datenschutz cert


DSGVO – information privacy standard

# Zertifizierung gemäß Art. 42 DSGVO

DuD 2025 / Datenschutz und Datensicherheit
Datenschutzkongress
am 2. und 3. Juni 2025 in Potsdam

**www.datenschutz-cert.de**

# Agenda

1. Hintergründe, Motivation, Vorteile
2. Zulassungsprozess
3. Methodik
4. Kriterien
5. Fazit

datenschutz cert

# 1.

# Hintergründe, Motivation, Vorteile

## Warum ist ein DSGVO-Zertifikat interessant? Und für wen?

# Gesetzliche Grundlagen

DSGVO definiert verschiedene Anforderungen an Verantwortliche und Auftragsverarbeiter

mit: Nachweispflicht für Verantwortliche und Auftragsverarbeiter

Art. 24, 25, 28 und 32 DSGVO erwähnen „genehmigte Zertifizierungsverfahren“ als „Gesichtspunkt“ zum Nachweis der „Erfüllung der Pflichten“

Art. 42 DSGVO enthält allgemeine Regelungen zur Zertifizierung

Art. 43 DSGVO definiert Vorgaben an Zertifizierungsstellen

datenschutz cert

# Beispiel: Art. 24

datenschutz cert

*Artikel 24*

**Verantwortung des für die Verarbeitung Verantwortlichen**

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

DSGVO information privacy standard

# Nachfrage nach Zertifikaten ist da!

endlich gibt es ein Datenschutz-Zertifikat – mit gesetzlichem Rahmen

interessant für Verantwortliche und Auftragsverarbeiter

wir sehen folgende Vorteile…

datenschutz cert

# 1: Wettbewerbsvorteil

datenschutz cert

Setzen Sie sich von Ihren Marktbegleitern ab und zeigen Sie durch ein offizielles Art. 42 DSGVO-Zertifikat, dass Ihnen der Schutz der Daten Ihrer Kunden absolute Priorität genießt.

insb. interessant für Auftragsverarbeitung gem. Art. 28 DSGVO

Seien Sie von Anfang dabei, wenn sich der Zertifizierungsstandard DSGVO – information privacy standard zum Must-Have der Auftragsverarbeiter entwickelt – ähnlich wie ISO/IEC 27001 bei Rechenzentren.

# 2: Marktzutritt

Zertifikate werden immer häufiger gefordert – in Ausschreibungen oder im Rahmen einer Zulassung. Es gibt erste gesetzliche Vorgaben, die die explizite Vorlage eines offiziellen Art. 42 DSGVO-Zertifikates verlangen: Videosprechstunden, DiGaV-Gesundheitsanwendungen. Ohne dieses Zertifikat ist kein Marktzutritt möglich!

Erfahrungsgemäß wird es nicht bei diesen Verordnungen bleiben. Nehmen Sie die – und kommende – gesetzliche Hürden in Angriff.

Definieren Sie Ihre Verarbeitungsvorgänge, die Sie gem. Art. 42 DSGVO zertifizieren lassen möchten.

datenschutz cert

# 3: Haftungsreduktion

datenschutz cert

Datenschutzverstöße sind teuer! Bis zu 2% des Jahresumsatzes können fällig werden. Und die Aufsichtsbehörden sind da nicht zimperlich.

Damit ist Datenschutz KontraG- und Bilanz-relevant.

Reduzieren Sie Ihre Haftung! Oder Ihre Rückstellungen! Oder Ihre Versicherungsbeträge!

# 4: Besserer Datenschutz

datenschutz cert

Sie verarbeiten personenbezogene Daten Ihrer Kunden, evtl. sogar besondere Arten personenbezogener Daten. Datenschutz ist für Ihr Business unabdingbare Voraussetzung.

Vier Augen sehen mehr! Verbessern Sie Ihren Datenschutz durch eine unabhängige Prüfung – und ein offizielles Art. 42 DSGVO-Zertifikat.

# 5: Datenschutz leichter durchsetzen

Ein offizielles Art. 42 DSGVO-Zertifikat wirkt – nicht nur nach außen ggü. Ihren Kunden, den Aufsichtsbehörden oder dem Gesetzgeber, sondern auch nach innen.

Denn mit einem DSGVO-Zertifikat im Nacken lässt sich so manches Datenschutz-Thema spielend leicht umsetzen.

datenschutz cert

# Fazit: Fünf Vorteile für ein DSGVO-Zertifikat

1. Wettbewerbsvorteil
2. Marktzutritt
3. Haftungsreduktion
4. besserer Datenschutz
5. Datenschutz leichter durchsetzen

datenschutz cert

datenschutz cert

# 2. Zulassungsprozess

## Warum dauert die Zulassung so lange?

# Beispiel: Art. 42: Genehmigte Kriterien

datenschutz cert

(5) Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Artikel 58 Absatz 3 oder — gemäß Artikel 63 — durch den Ausschuss genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen.

DSGVO information privacy standard

# Beispiel: Art. 43: Akkreditierte und befugniserteilte Zertifizierungsstellen

datenschutz cert

(1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 erteilen oder verlängern Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, nach Unterrichtung der Aufsichtsbehörde — damit diese erforderlichenfalls von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe h Gebrauch machen kann — die Zertifizierung. Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von einer oder beiden der folgenden Stellen akkreditiert werden:

a) der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde;

b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([1]) im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.

DSGVO information privacy standard

# Anspruchsvolles Zulassungsverfahren

DSGVO gibt Akkreditierungsnorm vor: ISO/IEC 17065 für Produkte/Dienstleistungen

Basis für Akkreditierung ist Konformitäts-bewertungsprogramm (KBP) mit Kriterienkatalog

Abnahme von Programm mit Kriterien durch DAkkS, zuständigen LfDI und EDPB

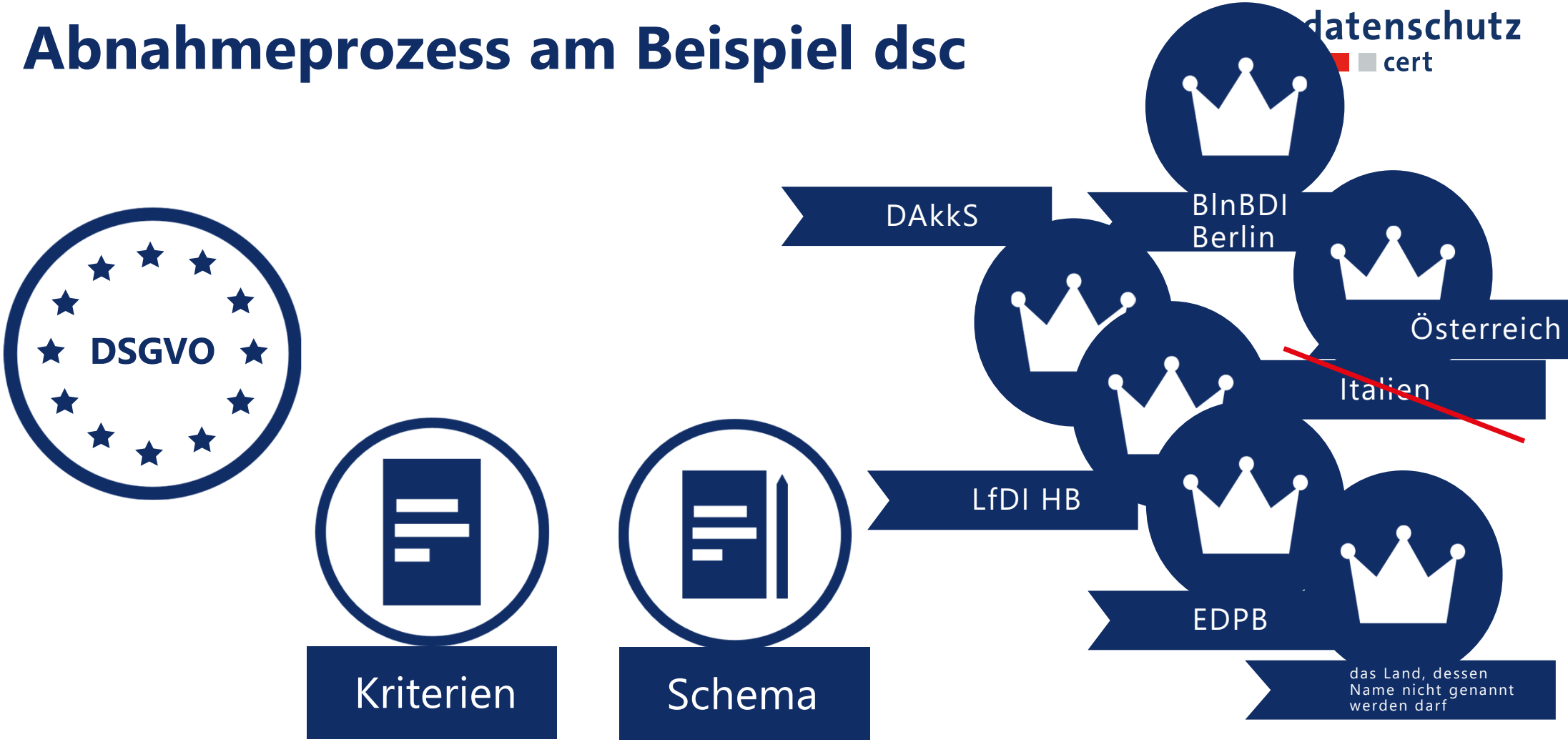
Akkreditierung von Zertifizierungsstellen durch DAkkS und zuständigen LfDI

erst danach: Erteilung von Zertifikaten

datenschutz cert

# Abnahmeprozess am Beispiel dsc

datenschutz cert



# Zugelassene Schemata

Webseite des Europäischen Datenschutz-Ausschusses

https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_de

datenschutz cert

# Register of certification mechanisms, seals and marks

datenschutz cert

| Name of the scheme | Scheme owner | Competent SA | Certification as tool for transfers | Type of criteria | |
|---|---|---|---|---|---|
| Europrivacy | European Centre for Certification and Privacy (ECCP) | LU | No | EU Data Protection Seal | Read more |
| GDPR-CARPA | LU | LU | No | National certification criteria | Read more |
| EuroPriSe | EuroPriSe Cert GmbH | DE/LDI NRW | No | National certification criteria | Read more |
| BC5701:2023 | Brand Compliance B.V. | NL | No | National certification criteria | Read more |
| AUDITOR conformity assessment | Competence Centre Trusted Cloud e.V. | DE/LDI NRW | No | National certification criteria | Read more |
| EuroPriSe European Privacy Seal | EuroPriSe Cert GmbH | DE/LDI NRW | No | EU Data Protection Seal | Read more |
| DSGVO-zt GmbH Certification criteria | DSGVO-zt GmbH | AT | No | National certification criteria | Read more |
| Catalogue of Criteria for the Certification of IT-supported processing of personal data | Datenschutz cert GmbH | DE/BE | No | National certification criteria | Read more |
| BC 5701:2024 | Brand Compliance B.V. | NL | No | EU Data Protection Seal | Read more |

# Programm und Kriterienkatalog

datenschutz cert



DSGVO
information
privacy
standard

# Webseite des Programms

datenschutz cert

Webseiten der Programmeignerin:

- http://www.ips-dsgvo-zertifikat.de
- http://www.ips-gdpr-certificate.com

Informationen für:

- Interessierte, die ein Zertifikat anstreben: Kriterienkatalog, Listung Zertifizierungsstellen
- Zertifizierungsstellen, die ‚information privacy standard' zertifizieren möchten
- Preferred Business Partner, die ‚information privacy standard' nutzen und ihre Kunden unterstützen wollen

datenschutz cert

# 3. Methodik

## Wie funktioniert denn nun der Zertifizierungsstandard ‚DSGVO – information privacy standard'?

# Was kann zertifiziert werden?

datenschutz cert

Zertifiziert werden kann konkrete Datenverarbeitung mit IT-Bezug:

„IT-gestützte Verarbeitung personenbezogener Daten“

Rolle: Verantwortliche und/oder Auftragsverarbeiter

Branchen:

- Banken und Versicherungen
- Energie- und Wasserversorgung
- Gesundheits- und Sozialwesen
- Industrie und Handel
- Marketing und Werbung
- EDV, Informationstechnologie und Telekommunikation
- Institute und Verbände
- Kultureinrichtungen
- öffentliche Stellen und öffentliche Verwaltung
- Transport, Verkehr und Logistik
- Schule, Bildung und Wissenschaft
- Ernährung

DSGVO information privacy standard

# Anwendungsbereich

datenschutz cert

**Bewertungsgegenstand (Scope) ist die Datenverarbeitung (DV): „IT-gestützte Verarbeitung personenbezogener Daten“**

charakterisiert durch folgende Elemente:

| | |
|---|---|
| Verarbeitungsvorgänge | VV |
| Datenschutz-Managementsystem | DSMS |
| Prozesse zur Realisierung der Datenverarbeitung | PRZ |
| physische Infrastruktur mit Standorten und Räumen | INFRA |
| IT-Infrastruktur | IT |
| Applikationen | APPL |
| externe Dritte | DL |

DSGVO information privacy standard

# Zertifizierungsansatz

datenschutz cert

generisch: ein Programm für alle

3 Jahre Gültigkeit, jährliche Überwachung

Evaluierung plus Zertifizierung

Evaluierung besteht aus:

- Basisprüfung
- rechtlicher Prüfung
- technischer Prüfung
- Auditierung
- Inspektion

# Aufbau des Kriterienkatalogs

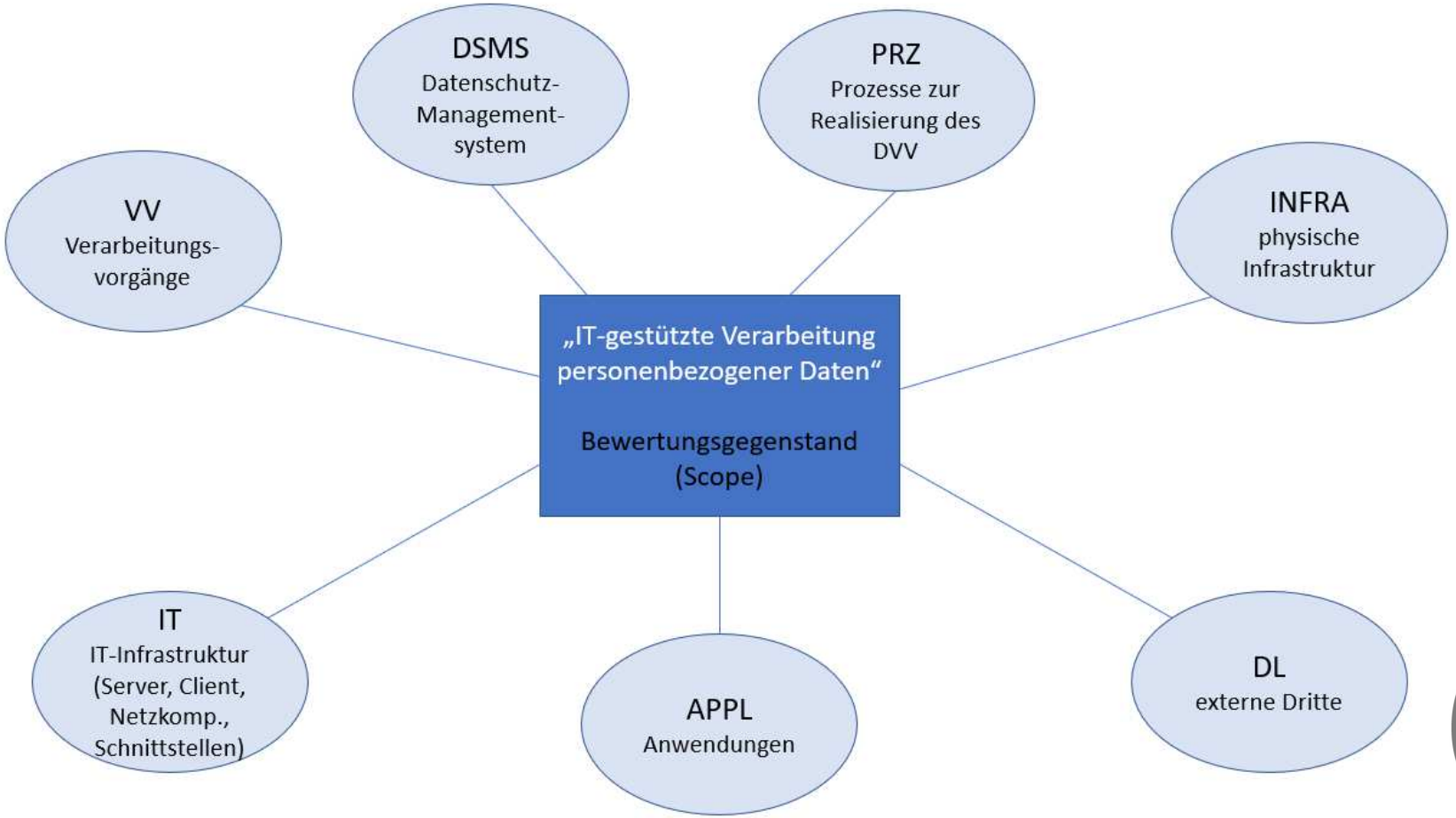
Ableitung der Anforderungen der DSGVO in prüfbare Kriterien

50 Kriterien

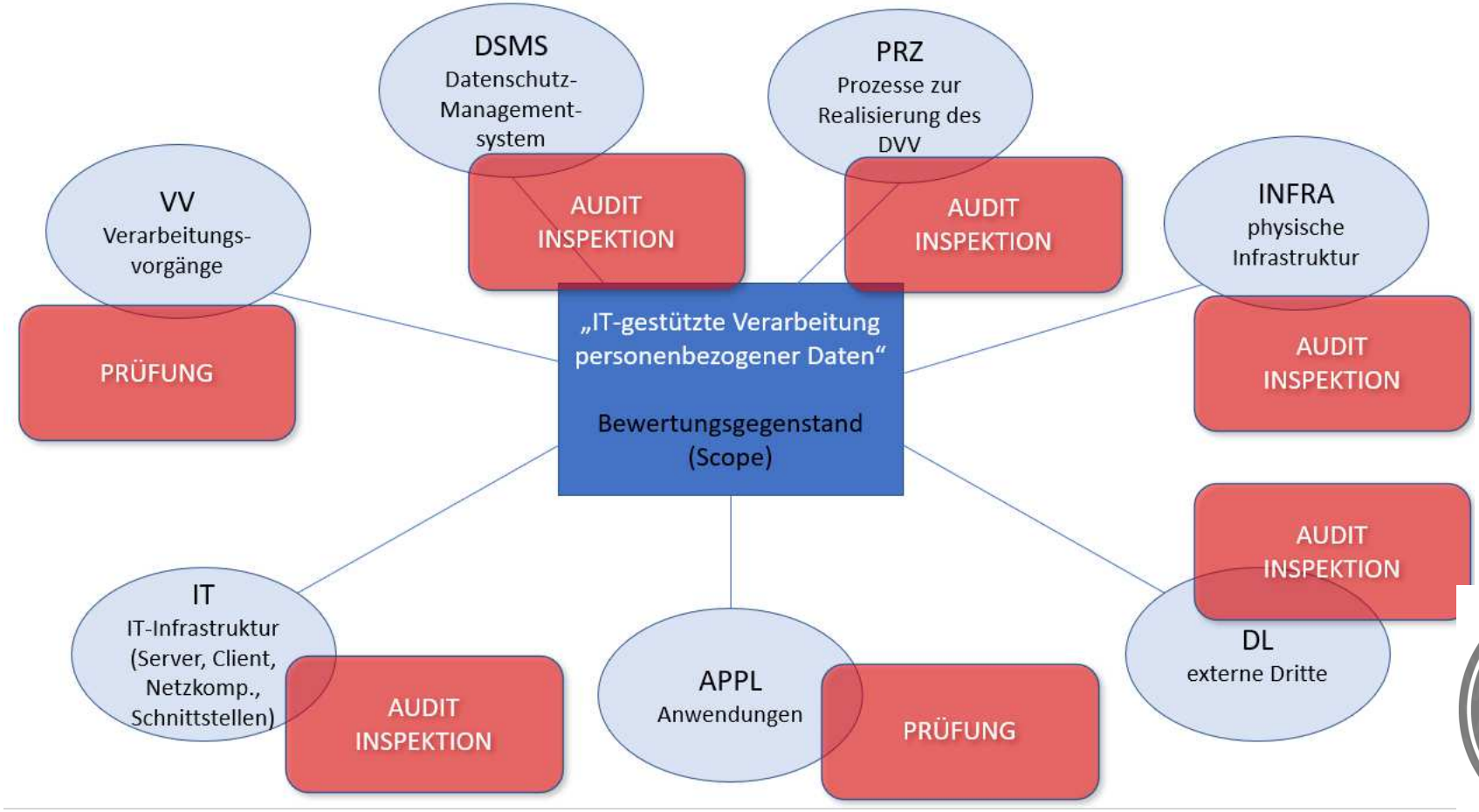
jeweils angegeben:

- Assets, auf die diese Anforderungen „wirken“
- Evaluierungsmethoden zur Überprüfung der Kriterien am jeweiligen Asset

datenschutz cert


DSMS
Datenschutz-Management-system
PRZ
Prozesse zur Realisierung des DVV
VV
Verarbeitungs-vorgänge
INFRA
physische Infrastruktur
„IT-gestützte Verarbeitung personenbezogener Daten“
Bewertungsgegenstand (Scope)
IT
IT-Infrastruktur (Server, Client, Netzkomp., Schnittstellen)
APPL
Anwendungen
DL
externe Dritte

datenschutz cert




DSGVO information privacy standard

# Weitere Dokumente zum Schema

datenschutz cert

„Anwendungshinweise, verbindliche Vorgaben und Interpretationen zum Schema (AVVIS)“:

- AVVIS-01: AVVIS-Liste: Übersicht über aktuelle Dokumente des Schemas
- AVVIS-02: Best-Practice-Kriterien: Umsetzungshinweise
- AVVIS-03: Beispiele
- AVVIS-04: Evaluations-Guide
- AVVIS-05: Korrigendum

DSGVO information privacy standard

datenschutz cert

# 4.

## Die Kriterien

Jetzt platze ich fast vor Neugier. Was sind denn nun diese berühmten ips-Kriterien?

# Übersicht über Kriterien

datenschutz cert

P.1 Zulässigkeit der Datenverarbeitung

P.2 Grundsätze

P.3 Pflichten des Kunden

P.4 Auftragsverarbeitung

P.5 Technisch-organisatorische Maßnahmen

P.6 Datenschutz-Management

P.7 Datenverarbeitung außerhalb der EU

P.8 Betroffenenrechte

DSGVO information privacy standard

# Beispiel Kriterium P.1.1 I

### 4.1.1. P.1.1 Identifikation Grundlagen

datenschutz cert

#### Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, über das sichergestellt ist, dass für die Verarbeitungsvorgänge (VV) eine vollständige Übersicht der relevanten Grundlagen aktuell vorliegt.

Insbesondere sind bei der Identifikation folgende Grundlagen relevant:

- DSGVO;
- einschlägige Rechtsgrundlagen aus nationalen Konkretisierungen der DSGVO auf Basis der Öffnungsklauseln;
- das Konformitätsbewertungs- bzw. Zertifizierungsprogramm mit dem vorliegenden Kriterienkatalog.

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss eine begründete Analyse der Rechtsgrundlagen inklusive relevantem Recht der Mitgliedsstaaten und der Anwendbarkeit der Rechtsgrundlagen für den Zertifizierungsgegenstand vorlegen.

Die Übersicht der relevanten Grundlagen muss dokumentiert vorliegen. Die identifizierten Grundlagen müssen jeweils exakt spezifiziert sein.

#### Verweis DSGVO

Art. 2 DSGVO

Art. 3 DSGVO

Art. 6 DSGVO

Art. 9 DSGVO

DSGVO information privacy standard

# Beispiel Kriterium P.1.1 II

datenschutz cert

## Nachweise

Verfahrens-, Prozessbeschreibungen

Übersicht über rechtliche Grundlagen

## Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

## Zielobjektkategorie

DSMS

VV

## Evaluatordisziplin

Evaluator (Recht)

## Evaluierungsmethode

Auditierung für die Zielobjektkategorie DSMS, ergänzend analysiert der Evaluator insbesondere, ob gilt:

- Übersicht über rechtliche Grundlagen liegt vor und ist aktuell
- es ist ein Prozess etabliert, um die Übersicht aktuell zu halten

Prüfung (rechtl.) für die Zielobjektkategorie VV

DSGVO information privacy standard

# P.1 Zulässigkeit der Datenverarbeitung

datenschutz cert

- P.1.1 Identifikation Grundlagen
- P.1.2 Rechtsgrundlage Vertrag
- P.1.3 Rechtsgrundlage berechtigtes Interesse
- P.1.4 Rechtsgrundlage Einwilligung
- P.1.5 Rechtsgrundlage rechtliche Verpflichtung
- P.1.6 Rechtsgrundlage lebenswichtige Interessen
- P.1.7 Rechtsgrundlage öffentliches Interesse
- P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten
- P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten
- P.1.10 Datenverarbeitung im Auftrag

# P.2 Grundsätze

datenschutz cert

- P.2.1 Privacy-by-Design (Datenschutz durch Technikgestaltung)
- P.2.2 Privacy-by-Default (Datenschutzfreundliche Voreinstellungen)
- P.2.3 Zweckbindung
- P.2.4 Datenminimierung
- P.2.5 Richtigkeit
- P.2.6 Speicherbegrenzung
- P.2.7 Treu und Glauben

# P.3 Pflichten des Kunden

datenschutz cert

- P.3.1 Informationspflichten des Kunden

# P.4 Auftragsverarbeitung

datenschutz cert

- P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag)
- P.4.2 Umsetzung der Maßnahmen gem. AV-Vertrag
- P.4.3 Audit

# P.5 Technisch-organisatorische Maßnahmen

datenschutz cert

- P.5.1 Festlegung geeign. Maßnahmen
- P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte)
- P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der System-zugänge)
- P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe)
- P.5.5 Transportkontrolle (Vertraulichkeit und Integrität auf Transport-Ebene)
- P.5.6 Trennungskontrolle
- P.5.7 Eingabekontrolle
- P.5.8 Verfügbarkeitskontrolle
- P.5.9 Pseudonymisierung / Anonymisierung
- P.5.10 Überprüfung, Bewertung und Evaluierung

# P.6 Datenschutz-Management

datenschutz cert

- P.6.1 Fortlaufende Datenschutz-Kontinuität
- P.6.2 Datenschutzbeauftragter
- P.6.3 Verpflichtung auf Vertraulichkeit / Schulungen
- P.6.4 Verzeichnis von Verarbeitungstätigkeiten
- P.6.5 Datenschutz-Folgenabschätzung
- P.6.6 Meldung von Datenschutzverletzungen
- P.6.7 Zusammenarbeit mit Aufsichtsbehörden

# P.7 Datenverarbeitung außerhalb der EU

datenschutz cert

- P.7.1 Datenübermittlung in Drittstaaten
- P.7.2 Vertreter innerhalb der EU

# P.8 Betroffenenrechte

datenschutz cert

- P.8.1 Recht auf Auskunft
- P.8.2 Recht auf Berichtigung
- P.8.3 Recht auf Löschung ("Recht auf Vergessenwerden")
- P.8.4 Recht auf Einschränkung
- P.8.5 Mitteilungspflicht
- P.8.6 Recht auf Datenübertragbarkeit
- P.8.7 Recht auf Widerspruch
- P.8.8 Recht auf Widerruf bei Einwilligung
- P.8.9 Automatisierte Entscheidungen / Profiling
- P.8.10 Beschwerde-Management

datenschutz cert

# 5.

# Fazit

Ende gut? Alles gut?

# DSGVO – information privacy standard – der Standard für DSGVO-Zertifikate

Gesetzlicher Rahmen ist da!

Die Nachfrage ist da!

DSGVO – information privacy standard ist da!

Vision:

- *ein* einheitliches DSGVO-Zertifikat
- Gemeinschaft von vielen ips-Zert'Stellen und Partnern
- stärkt Bekanntheit, Kompatibilität und Standing

www.ips-DSGVO-Zertifikat.de

datenschutz cert


datenschutz cert

**Dr. Sönke Maseberg**

datenschutz cert GmbH

**E-Mail** smaseberg@datenschutz-cert.de
**T** +49 421 69 66 32-0

**Geschäftsführer und Leiter der Zertifizierungsstelle**