



**Vorbereitungshandbuch**

Ausgabe 201810

Copyright © EXIN Holding B.V. 2018. All rights reserved.  
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.



# Inhalt

1. Überblick	4
2. Prüfungsanforderungen	6
3. Liste der Grundbegriffe	9
4. Literatur	13

# 1. Überblick

EXIN Privacy & Data Protection Essentials (PDPE.DE)

## Anwendungsbereich

EXIN Privacy and Data Protection Essentials (PDPE) ist eine Zertifizierung, die das Fachwissen einer Person über die Organisation des Schutzes personenbezogener Daten, die EU-Vorschriften und Bestimmungen hinsichtlich des Datenschutzes bestätigt.

## Zusammenfassung

Wann immer personenbezogene Daten erhoben, gespeichert, verwendet und letztendlich gelöscht oder vernichtet werden, kommen Bedenken hinsichtlich des Datenschutzes auf. Mit der EU-Datenschutz Grundverordnung (DSGVO) versucht der Rat der Europäischen Union den Datenschutz für alle Personen innerhalb der Europäischen Union (EU) zu stärken und zu vereinheitlichen. Diese Verordnung betrifft jede Organisation, die personenbezogene Daten von Personen aus der EU verarbeitet. Die PDPF-Zertifizierung deckt die Hauptthemen im Zusammenhang mit der EU-Datenschutz Grundverordnung (DSGVO) ab.

## Kontext

Die Zertifizierung EXIN Privacy and Data Protection Essentials (PDPE) ist Teil des EXIN-Qualifizierungsprogramms Privacy and Data Protection (Privatsphäre und Datenschutz). Die Essentials-Prüfung ist eine Teilmenge der Foundation-Prüfung. Es kann nicht für den Zugang zur Practitioner-Prüfung verwendet werden, ist aber für diejenigen gedacht, die ein grundlegendes Verständnis der DSGVO benötigen.



## Zielgruppe

Alle, die ein Grundverständnis für den Datenschutz und die europäischen gesetzlichen Anforderungen, wie in der DSGVO definiert, haben wollen oder müssen. Die Essentials-Prüfung eignet sich hervorragend für alle, die fundierte Entscheidungen in Bezug auf die Privatsphäre und den Datenschutz ihrer eigenen Daten treffen möchten oder müssen.

## Zertifizierungsvoraussetzungen

- Erfolgreicher Abschluss der Prüfung zum EXIN Privacy und Data Protection Essentials.

## Einzelheiten zur Prüfung

Prüfungsart:	Multiple-Choice-Fragen
Anzahl der Fragen:	20
Mindestpunktzahl:	65%
Einsicht in Dokumentation/Notizen:	Nein
Elektronische Geräte/Hilfsmittel erlaubt:	Nein
Prüfungsdauer:	30 Minuten

Es gelten die EXIN Examen-Regeln und -Vorschriften.

## Taxonomiestufen nach Bloom

Die EXIN Privacy & Data Protection Essentials Zertifizierung testet Kandidaten auf Bloom Level 1.

- Bloom Level 1: Wissen – basiert auf dem wieder Abrufen von Informationen. Kandidaten müssen aufnehmen, merken, erkennen und wiedergeben. Dies ist das Lern-Fundament, ehe Kandidaten sich auf höhere Stufen weiterbewegen können.

## Schulung

### Präsenzstunden

Dieser Kurs umfasst mindestens 7 Präsenzstunden. Darin enthalten sind Gruppenarbeiten, die Vorbereitung auf das Examen sowie kurze Pausen, nicht enthalten sind: Hausaufgaben, die Logistik im Zusammenhang mit dem Examenstermin, der Examenstermin und Mittagspausen.

### Regelstudiendauer

20 Stunden, je nach Vorwissen.

### Schulungsanbieter

Eine Liste der akkreditierten Schulungsanbieter finden Sie auf der Webseite von EXIN [www.exin.com](http://www.exin.com).

## 2. Prüfungsanforderungen

Die Prüfungsanforderungen sind im Einzelnen in den Prüfungsspezifikationen erläutert. In der unten dargestellten Tabelle finden Sie eine Liste mit den Themen des Moduls (Prüfungsanforderungen).

Prüfungsanforderung	Prüfungsspezifikationen	Gewichtung
<b>1. Grundlagen und Bestimmungen hinsichtlich des Datenschutzes</b>		<b>50%</b>
	1.1 Definitionen	10%
	1.2 Personenbezogene Daten	15%
	1.3 Berechtigte Gründe und Zweckbindung	10%
	1.4 Weitere Anforderungen an eine legitime Verarbeitung personenbezogener Daten	5%
	1.5 Rechte von betroffenen Personen	5%
	1.6 Verletzung des Schutzes personenbezogener Daten und damit zusammenhängende Verfahren	5%
<b>2. Organisation des Datenschutzes</b>		<b>25%</b>
	2.1 Bedeutung des Datenschutzes für die Organisation	10%
	2.2 Aufsichtsbehörde	5%
	2.3 Übermittlung personenbezogener Daten an Drittländer <sup>1</sup>	--
	2.4 Verbindliche interne Datenschutzvorschriften und Datenschutz in Verträgen	10%
<b>3. Praxis des Datenschutzes</b>		<b>25%</b>
	3.1 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Bezug auf die Informationssicherheit	5%
	3.2 Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) und Prüfung des Schutzes personenbezogener Daten	5%
	3.3 Praxisbezogene Anwendungen hinsichtlich der Nutzung von Daten, Marketing und sozialer Medien	15%
Total		100%

<sup>1</sup> Prüfungsspezifikation 2.3 wird nur in EXIN Privacy & Data Protection Foundation getestet.

## Prüfungsspezifikationen

### 1 Grundlagen und Bestimmungen hinsichtlich des Schutzes personenbezogener Daten

- 1.1 Definitionen
  - Der Kandidat kann ...
  - 1.1.1 privatsphärenbezogene Definitionen abrufen.
  - 1.1.2 die Privatsphäre mit dem Konzept des Datenschutzes in Zusammenhang bringen.
- 1.2 Personenbezogene Daten
  - Der Kandidat kann ...
  - 1.2.1 eine Definition personenbezogener Daten nach der DSGVO nennen.
  - 1.2.3 die Rechte der betroffenen Person hinsichtlich personenbezogener Daten beschreiben.
  - 1.2.5 die Rollen, Verantwortlichkeiten und Interessensträger auflisten.
- 1.3 Berechtigte Gründe und Zweckbindung
  - Der Kandidat kann ...
  - 1.3.1 die sechs berechtigten Gründe für Verarbeitung auflisten.
  - 1.3.2 das Konzept der Zweckbindungen beschreiben.
  - 1.3.3 die Verhältnismäßigkeit und Subsidiarität beschreiben.
- 1.4 Weitere Anforderungen an eine berechtigte Verarbeitung personenbezogener Daten
  - Der Kandidat kann ...
  - 1.4.1 die Anforderungen an die Datenverarbeitung beschreiben.
  - 1.4.2 den Zweck der Verarbeitung personenbezogener Daten beschreiben.
- 1.5 Rechte von betroffenen Personen
  - Der Kandidat ...
  - 1.5.2 hat Kenntnis von dem „Recht auf Vergessenwerden“.
- 1.6 Verletzung des Schutzes personenbezogener Daten und damit zusammenhängende Verfahren
  - Der Kandidat kann ...
  - 1.6.1 das Konzept der Verletzung des Schutzes personenbezogener Daten beschreiben.

### 2 Organisation des Datenschutzes

- 2.1 Bedeutung des Datenschutzes für die Organisation
  - Der Kandidat kann ...
  - 2.1.2 anführen, welche Aktivitäten für die Einhaltung der DSGVO erforderlich sind.
  - 2.1.3 eine Definition von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nennen.
  - 2.1.5 die Meldepflicht im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten gemäß der DSGVO beschreiben.
- 2.2 Aufsichtsbehörde
  - Der Kandidat kann ...
  - 2.2.1 die allgemeinen Pflichten einer Aufsichtsbehörde beschreiben.
- 2.4 Verbindliche interne Datenschutzvorschriften und Datenschutz in Verträgen
  - Der Kandidat kann ...
  - 2.4.1 das Konzept verbindlicher interner Datenschutzvorschriften beschreiben.
  - 2.4.2 beschreiben, wie Datenschutz in schriftlichen Verträgen zwischen dem Verantwortlichen und dem Auftragsverarbeiter formalisiert ist.

### 3 Praxis des Datenschutzes

- 3.1 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Bezug auf die Informationssicherheit  
Der Kandidat kann ...
  - 3.1.1 die Vorteile der Anwendung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen beschreiben.
- 3.2 Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA)  
Der Kandidat kann ...
  - 3.2.1 beschreiben, was eine DPIA umfasst und wann sie angewendet wird.
- 3.3 Praxisbezogene Anwendungen hinsichtlich der Nutzung von Daten, Marketing und sozialer Medien  
Der Kandidat kann ...
  - 3.3.1 den Zweck der Verwaltung von Daten über den gesamten Nutzungszeitraum (DLC) beschreiben.
  - 3.3.3 beschreiben, was ein Cookie ist und was es tut.
  - 3.3.4 aus Datenschutzperspektive beschreiben, wie die weit verbreitete Nutzung des Internets den Bereich des Marketings beeinflusst hat.



### 3. Liste der Grundbegriffe

Dieses Glossar enthält Begriffe, mit denen den Teilnehmern vertraut sein sollten.

Bitte beachten Sie, dass die Kenntnis dieser Begriffe alleine nicht ausreicht. Den Teilnehmern müssen diese Begriffe auch verstehen und mit Beispielen belegen können.

<b>English</b>	<b>Deutsch</b>
adequate	angemessen
appropriate technical and organizational measures	geeignete technische und organisatorische Maßnahmen
authenticity	Authentizität
availability	Verfügbarkeit
binding	verbindlich
binding corporate rules	Verbindliche interne Datenschutzvorschriften
biometric data	biometrische Daten
certification	Zertifizierung
certification bodies	Zertifizierungsstelle
child's consent	Einwilligung des Kindes
codes of conduct	Verhaltenskodex
collection of personal data (verb.)	Erfassung personenbezogener Daten
commission reports	Berichte der Kommission
complaint	Beschwerde
compliance	Konformität (Compliance)
conditions for consent	Bedingungen für die Einwilligung
consent	Einwilligung
consistency	Kohärenz
consistency mechanism	Kohärenzverfahren
constitution	Verfassung
contract	Vertrag
controller	Verantwortlicher
cross-border processing	grenzüberschreitende Verarbeitung
data breach	Verletzung des Schutzes personenbezogener Daten
data concerning health	Gesundheitsdaten
data controller	Verantwortlicher
data protection	Datenschutz
data protection authority	Aufsichtsbehörde
data protection by default	datenschutzfreundliche Voreinstellungen
data protection by design	Datenschutz durch Technikgestaltung
data protection impact assessment (DPIA)	Datenschutzfolgeabschätzung (DPIA)
data protection officer (DPO)	Datenschutzbeauftragter
<ul style="list-style-type: none"> <li>• designation</li> <li>• position</li> <li>• tasks</li> </ul>	<ul style="list-style-type: none"> <li>• Bestellung</li> <li>• Stellung</li> <li>• Aufgaben</li> </ul>
data subject	betroffene Person

data transfer	Datenübertragung
delegated acts and implementing acts <ul style="list-style-type: none"> <li>• committee procedure</li> </ul>	Delegierte Rechtsakte und Durchführungsrechtsakte <ul style="list-style-type: none"> <li>• Ausschussverfahren</li> </ul>
derogation	abweichende Regelung
enforcement <ul style="list-style-type: none"> <li>• administrative fines</li> <li>• administrative penalties</li> <li>• criminal penalties</li> <li>• dissuasive penalties</li> <li>• effective penalties</li> <li>• proportionate penalties</li> </ul>	Durchsetzungsverfahren <ul style="list-style-type: none"> <li>• Geldbußen</li> <li>• verwaltungsrechtliche Sanktionen</li> <li>• Strafen</li> <li>• abschreckende Sanktionen</li> <li>• wirksame Sanktionen</li> <li>• verhältnismäßige Sanktionen</li> </ul>
enterprise	Unternehmen
European Economic Area (EEA)	Europäischer Wirtschaftsraum (EWR)
EU types of legal act <ul style="list-style-type: none"> <li>• decision</li> <li>• directive</li> <li>• opinion</li> <li>• recommendation</li> <li>• regulation</li> </ul>	Rechtsakte der Europäischen Union <ul style="list-style-type: none"> <li>• Beschluss</li> <li>• Richtlinien</li> <li>• Stellungnahme</li> <li>• Empfehlung</li> <li>• Verordnung</li> </ul>
European Data Protection Board <ul style="list-style-type: none"> <li>• chair</li> <li>• confidentiality</li> <li>• independence</li> <li>• procedure</li> <li>• reports</li> <li>• secretariat</li> <li>• tasks</li> </ul>	Europäische Datenschutzausschuss <ul style="list-style-type: none"> <li>• Vorsitz</li> <li>• Vertraulichkeit</li> <li>• Unabhängigkeit</li> <li>• Verfahren</li> <li>• Berichte</li> <li>• Sekretariat</li> <li>• Aufgaben</li> </ul>
European Data Protection Supervisor (EDPS)	Europäischer Datenschutzbeauftragter
European Union legal acts on data protection	Rechtsakte der Europäischen Union zum Datenschutz
exchange of information	Informationsaustausch
exemption	Ausnahme
explicit consent	ausdrückliche Einwilligung
genetic data	genetische Daten
filing system	Dateisystem
General Data Protection Regulation (GDPR)	Datenschutz-Grundverordnung (DSGVO)
governing body	leitende Stelle
group of undertakings	Unternehmensgruppe
independent supervisory authorities <ul style="list-style-type: none"> <li>• activity reports</li> <li>• competence</li> <li>• establishment</li> <li>• powers</li> <li>• tasks</li> </ul>	unabhängige Aufsichtsbehörden <ul style="list-style-type: none"> <li>• Tätigkeitsberichte</li> <li>• Kompetenz</li> <li>• Geltendmachung</li> <li>• Befugnisse</li> <li>• Aufgaben</li> </ul>
information society service	Dienst der Informationsgesellschaft
international organization	internationale Organisationen
joint controllers	gemeinsam Verantwortliche
judicial remedy	gerichtlicher Rechtsbehelf
lawfulness of processing	Rechtmäßigkeit der Verarbeitung
legal basis	Rechtsgrundlage

legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)	berechtigter Grund (17/1c) zulässige Rechtsgrundlage (DSGVO 40)
legitimate interest	berechtigtes Interesse
liability	Haftung
main establishment	Hauptniederlassung
material scope	sachlicher Anwendungsbereich
National Identification Number	nationale Kennziffer
non-repudiation	Nichtabstreitbarkeit
opinion of the board	Stellungnahme des Ausschusses
personal data	personenbezogene Daten
personal data breach	Verletzung des Schutzes personenbezogener Daten
personal data relating to criminal convictions and offences	personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten
principles relating to processing of personal data	Grundsätze für die Verarbeitung personenbezogener Daten
<ul style="list-style-type: none"> <li>• accountability</li> <li>• accuracy</li> <li>• confidentiality</li> <li>• data minimization</li> <li>• fairness</li> <li>• integrity</li> <li>• lawfulness</li> <li>• purpose limitation</li> <li>• storage limitation</li> <li>• transparency</li> </ul>	<ul style="list-style-type: none"> <li>• Rechenschaftspflicht</li> <li>• Richtigkeit, Korrektheit</li> <li>• Vertraulichkeit</li> <li>• Datenminimierung</li> <li>• Verarbeitung nach Treu und Glauben (fairness)</li> <li>• Integrität</li> <li>• Rechtmäßigkeit</li> <li>• Zweckbindung</li> <li>• Speicherbegrenzung</li> <li>• Transparenz</li> </ul>
prior consultation	vorherige Konsultation
privacy	Privatsphäre
processing	Verarbeitung
processing situations	Verarbeitungssituationen
<ul style="list-style-type: none"> <li>• data protection rules of churches and religious associations</li> <li>• employment</li> <li>• for archiving purposes in the public interest</li> <li>• for scientific or historical research purposes</li> <li>• for statistical purposes</li> <li>• freedom of expression and information</li> <li>• National Identification Number</li> <li>• obligations of secrecy</li> <li>• public access to official documents</li> </ul>	<ul style="list-style-type: none"> <li>• Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften</li> <li>• Beschäftigung</li> <li>• im öffentlichen Interesse liegende Archivzwecke</li> <li>• wissenschaftliche oder historische Forschungszwecke</li> <li>• für statistische Zwecke</li> <li>• freie Meinungsäußerung und Information</li> <li>• nationale Kennziffer</li> <li>• Geheimhaltungspflichten</li> <li>• Zugang der Öffentlichkeit zu amtlichen Dokumenten</li> </ul>
processing which does not require identification	Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist
processor	Auftragsverarbeiter
profiling	Profiling
pseudonymization	Pseudonymisierung
recipient	Empfänger

relevant and reasoned objection	maßgeblicher und begründeter Einspruch
representative	Vertreter
restriction of processing	Einschränkung der Verarbeitung
retention period	Aufbewahrungsfrist
right to compensation	Recht auf Schadenersatz
rights of the data subject	Rechte der betroffenen Person
<ul style="list-style-type: none"> <li>• automated individual decision-making</li> <li>• data portability</li> <li>• information and access</li> <li>• modalities</li> <li>• notification obligation</li> <li>• rectification and erasure</li> <li>• restriction of processing</li> <li>• restrictions</li> <li>• 'right to be forgotten'</li> <li>• right to objection</li> <li>• transparency</li> </ul>	<ul style="list-style-type: none"> <li>• automatisierte Entscheidungsfindung im Einzelfall</li> <li>• Datenübertragbarkeit</li> <li>• Informationspflicht und Recht auf Auskunft</li> <li>• Modalitäten</li> <li>• Mitteilungspflicht</li> <li>• Berichtigung und Löschung</li> <li>• Einschränkung der Verarbeitung</li> <li>• Einschränkungen</li> <li>• Recht auf Vergessenwerden</li> <li>• Widerspruchsrecht</li> <li>• Transparenz</li> </ul>
rules of procedure	Geschäftsordnung
security breach (security incident)	Sicherheitsverstoß (Sicherheitsvorfall)
security of personal data	Sicherheit personenbezogener Daten
security of processing	Sicherheit der Verarbeitung
sensitive data	sensible Daten
special categories of personal data	besondere Arten personenbezogener Daten
<ul style="list-style-type: none"> <li>• biometric data</li> <li>• data concerning health</li> <li>• genetic data</li> <li>• political opinions</li> <li>• racial or ethnic origin</li> <li>• religious or philosophical beliefs</li> <li>• sex life or sexual orientation</li> <li>• trade union membership</li> </ul>	<ul style="list-style-type: none"> <li>• biometrische Daten</li> <li>• Gesundheitsdaten</li> <li>• genetische Daten</li> <li>• politische Einstellung</li> <li>• Rasse oder ethnische Herkunft</li> <li>• Religion oder Weltanschauung</li> <li>• Sexualleben oder sexuelle Orientierung</li> <li>• Gewerkschaftszugehörigkeit</li> </ul>
Supervisory Authority	Aufsichtsbehörde
Supervisory Authority concerned	betroffene Aufsichtsbehörde
suspension of proceedings	Aussetzung des Verfahrens
territorial scope	Räumlicher Anwendungsbereich
third party	Dritter
transfer of personal data to third countries and to international organizations	Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen
<ul style="list-style-type: none"> <li>• adequacy decision</li> <li>• appropriate safeguards</li> <li>• binding corporate rules</li> <li>• derogations</li> <li>• disclosures</li> <li>• international protection of personal data</li> </ul>	<ul style="list-style-type: none"> <li>• Angemessenheitsbeschluss</li> <li>• geeignete Garantien</li> <li>• Verbindliche interne Datenschutzvorschriften</li> <li>• Abweichende Regelung</li> <li>• Offenlegung</li> <li>• internationaler Schutz personenbezogener Daten</li> </ul>

## 4. Literatur

### Prüfungsliteratur

- A. A. Calder  
**EU GDPR, A pocket guide**  
IT Governance Publishing  
ISBN 978-1-84928-855-2  
(or ISBN 978-1-84928-857-6 for e-book)
- A. Calder  
**EU-DSGVO, eine Kurzanleitung**  
IT Governance Publishing  
ISBN-13: 9781849288637  
(oder ISBN13: 9781849288644 für e-buch)
- B. L. Besemer  
**White Paper – EXIN Privacy and Data Protection Foundation**  
Gratis zum Download auf [www.exin.com](http://www.exin.com)
- C. European Commission  
**General Data Protection Regulation (GDPR)** Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016, available at:  
<http://eur-lex.europa.eu>  
PDF:  
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>  
HTML:  
<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN>

### Anmerkungen

- Die deutsche Übersetzung der DSGVO kann von der Website der EU (<http://eur-lex.europa.eu/>) heruntergeladen werden.
- Die Prüfungsanforderungen basieren auf der Examen-Literatur. Literaturquelle C ist keine primäre Literaturquelle, da die andere Examen-Literatur ausreichenden Inhalt zur DSGVO bietet.
- Kandidaten sollten mit Literaturquelle C so weit vertraut sein, wie es die Referenzen aus den anderen Literaturquellen verlangen.

## Literaturmatrix

Prüfungsanforderung	Prüfungsspezifikation	Literaturverweis	DSGVO Referenz
<b>1. Grundlagen und Bestimmungen hinsichtlich des Datenschutzes</b>			
	1.1 Definitionen	A: Ch. 1, Ch. 3 B: §1.1.1	rec. 1, 2 & art 96-99
	1.2 Personenbezogene Daten	A: Ch. 2, Ch. 3 B: §1.1.3, §1.3.6, §1.3.7, §4	art. 4.1 (a), art 9.1, art 17, art 4.10
	1.3 Berechtigte Gründe und Zweckbindung	B: §3.1, §3.2, §3.3	art 6.1, art 24
	1.4 Weitere Anforderungen an eine legitime Verarbeitung personenbezogener Daten	B: §2.1, §6.1	art 25, art 27-32, art 5
	1.5 Rechte von betroffenen Personen	B: §4.3, §4.4.2	Kein Ref.
	1.6 Verletzung des Schutzes personenbezogener Daten und damit zusammenhängende Verfahren	B: §5.1-5.3	art 4(12), art 33, art 34
<b>2. Organisation des Datenschutzes</b>			
	2.1 Bedeutung des Datenschutzes für die Organisation	A: Ch. 3, Ch. 4 B: §5.2, §5.3, §6.1, §6.3, §8.1	art 7, art 8, art 13, art 30, art 25(1), art 83
	2.2 Aufsichtsbehörde	A: Ch. 3 B: §7.1, §7.3	art 36, art 33, art 34
	2.4 Verbindliche interne Datenschutzvorschriften und Datenschutz in Verträgen	A: Ch. 3 B: §7.4.3.3, §8.2	art 47, art 24, art 28
<b>3. Praxis des Datenschutzes</b>			
	3.1 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Bezug auf die Informationssicherheit	B: §5.2, §8.1.1	Kein Ref.
	3.2 Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) und Prüfung des Schutzes personenbezogener Daten	§6.1.3, §8.3, §8.5	Kein Ref.
	3.3 Praxisbezogene Anwendungen hinsichtlich der Nutzung von Daten, Marketing und sozialer Medien	§8.4, §8.6	Kein Ref.



# Kontakt EXIN

[www.exin.com](http://www.exin.com)

