wird in einem Prozess beschrieben.
- Diese Verfahren (Prozesse) müssen regelmäßig durchgeführt werden. Ein Auditprogramm nach ISO 19011:2018 basiert auf dem PDCA-Zyklus. Somit ist die Planung, Durchführung, Überwachung und Verbesserung als zyklischer Prozess angelegt und Audits müssen von der zu auditierenden Organisation regelmäßig durchgeführt werden.
- Es muss in Form einer Überprüfung stattfinden. Die ISO 19011:2018 ist bei der Definition der Auditziele und der Auditkriterien offen. Wenn die zu auditierende Organisation festlegt, dass ein Auditziel die Feststellung der Datenschutz-Compliance im Stichprobenumfang ist und als Auditkriterien die anzuwendenden Datenschutzgesetze benannt werden (z.B. DSGVO und BDSG-neu), wird diese Anforderung von Nawroth/Grihn durch die ISO 19011:2018 erfüllt.
- Es muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden. Im Audit ist es Aufgabe der Auditoren nach objektiven Nachweisen für die Konformität oder Nichtkonformität des DSMS zu suchen. Eine Nichtkonformität kann auch eine systematische Verletzung von Anforderungen sein.
- Es muss ein risikobasierter Ansatz adressiert werden. Für Audits nach der ISO 19011:2018 werden Auditprinzipien verbindlich vorgeschrieben. Ein Auditprinzip ist die Berücksichtigung des risikobasierten Ansatzes bei der Planung und Umsetzung des Auditprogramms.

Fazit: Die ISO 19011:2018 ist als Rahmenwerk für die Auditierung von Datenschutz-Managementsystemen bzw. der Bewertung der Einhaltung von gesetzlichen Anforderungen für einen Datenschutzbeauftragten oder eine Organisation geeignet, die Forderung nach einem systemischen Ansatz für Datenschutzaudits zu erfüllen.

Über den Autor

Dipl.-Ök. Stephan Rehfeld
ist externer Datenschutzbeauftragter der scope & focus GmbH Hannover und akkreditierter Datenschutzauditor der DQS GmbH. Als stimmberechtigtes Mitglied des AK05 des NIA27 des DIN arbeitet er aktiv an der Erstellung und Überarbeitung von Datenschutz-ISO- und -DIN-Normen mit. Ferner ist er im Leitungskreis des GDD-Erfa-Kreises Hannover engagiert, im AK Datenschutz der Bitkom und in der Fachgruppe Datenschutz von Niedersachsen.Digital e.V.
Stephan Rehfeld ist außerdem BvD-Vorstandsmitglied und Mitglied im Ausschuss Prüfaufgaben Datenschutzbeauftragter des BvD.

BvD-Webinare & Online-Seminare

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

WIR BIETEN SEMINARE UNTER ANDEREM ZU:

- Grundlagen- und Intensivseminare zur DSGVO
- Datenschutz & Datensicherheit
- Mitarbeiterdatenschutz
- Die rechtskonforme Einwilligung
- Verfahrensverzeichnis 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. gesetz. 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.

BvD e.V.

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