# Merkblatt zu Akkreditierungsverfahren im Datenschutz

**M Datenschutz**

18. Juli 2022

## Geltungsbereich:

Dieses Merkblatt enthält Informationen für alle Konformitätsbewertungsstellen, die Prüf-, Inspektions- oder Zertifizierungsleistungen zur Bestätigung der Einhaltung von Datenschutzanforderungen erbringen wollen und ihren Sitz in Deutschland haben.

Abgestimmt mit dem Arbeitskreis (AK) Zertifizierung der Datenschutzkonferenz (DSK).

## Zum Inhalt von Merkblättern

- Merkblätter der DAkkS sind keine Regeln.
- Merkblätter der DAkkS generieren keine neuen Anforderungen. Sie können gleichwohl bestehende Anforderungen aus Gesetzen, Normen oder Regeln erklären und insofern wiederholen.
- Merkblätter der DAkkS informieren Antragsteller, akkreditierte Konformitätsbewertungs-stellen und weitere an der Akkreditierung interessierte Kreise – wo erforderlich oder sinn-voll – über das Akkreditierungsverfahren, welches auf der Basis der DIN EN ISO/IEC 17011 sowie ggf. weiterer Anforderungsdokumente durchzuführen ist.
- Merkblätter der DAkkS erläutern – wo erforderlich – die Inhalte der DIN EN ISO/IEC 17011 und informieren darüber, wie die DAkkS diese Norm anwendet. Merkblätter unterstützen somit das einheitliche Verständnis der Norm auf Seiten der Konformitätsbewertungsstellen und die einheitliche Anwendung durch die DAkkS einschließlich Ihrer Begutachter und Fachexperten.
- Merkblätter der DAkkS erläutern – wo erforderlich oder sinnvoll – die Inhalte der harmonisierten Normen sowie ggf. weiterer Dokumente, die Anforderungen an Konformitätsbewertungsstellen, deren Tätigkeiten und Verfahren beinhalten und unterstützen somit ein einheitliches Verständnis und eine einheitliche Anwendung dieser Dokumente im Akkreditierungsverfahren und durch akkreditierte Konformitätsbewertungsstellen.
- Merkblätter orientieren sich i. d. R. an der Struktur der relevanten harmonisierten Normen. Es ist jedoch auch möglich, Merkblätter zu einzelnen Sektoren oder Bereichen zu veröffentlichen, um den interessierten Lesern einen Überblick über Akkreditierungen in einem speziellen Sektor oder Bereich zu verschaffen.
- Merkblätter werden bei Bedarf fortgeschrieben und mit dem jeweils aktuellen Ausgabe-stand auf der Website der DAkkS veröffentlicht.
- Merkblätter erheben zu keinem Zeitpunkt den Anspruch auf Vollständigkeit in dem Sinne, dass alle Punkte in einem Gesetz oder einer Norm adressiert werden.

## Inhaltsverzeichnis

## I Geltungsbereich im Datenschutz

Dieses Merkblatt enthält Informationen für alle Konformitätsbewertungsstellen, die Prüf-, Inspektions- oder Zertifizierungsleistungen zur Bestätigung der Einhaltung von Datenschutzanforderungen erbringen wollen und ihren Sitz in Deutschland haben.

Zu unterscheiden sind hierbei:

1 Konformitätsbewertungsstellen, die Zertifizierungsleistungen gemäß EN ISO/IEC 17065 i.V.m. Art 43 Abs. 1 S. 1 der Verordnung (EU) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO) i.V.m. § 39 Bundesdatenschutzgesetz (BDSG) erbringen und

2 Konformitätsbewertungsstellen, die beigestellte Evaluierungen im Datenschutz anbieten, die im Rahmen einer Zertifizierung nach DS-GVO angerechnet werden sollen oder Konformitätsbewertungsstellen, die sonstige Konformitätsaussagen in Bezug auf Datenschutz formulieren und nicht nach EN ISO/IEC 17065 akkreditiert werden können.

Unter den Voraussetzungen der grenzüberschreitenden Akkreditierung gemäß Art. 7 VO (EG) Nr. 765/2008 und EA 2/13 (Cross Frontier Accreditation) [UP 731] können auch Stellen mit Sitz in der EU und dem EWR in Deutschland akkreditiert werden. In diesem Fall kann dieses Merkblatt auch für diese Stellen angewendet werden. Stellen mit Sitz in Drittstaaten beachten diese Reglungen, wenn diese Zertifizierungen zur Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen im Sinne von Art. 46 Abs. 2 lit. e) oder f) DS-GVO erbringen und durch die DAkkS und die zuständigen unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (Datenschutz-Aufsichtsbehörde) im Sinne von Art. 55 und 56 DS-GVO hierfür akkreditiert werden sollen.

Sofern in diesem Dokument nichts anderes festgelegt wird, gelten zur Auslegung der Regelungen der DS-GVO, des BDSG und des Akkreditierungsstellengesetzes (AkkStelleG) für den festgelegten Geltungsbereich dieses Merkblatts, alle horizontalen Akkreditierungsregelungen der DAkkS und die nachfolgenden Festlegungen, sowie alle Festlegungen der zuständigen Datenschutz-Aufsichtsbehörden im Sinne von Art. 55 und 56 DS-GVO, auch wenn diese hier nicht ausdrücklich referenziert werden.

### 1. Konformitätsbewertungsstellen nach EN ISO/IEC 17065 im Datenschutz

Für Konformitätsbewertungsstellen gemäß EN ISO/IEC 17065 i.V.m. Art. 43 Abs. 1 S. 1 DS-GVO i.V.m. § 39 BDSG erfolgt die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Datenschutz-Aufsichtsbehörde auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS). Die §§ 2 Abs. 3 S. 2, § 4 Abs. 3 und § 10 Abs. 1 S. 1 Nr. 3 AkkStelleG finden mit der Maß-gabe Anwendung, dass der Datenschutz als ein dem Anwendungsbereich des § 1 Abs. 2 S. 3 AkkStelleG unterfallender Bereich gilt.

## 2. Konformitätsbewertungsstellen für beigestellte Evaluierungen im Datenschutz und für sonstige Konformitätsaussagen zum Datenschutz

Beigestellte Evaluierungen, die im Rahmen der Zertifizierung nach Art. 42, 43 DS-GVO angerechnet werden sollen, können gemäß Abschnitt 6.2.2.1 EN ISO/IEC 17065 (Outsourcing) durch die Konformitätsbewertungsstelle an Evaluatoren und/oder Prüf- und Zertifizierungsstellen ausgegliedert werden, die die geltenden Anforderungen einhalten, die in den relevanten internationalen Normen und anderen Dokumenten enthalten sind. Die relevanten internationalen Normen schließen für die Prüfung ISO/IEC 17025, für die Inspektion ISO/IEC 17020, für die Durchführung von Audits von Managementsystemen ISO/IEC 17021 und für Personenzertifizierungen ISO/IEC 17024 mit ein. Für Akkreditierungsverfahren solcher Stellen und Stellen, die sonstige Konformitätsbewertungen im Datenschutz ausgeben und nicht gem. EN ISO/IEC 17065 akkreditiert werden, wendet die DAkkS im Rahmen der Akkreditierung die ergänzenden Anforderungen zur Akkreditierung gem. Art 43 Abs. 3 DS-GVO der Datenschutz-Aufsichtsbehörden entsprechend an.

### 2.1 Laborprüfung im Bereich Datenschutz

Genehmigte Zertifizierungsprogramme können gemäß Abschnitt 6.1.1 i.V.m. 7.1.1 EN ISO/IEC 17065 eine Laborprüfung als Teilprüfung fordern.

IT-Sicherheitslabore für Prüfungen im Anwendungsbereich dieses Merkblatts werden gemäß **ISO/IEC 17025** akkreditiert. Auf diese Konformitätsbewertungsaussagen darf sich eine gemäß EN ISO/IEC 17065 akkreditierte Konformitätsbewertungsstelle innerhalb der Zertifizierung stützen (Unterauftrag oder beigestellte Prüfung gemäß Abschnitt 7.4.5 EN ISO/IEC 17065).

Dies betrifft insbesondere Prüfungen nach **ISO/IEC 15408, ISO/IEC 18045, IEC 62443** (erforderlich z.B. im Anwendungsbereich smart-Grit, IoT, Industrie 4.0, Vertrauensdienste Gesetz, eIDAS-VO) etc.

Prüfberichte eines akkreditierten Labors sind keine Zertifikate im Sinne der DS-GVO und können deshalb nicht (allein) zu einer Zertifizierung der Konformität mit den Anforderungen der DS-GVO führen. Sie können nur als Teilevaluierungen Berücksichtigung finden.

Die Prüfberichte und sonstigen Bescheinigungen haben einen ausdrücklichen Hinweis zu enthalten, aus dem der Geltungsbereich und der Zweck der Laborprüfung hervorgehen.

Im Zertifizierungsprogramm ist durch die Konformitätsbewertungsstelle für Datenschutz unter Berücksichtigung der ergänzenden Anforderungen der Datenschutz-Aufsichtsbehörden genau festzulegen, wie solche Berichte als Teilevaluierung Berücksichtigung finden.

## 2.2 Zertifizierungsstelle für Managementsysteme im Datenschutz

Genehmigte Zertifizierungsprogramme können gemäß Abschnitt 6.1.1 i.V.m. 7.1.1 EN ISO/IEC 17065 als Teilprüfung fordern, dass der Verantwortliche (Art. 4 Nr. 7 DS-GVO) oder der Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) ein Managementsystem betreibt. Insbesondere können Qualitätsmanagementsysteme, Informationssicherheitsmanagementsysteme oder Business Continuity Managementsysteme (BCMS) gefordert werden. Mögliche internationale harmonisierte Managementsystemnormen sind insbesondere ISO/IEC 9001, ISO/IEC 27001, ISO 27701, ISO/IEC 27017 i.V.m. ISO/IEC 27018. Zertifizierungsstellen für Managementsysteme im Anwendungsbereich dieses Merkblatts werden gemäß **ISO/IEC 17021** akkreditiert.

Die Anforderungen an die Konformitätsbewertungstätigkeit der nach EN ISO/IEC 17021 akkreditierten Stelle, werden näher bestimmt durch die Norm ISO/IEC 27006 und als Anwendungshilfe ISO/IEC 17021-6 (BCM)

Die Anforderungen an ein Zertifizierungsprogramm für Managementsysteme ergeben sich aus ISO/IEC 17021-1 Abschnitt 9.1.1 i.V.m. Anhang E sowie den Konkretisierungen in der relevanten Normen ISO/IEC 27006 und ISO/IEC 27006-2. Das Programm muss nur dort Regelungen festlegen, soweit diese nicht bereits durch die Norm abgedeckt sind. Zu beachten ist, dass die normativen Vorgaben im Hinblick auf die gesetzlichen Mindestanforderungen der DSK anzupassen sind. Das betrifft insbesondere die Qualifikationsanforderungen in Tz. 7.1.2.1 und 7.1.2.2 der ISO/IEC 27006-2. Die DAkkS-Regel zur Prüfung und Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme gibt Hinweise zum Vorgehen. Das Programm der Zertifizierungsstelle muss Prüfkriterien für die gesetzlichen Anforderungen der DSGVO konkretisieren (wie in Anhang D der ISO/IEC 27701 dargestellt) die aufzeigen, aus welchen objektiven Nachweisen im Rahmen des Audits geschlossen werden kann, dass das Managementsystem alle relevanten Anforderungen des Datenschutz unterstützt. Dabei ist darzulegen, inwieweit die Prozesse des Kunden die Zielkonflikte zwischen Informationssichert und Datenschutz berücksichtigen und in Prozesse implementiert haben.

Zertifikate einer akkreditierten Zertifizierungsstelle nach ISO/IEC 17021 sind keine Zertifikate im Sinne der DS-GVO. Die Konformitätsaussage im Zertifikat muss sich auf die Bezeichnung der internationalen Managementsystemnorm ohne jeden Bezug auf die DS-GVO beschränken. Das Zertifikat für ein Managementsystem nach ISO/IEC 27001 kann gemäß Anlage 3 mit dem Konformitätszusatz zur ISO/IEC 27701 ergänzt werden. Eine gesonderte Ausgabe von Zertifikate zur ISO/IEC 27701 ist irreführend und unzulässig. Das Zertifikat und die Prüfberichte und sonstigen Bescheinigungen haben einen ausdrücklichen Hinweis zu enthalten, aus dem sich der eingeschränkte Geltungsbereich und der Zweck der Managementzertifizierung hervorgehen.

Im Zertifizierungsprogramm ist durch die Konformitätsbewertungsstelle für Datenschutz unter Berücksichtigung der ergänzenden Anforderungen der Datenschutz-Aufsichtsbehörden genau festzulegen, wie solche Berichte als Teilevaluierung Berücksichtigung finden.

## 2.3 Datenschutzinspektionsstelle

Genehmigte Zertifizierungsprogramme können gemäß Abschnitt 6.1.1 i.V.m. 7.1.1 EN ISO/IEC 17065 als Teilprüfung fordern, dass der Verantwortliche (Art. 4 Nr. 7 DS-GVO) oder der Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) Inspektionsberichte vorlegt.

Gegenstand solcher Inspektionen durch Überwachungsstellen können auch bestimmte auftragsbezogene Datenschutzanforderungen im Rahmen von Vergabebedingungen sein, die dann als akkreditierter Test-/und Inspektionsberichte gem. Art. 44 der Vergaberichtlinie (Richtlinie (EU) 2014/24 vom 26.02.2014 über die öffentliche Auftragsvergabe bzw. § 33 Vergabeverordnung (VgV) verwendet werden können.

Ein weiterer Anwendungsbereich für akkreditierte Inspektionsleistungen ist die laufende Inspektion im Unterauftrag einer nach EN ISO/IEC 17065 akkreditierten Konformitätsbewertungsstelle zur Nachweisführung der Einhaltung von geeigneten technischen und organisatorischer Maßnahmen gem. Art. 32 Abs. 1 lit. a) bis d) DS-GVO in **komplexen IT-Systemen** (insbesondere Cloud-Systeme, komplexe smart-Grid Anwendungen/intelligente Verkehrssysteme/Big-Data Anwendungen, etc.). Auf diese Konformitätsbewertungsaussagen (Inspektionsbericht) darf sich eine gemäß EN ISO/IEC 17065 akkreditierte Konformitätsbewertungsstelle innerhalb der Zertifizierung stützen.

Inspektionsstellen im Anwendungsbereich dieses Merkblatts werden gemäß **ISO/IEC 17021** akkreditiert.

Inspektionsberichte einer akkreditierten Inspektionsstelle sind keine Zertifikate im Sinne der DS-GVO und können deshalb nicht (allein) zu einer Zertifizierung der Konformität mit den Anforderungen der DS-GVO führen. Die Inspektionsberichte und sonstigen Bescheinigungen haben einen ausdrücklichen Hinweis zu enthalten, aus dem der eingeschränkte Geltungsbereich und der Zweck der Inspektionsleistung hervorgehen.

Im Zertifizierungsprogramm ist durch die Konformitätsbewertungsstelle für Datenschutz unter Berücksichtigung der ergänzenden Anforderungen der Datenschutz-Aufsichtsbehörden genau festzulegen, wie solche Berichte als Teilevaluierung Berücksichtigung finden.

## 2.4 Personenzertifizierungsstelle im Datenschutz

Genehmigte Zertifizierungsprogramme können gemäß Abschnitt 6.1.1 i.V.m. 7.1.1 EN ISO/IEC 17065 als Teilprüfung fordern, dass das Personal des Verantwortlichen (Art. 4 Nr. 7 DS-GVO) oder des Auftragsverarbeiters (Art. 4 Nr. 8 DS-GVO) zur Gewährleistung eines angemessenen Datenschutzniveaus bestimmte personelle Kompetenzen nachweist. Das betrifft insbesondere Personenzertifikate zum Kompetenznachweis für den Datenschutzbeauftragten beim Auftragsverarbeiter oder beim Verantwortlichen. Auf Konformitätsbewertungsaussagen einer nach ISO/IEC 17024 akkreditierten Personenzertifizierungsstelle darf sich eine gemäß EN ISO/IEC 17065 akkreditierte Konformitätsbewertungsstelle innerhalb der Zertifizierung stützen.

Personenzertifizierungsstellen werden gemäß **ISO/IEC 17024** akkreditiert.

Ein Personenzertifikat einer akkreditierten Personenzertifizierungsstelle bestätigt keine Konformität des Auftragsverarbeiters oder des Verantwortlichen. Es bestätigt allein die Kompetenz einer natürlichen Person mit einem genehmigten Personenzertifizierungsprogramm.

Die Personenzertifikate haben einen ausdrücklichen Hinweis zu enthalten, aus dem der eingeschränkte Geltungsbereich und der Zweck der Personenzertifizierung hervorgehen.

Die Anforderungen an ein Personenzertifizierungsprogramm ergeben sich aus Abschnitt 8 ISO/IEC 17024.

## II Ablauf und Hinweise zum Akkreditierungsverfahren (IAF/EA-Level 1)

(Abschnitt 7 der ISO/IEC 17011 – Akkreditierungsverfahren)

### 1. Vorgezogene Prüfung von Zertifizierungsprogrammen und Genehmigung von Zertifizierungskriterien

Zur Vorbereitung der Akkreditierung muss die Zertifizierungsstelle oder der Programmeigner ein Zertifizierungsprogramm erstellen und durch die DAkkS gemäß Abschnitt 4.6.3 EN ISO/IEC 17011 auf Eignung prüfen lassen vgl. DAkkS Regel zur Prüfung und Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme. Dieses Zertifizierungsprogramm enthält als wesentlichen Teil die Zertifizierungskriterien zur Umsetzung der datenschutzrechtlichen Anforderungen, die gem. Art. 57 Abs. 1 lit. n) DS-GVO i.V.m. Art. 42 Abs. 5 DS-GVO entweder von der zu-ständigen Datenschutz-Aufsichtsbehörde genehmigt werden oder (i.d.R. über die zuständige Aufsichtsbehörde) dem Europäischen Datenschutzausschuss zur Genehmigung bzw. Billigung gemäß Art. 63, 64 Abs. 1 lit. c) DS-GVO zu übermitteln sind.

Werden die Kriterien gemäß Art. 57 Abs. 1 lit. n) DS-GVO i.V.m. Art. 42 Abs. 5 DS-GVO nur von der zuständigen Datenschutz-Aufsichtsbehörde genehmigt, so übermittelt sie diese Kriterien gemäß Art. 43 Abs. 6 Satz 2 DS-GVO dem Europäischen Datenschutzausschuss.

Die Programmprüfung bei der DAkkS erfolgt gemäß der Regel zur Prüfung der Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme. Bestandteil des Verfahrens ist die Übermittlung des Zertifizierungsprogramms an die zuständige Datenschutz-Aufsichtsbehörde zur Genehmigung der Zertifizierungskriterien gem. Art. 57 Abs. 1 lit. n) DS-GVO i.V.m. Art. 42 Abs. 5 DS-GVO. Nach erfolgreicher Genehmigung der Zertifizierungskriterien und der Beseitigung sonstiger Abweichungen wird das Programmprüfungsverfahren durch einen feststellenden Bescheid des Programmausschusses der DAkkS abgeschlossen.

Die Genehmigung der Zertifizierungskriterien durch die zuständige Aufsichtsbehörde erfolgt auf Antrag der Zertifizierungsstelle. Hierbei handelt es sich um ein eigenständiges Genehmigungsverfahren der zuständigen Datenschutz-Aufsichtsbehörde, das unabhängig vom Akkreditierungsverfahren der DAkkS ist. Den Antrag auf Genehmigung nimmt die DAkkS im Rahmen der Programm-prüfung entgegen und leitet diesen an die zuständige Datenschutz-Aufsichtsbehörde weiter.

Da jede Akkreditierung mithin die Existenz eines Zertifizierungsprogramms mit genehmigten Kriterien voraussetzt, um in der Urkundenanlage den Geltungsbereich der Akkreditierung bestimmen zu können, muss der Antragsteller mit dem Antrag auf Akkreditierung angeben, für welche öffentlich verfügbaren, genehmigten Zertifizierungsprogramme oder Gütesiegel eine Akkreditierung beantragt wird.

Weitere Hinweise sind auf der Webseite der DAkkS im Akkreditierungs-Bereich unter „Programme der Konformitätsbewertung“ verfügbar.

## 2. Hinweise zum Konformitätsbewertungsprogramm

### 2.1 Festlegung der Kriterien, Prüfsystematik und -methodik

Ergänzend zu Abschnitt 6.5.1. der EN ISO/IEC 17067 (Programmtyp 6, Tabelle 1) sind bei der Erstellung von Zertifizierungsprogrammen für Zertifizierungsstellen nach EN ISO/IEC 17065 - neben den einschlägigen Leitlinien[1] des Europäischen Datenschutzausschusses in der jeweils aktuellen Fassung – auch die Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in der jeweils aktuellen Fassung zu beachten, die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes der Länder (DSK) erstellt wurden.

Folgende Punkte sind mindestens in einem Zertifizierungsprogramm obligatorisch darzulegen[2]:

- Eine Beschreibung eines Zertifizierungsgegenstands im Bereich seiner Anwendung der als DS-GVO-konforme Verarbeitung personenbezogener Daten mittels einer oder mehrerer Verarbeitungstätigkeiten durch
  - ein System,
  - einen Prozess, oder
  - einen Dienst

  realisiert ist, wobei
  - die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten, insbesondere unter Berücksichtigung von Art. 5 DS-GVO,
  - die Rechtmäßigkeit der Verarbeitung personenbezogener Daten unter Angabe der Rechtsgrundlage, vgl. Art. 6 DS-GVO ggf. in Verbindung mit anderen einschlägigen Rechtsgrundlagen,
  - die [tatsächlich] verarbeiteten Daten, insbesondere personenbezogene Daten ggf. unter Berücksichtigung von Art. 9 DS-GVO, und
  - das Einsatzgebiet hinsichtlich seiner Anwendung im Zusammenhang mit
    - Pflichten eines Verantwortlichen gemäß Art. 24 Abs. 3 DS-GVO,
    - Pflichten eines Auftragsverarbeiters gemäß Art. 28 Abs. 5 DS-GVO,
    - einer datenschutzfreundlichen Technikgestaltung gemäß Art. 25 Abs. 3 DS-GVO,
    - Sicherheit der Verarbeitung gemäß Art. 32 Abs. 3 DS-GVO unter Darstellung angemessener und geeigneter Maßnahmen und/oder

[1] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Version 3.0 vom 4. Juni 2019; Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), Version 3.0 vom 4. Juni 2019.

[2] Die Darstellung der hier im Folgenden aufgezählten Punkte impliziert keine Vorgaben bzgl. der Rei-henfolge ihrer Berücksichtigung bei der Umsetzung in Zertifizierungsprogrammen.

- geeigneter Garantien gemäß Art. 46 Abs. 2 lit. f

darzustellen sind;

- eine Festlegung von Prüfkriterien und eine Beschreibung der Prüfsystematik und -methodik, mittels denen die Prüfkriterien geprüft, deren Einhaltung nachgewiesen werden kann und die DS-GVO-Konformität des Zertifizierungsgegenstands im Geltungszeitraum der Zertifizierung gewährleistet ist, wobei diese für einen Zertifizierungsgegenstand genehmigt sein müssen (zu genehmigende Zertifizierungskriterien gemäß Art. 42 Abs. 5 DS-GVO);
- die Nachweise/Zugänge/Anforderung von Prüfnachweisen als begleitende datenschutzrechtliche Prozesse bei Durchführung
  - einer Zertifizierung oder anlassbezogenen Re-Zertifizierung durch die Zertifizierungsstelle,
  - eines Audits durch die Zertifizierungsstelle beim Zertifizierungsinhaber und/oder
  - eine eigenständige Kontrolle durch und beim Zertifizierungsinhaber oder
  - einer Prüfung durch die zuständigen Datenschutzaufsichtsbehörden

  in Abhängigkeit des Zertifizierungsgegenstands unter Angabe des Turnus und/oder möglicher Anlässe, die eine Re-Zertifizierung, ein Audit, eine Kontrolle oder eine datenschutz-rechtliche Prüfung notwendig machen, wobei die Festlegung von Turnus und notwendiger Prüfnachweise im Kontext einer Prüfung der Datenschutzaufsichtsbehörde obliegt;
- die Kriterien zur Prüfung der Risikobetrachtung[3] durch den Zertifizierungsinhaber sowie ei-ne Darstellung zum Vorgehen bei deren Anwendung in Abhängigkeit des Zertifizierungsgegenstands
  - sowohl zum Zeitpunkt der Zertifizierung i. V. m. einer etwaig erforderlichen Datenschutzfolgenabschätzung nach den Vorgaben des Art. 35 DS-GVO;
  - als auch im Geltungszeitraum der erteilten Zertifizierung;
  - die in einem Datenschutzmanagement vorgehalten werden und bei einer daten-schutzrechtlichen Prüfung vorgelegt werden müssen;
- die Nachweise/Zugänge/Anforderung zur Gewährung der Rechte betroffener Personen einschließlich der Informationspflichten im Einsatzgebiet des Zertifizierungsgegenstands;
- den Umgang mit Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 und Art. 34 DS-GVO;
- die Nachweise/Zugänge zu einer Beschwerdestelle, so dass betroffene Personen ihre Rechte geltend machen können;

[3] Die Kriterien zur Prüfung der Risikobetrachtung sind Basis gegen die zu prüfen ist. Parallel dazu ist im Zertifizierungsprogramm eine entsprechende Prüfsystematik und -methodik darzustellen. Diese Prüfsystematik und -methodik muss sicherherstellen, dass u.a. die Ergebnisse der Risikobewertung durch die Datenschutzaufsichtsbehörden beurteilt werden können.

- festgelegte Überwachungsart und -intervall in Abhängigkeit des Zertifizierungsgegenstands mit Prüfsystematik und -methodik, mittels denen die Anforderungen/Kriterien geprüft und nachgewiesen werden;
- dazugehörige Dokumentationen, die bei einer datenschutzrechtlichen Prüfung vorgelegt werden müssen.
- Das Konformitätsbewertungsprogramm muss ein Musterzertifikat enthalten, dass die Mindestinformationen gem. Anlage 1 enthält, um eine Prüfung durch die DAkkS und die zuständige Datenschutz-Aufsichtsbehörde zu ermöglichen (Anlage 1 – Musterzertifikat).

Zudem gelten für Zertifizierungsprogramme die ergänzenden Anforderungen der DSK.

### 2.2 Transferkonzept zur DS-GVO für Bestandszertifikate

Für die Überführung/Anerkennung von bereits bestehenden Zertifikaten aus dem Bereich Datenschutz oder Datensicherheit im Rahmen der Konformitätsbewertung zur DS-GVO kann die Konformitätsbewertungsstelle ein Transferkonzept im Zertifizierungsprogramm darlegen. Dieses wird durch die Datenschutz-Aufsichtsbehörden und die DAkkS im Rahmen der Programmprüfung und Genehmigung der Kriterien geprüft und genehmigt.

Grundsätzlich sind beim Transferkonzept die ergänzenden Anforderungen zur Akkreditierung der Datenschutz-Aufsichtsbehörden sowie die in diesem Merkblatt beschriebenen Regelungen für beigestellte Evaluierungen zu beachten.

Das Transferkonzept muss nachweisen, dass die geprüften Prüfobjekte für die Datenverarbeitungstätigkeiten sowohl im Hinblick auf die Kriterien als auch im Hinblick auf die Evaluierungsarten und -methoden vollständig gleichwertig zu den Festlegungen des Zertifizierungsprogramms durch-geführt wurden.

### 2.3 Akkreditierungsbereiche (Scopes)

Entsprechend der ergänzenden Anforderungen zur Akkreditierung gem. Art. 43 Abs. 3 DS-GVO i.V.m. EN ISO/IEC 17065 der Datenschutz-Aufsichtsbehörden werden in diesem Dokument keine Geltungsbereiche (Scopes) für die Akkreditierung von Zertifizierungsstellen vorgegeben. Die Zertifizierungsstellen müssen jedoch mit Stellung des Antrags auf Programmprüfung den Geltungsbereich des Zertifizierungsprogramms festlegen und genau beschreiben.

## 3. Befristung der Akkreditierung, Wiederholungsbegutachtung und Überwachung

(Zu Abschnitt 7.11 der EN ISO/IEC 17011 i.V.m. Art. 43 Abs. 7 S. 2 DS-GVO)

### 3.1 Konformitätsbewertungsstellen nach EN ISO/IEC 17065 im Datenschutz

Die Akkreditierung wird gemäß Art. 43 Abs. 4 DS-GVO auf höchstens 5 Jahre befristet.

Vor Ablauf der Akkreditierung ist ein Antrag auf Reakkreditierung zu stellen.

Die DAkkS überwacht gem. Art 43 Abs. 7 S. 2 DS-GVO gemeinsam mit den Datenschutz-Aufsichtsbehörden die Einhaltung der sich aus der EN ISO/IEC 17065 und den ergänzenden Anforderungen der Datenschutz-Aufsichtsbehörden gem. Art 43 Abs. 3 DS-GVO ergebenden Anforderungen und Verpflichtungen. Zur Aufrechterhaltung der Akkreditierung sind deshalb während des Akkreditierungszeitraums regelmäßige Überwachungsmaßnahmen erforderlich. Überwachungen definieren sich nach Abschnitt 6.1 der DIN EN ISO/IEC 17000 als sich systematisch wiederholende Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Akkreditierung.

Das Intervall, die Art und der Umfang von Überwachungsmaßnahmen werden durch die DAkkS festgelegt und basieren auf einem risikobasierten Ansatz. Es gelten die jeweils aktuellen von der DAkkS dazu festgelegten Rahmenbedingungen. Die Überwachungen werden in der Form einer Geschäftsstellenbegutachtung (Vor-Ort-Begutachtung) durchgeführt, ergänzt um planmäßige Witnessaudits.

Für die Durchführung der Witnessaudits wird auf Anhang 2 („Witnessing-Modell“) der ergänzenden Anforderungen der Datenschutz-Aufsichtsbehörden verwiesen.

### 3.2 Konformitätsbewertungsstellen für beigestellte Evaluierungen im Datenschutz und für sonstige Konformitätsaussagen zum Datenschutz

Die Akkreditierung für Konformitätsbewertungsstellen für beigestellte Evaluierungen im Datenschutz und für sonstige Konformitätsaussagen zum Datenschutz erfolgt unbefristet. Innerhalb des Akkreditierungszyklus von 5 Jahren ist eine Wiederholungsbegutachtung erfolgreich abzuschließen.

Zur Aufrechterhaltung der Akkreditierung sind während des Akkreditierungszeitraums regelmäßige Überwachungsmaßnahmen erforderlich. Überwachungen definieren sich nach Abschnitt 6.1 der DIN EN ISO/IEC 17000 als sich systematisch wiederholende Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Akkreditierung.

Das Intervall, die Art und der Umfang von Überwachungsmaßnahmen werden durch die DAkkS festgelegt und basieren auf einem risikobasierten Ansatz. Es gelten die jeweils aktuellen von der DAkkS dazu festgelegten Rahmenbedingungen. Die Überwachungen werden in der Form einer Geschäftsstellenbegutachtung (Vor-Ort-Begutachtung) durchgeführt, ergänzt um planmäßige Witnessaudits.

## III Umsetzungshinweise für Konformitätsbewertungsstellen (IAF/EA-Level 4)

### 1. Für Konformitätsbewertungsstellen nach EN ISO/IEC 17065 im Datenschutz

Gem. Art 43 Abs. 3 S. 1 DS-GVO erfolgt die Akkreditierung von Zertifizierungsstellen anhand der EN ISO/IEC 17065 und der ergänzenden Anforderungen zur EN ISO/IEC 17065, die von der gem. Art. 55 DS-GVO oder Art. 56 DS-GVO zuständigen Aufsichtsbehörde oder – gem. Art. e 63 DS-GVO – von dem Ausschuss genehmigt wurden. Diese werden durch die Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) veröffentlicht.

### 2. Für Konformitätsbewertungsstellen für beigestellte Evaluierungen im Datenschutz und für sonstige Konformitätsaussagen zum Datenschutz

Auch für beigestellte Evaluierungen und für sonstige Konformitätsaussagen zum Datenschutz gelten die ergänzenden Anforderungen zur Akkreditierung nach Art. 43 Abs. 3 DS-GVO der Datenschutz-Aufsichtsbehörden sinngemäß soweit diese auf die Akkreditierungsnorm ISO/IEC 17020, 17021, 17024, 17025 anwendbar sind. Dies betrifft insbesondere die personelle Kompetenz der Konformitätsbewertungsstellen.

## IV Glossar

| | |
|---|---|
| Anforderungen | Bezeichnet die datenschutzspezifischen Ergänzungen der gesetzlichen und normativen Anforderungen zur Akkreditierung gem. VO (EG) 765/2008 i.V.m. EN ISO/IEC 17065 gemäß Art. 43 Abs. 1 lit. b DS-GVO. |
| Akkreditierung | Akkreditierung ist die Bestätigung durch eine nationale Akkreditierungsstelle, dass eine Zertifizierungsstelle die in Normen festgelegten Anforderungen und, gegebenenfalls, zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen, erfüllt, um eine spezielle Konformitätsbewertungstätigkeit durchzuführen. |
| Akkreditierungsausschuss (AKA) | Der AKA ist ein internes Verfahrensbezogenes Entscheidungsgremium der DAkkS, dass die Akkreditierungsentscheidung auf Basis der Begutachtungsergebnisse und weiterer Erkenntnisse trifft (Verwaltungsakt). Der AKA besteht aus drei Mitgliedern. Eine positive Akkreditierungsentscheidung kann nur Einstimmig erfolgen. Für eine negative Entscheidung genügt ein negatives Votum. |
| AKA-Mitglied | AKA-Mitglieder sind sach- und fachkundige Personen, die an der Akkreditierungsentscheidung mitwirken dürfen und nicht an der Begutachtung beteiligt waren, über die der AKA im konkreten Verfahren entscheiden soll. |
| (Genehmigte) Kriterien | Genehmigte Zertifizierungskriterien im Sinne der DS-GVO sind Kriterien, die durch die Datenschutzaufsicht nach Art 57 Abs. 1 DSGVO als Teil von durch die DAkkS auf Eignung geprüften Zertifizierungsprogrammen genehmigt worden sind. |
| Kunde | Verantwortlicher oder Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft (Art. 42 Abs. 6 S. 1 DS-GVO). |
| Programmeigner | Person oder Organisation, die für die Entwicklung und Aufrechterhaltung eines bestimmten Zertifizierungspro-gramms verantwortlich ist. |
| Zertifizierungsstelle | Konformitätsbewertungsstelle als dritte Seite, die Zertifizierungsprogramme betreibt. |
| Zertifizierungsprogramm | Zertifizierungsprogramm ist ein Dokument einer Zertifizierungsstelle oder eines unabhängigen privaten oder öffentlichen Programmeigners, das für die Zertifizierungs-stellen die spezifischen Anforderungen, Regeln sowie Prüf- und Inspektionsverfahren beschreibt, die zur Konformitätsbewertung eines Produkts, Verfahrens, einer Dienst-leistung, eines Systems oder einer Person verwendet werden müssen, um die mit dem Konformitätsbewertungsnachweis (z.B. Laborwert, Analyse, Inspektionsbericht, Versuch, Zertifizierung usw.) verbundene Aussage, auf wissenschaftlich nachvollziehbare und systematische Weise treffen zu können. Auf Antrag wird die Akkreditierungsfähigkeit eines Zertifizierungsprogramms durch fest-stellenden Verwaltungsakt |

| | |
|---|---|
| | durch die DAkkS bestätigt. Teil des Zertifizierungsprogramms sind die genehmigten Kriterien. |

## V Mitgeltende Unterlagen

- Verordnung (EG) Nr. 765/2008 vom 9. Juli 2008
- Beschluss Nr. 768/2008/EG vom 9. Juli 2008
- DIN EN ISO/IEC 17000:2005
- EN ISO/IEC 17011:2004/:2017
- EN ISO/IEC 17065: 2013
- IAF/ILAC A5:11/2013
- IAF MD 2: 2007 – IAF Mandatory Document for the Transfer of Accredited Certification of Management Systems
- IAF MD 12:2016 – Accreditation Assessment of Conformity Assessment Bodies with Activities in Multiple Countries
- IAF MD 17:2015 – Witnessing Activities for the Accreditation of Management Systems Certification Bodies
- Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065 der Datenschutzkonferenz (DSK)
- Regelwerk der DAkkS, insbesondere:
  - 71 SD 0 001 Allgemeine Regeln zur Akkreditierung von Konformitätsbewertungsstellen
  - 71 SD 0 008 Begutachterwesen
  - 71 SD 0 009 DAkkS Beschwerdeverfahren
  - 71 SD 0 014 Akkreditierung von Konformitätsbewertungsstellen mit mehreren Standorten
  - 71 SD 0 016 Regel zur Prüfung und Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme
  - DAkkS Rahmenbedingungen zum risikobasierten Begutachtungs- und Überwachungs-ansatz gem. Art. 5 Abs. 1, 3 und 4 VO (EG) Nr. 765/2008 i.V.m EN ISO/IEC 17011.
- Formblätter der DAkkS, insbesondere:
  - Antrag zur Prüfung der Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme (46 FB 001)
  - Liste einzureichender Unterlagen für die Prüfung der Akkreditierungsfähigkeit neuer Konformitätsbewertungsprogramme (46 FB 002)

- Kombinierte Checkliste/Bericht Bewertung von neuen Konformitätsbewertungspro-grammen nach 71 SD 0 016 durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) (46 FB 003)
- Muster-Matrix zu Abschnitt 6.5.1. der DIN EN ISO/IEC 17067 (Antrag auf Akkreditierung (72 FB 001)
- Antrag auf Benennung durch die zuständige Datenschutz-Aufsichtsbehörde (72 FB 002)

## Musterzertifikat

Prüfstelle Logo und Anschrift

# Zertifikat

Die **Zertifizierungsstelle xxxx** bestätigt hiermit als Ergebnis der Zertifizierungsentscheidung am TT.MM.JJJJ gemäß Art. 42 Abs. 5 DS-GVO, dass

**[Antragsteller]:** <exakter Name und Anschrift des Kunden>
**[optional Niederlassungen]** <Anschrift der Niederlassungen>

die Datenverarbeitung

**[Bezeichnung EVG]** Cloud-Mailservice AJAX 4.0 gemäß Anlage 1

als **[Datenschutzrolle g. DSGVO ]** Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO / als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO innerhalb **[Geltungsbereich Regional]** D / EU / Drittland

**[Optional weitere Beschränkungen Einsatzbereich]** z.B. nur für B2B; unter **Beachtung der Nutzungsausschlüsse** gemäß Anlage 2

konform zu den Anforderungen der EU Verordnung 2016/679 (DS-GVO) und den zusätzlichen Anforderungen der Datenschutzaufsichtsbehörden betreibt und innerhalb der Laufzeit des Zertifikats auf Konformität überwacht wird.

Die Gründe für die Erteilung des Zertifikats wurden der Datenschutzaufsichtsbehörde (xxx) gemäß Art 43 Abs. 5 DS-GVO am TT.MM.JJJJ mitgeteilt.

| | | |
|---|---|---|
| Prüfgrundlagen | [Name Programm] akkreditiertes Konformitätsbewertungsprogramm V1.2<br>[Name Kriterienkatalog] Von der Datenschutzaufsichtsbehörde xxx genehmigte Kriterien V 1.2. | |
| Zertifikats-ID/-Nummer: | XXX Zertifikatsnummer von der Prüfstelle | |
| letzter Audittag vor Ort: | <tt.mm.jjjj> /Berichtsnummer/Datum | |
| Überwachung | nächste geplante Überwachung bis spätestens <tt.mm.jjjj> | |
| Datum der Ausstellung | <tt.mm.jjjj> | Laufzeit bis <tt.mm.jjjj> max. 3 Jahre> |

Unterschrift/Benannter Entscheider der KBS

D-XX-YYYYY-ZZ-NN

zur Verwendung gemäß SymbolVO und DAkkS-Regel 71 SD 0 011

DAkkS Deutsche Akkreditierungsstelle

## Musterzertifikat mit Konformität zur ISO/IEC 27001 mit Deklaration der ISO/IEC 27701

Prüfstelle Logo und Anschrift

# Zertifikat

Die **Zertifizierungsstelle xxxx** bestätigt hiermit als Ergebnis der Zertifizierungsentscheidung am TT.MM.JJJJ gemäß DIN EN ISO/IEC 17021-1, dass der

**[Antragsteller]:** <exakter Name und Anschrift des Kunden>
**[optional Niederlassungen]** <Anschrift der Niederlassungen>

ein

## Informationssicherheitsmanagementsystem gemäß DIN EN ISO/IEC 27001

für den IT-Verbund
**[Bezeichnung EVG/ Geltungsbereich des ISMS, [ ggf. Anlage 1]**
**[SOA in Version]** gemäß [**Anlage 2]**

als **[**Verantwortlicher / Auftragsverarbeiter [Datenschutzrolle]] konform zu den Anforderungen der DIN EN ISO/IEC 27001 betreibt und dieses zertifizierte Managementsystem die zusätzlichen Maßnahmen für eine Datenschutzmanagementsystem gemäß ISO/IEC 27701 erfüllt und durch die Zertifizierungsstelle in der Laufzeit des Zertifikats überwacht wird.

Dieses Zertifikat bestätigt keine Konformität zur DSGVO.

| | | |
|---|---|---|
| Prüfgrundlagen | [Konformitätsbewertungsprogramm V1.2] | |
| Zertifikats-ID/-Nummer: | XXX Zertifikatsnummer von der Prüfstelle | |
| letzter Audittag vor Ort: | <tt.mm.jjjj> /Berichtsnummer/Datum | |
| Überwachung | nächste geplante Überwachung bis spätestens <tt.mm.jjjj> | |
| Datum der Ausstellung | <tt.mm.jjjj> | Laufzeit bis <tt.mm.jjjj> max. 3 Jahre> |

Unterschrift/Benannter Entscheider der KBS

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

DAkkS Deutsche Akkreditierungsstelle D-XX-YYYYY-ZZ-NN

zur Verwendung gemäß SymbolVO und DAkkS-Markennutzung

### Anlage 1

- Muss genau beschreiben, was alles unter Einsatz des Zertifizierungsgegenstands erlaubt ist. Alles andere ist in Anlage 2 auszuschließen.
- Hat den Verweis auf das öffentliche Kurzgutachten über das Ergebnis der Zertifizierung gem. Tz. 7.6 und 7.8 der Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065 der Datenschutzkonferenz (DSK) zu enthalten. Das Kurzgutachten muss die Nutzung des Zertifizierungsgegenstands im Einsatzgebiet und im Anwendungsfall in transparenter und nachvollziehbarer Weise dokumentieren, so dass auch der (End-) Kunde bzw. eine betroffene Person in angemessener Zeit nachvollziehen kann, was unter Nutzung des Zertifizierungsgegenstands im datenschutzrechtlichen Sinn gewährleistet ist.

### Anlage 2

- Darin sind alle Nutzungsausschlüsse zu nennen, d.h. was unter Einsatz des Zertifizierungsgegenstands im Anwendungsgebiet nicht gewährleistet wird.

### Anlage 3

- Zertifikate einer akkreditierten Zertifizierungsstelle nach DIN EN ISO/IEC 17021 sind keine Zertifikate im Sinne der DS-GVO. Die Konformitätsaussage im Zertifikat muss sich auf die Bezeichnung der inter-nationalen Managementsystemnorm ohne jeden Bezug auf die DS-GVO beschränken. Das Zertifikat für ein Managementsystem nach DIN EN ISO/IEC 27001 kann gemäß Anlage X mit dem Konformitätszusatz zur DIN EN ISO/IEC 27701 ergänzt werden. Eine gesonderte Ausgabe von Zertifikate zur ISO/IEC 27701 ist irreführend und unzulässig. Das Zertifikat und die Prüfberichte und sonstigen Bescheinigungen haben einen ausdrücklichen Hinweis zu enthalten, aus dem sich der eingeschränkte Geltungsbereich und der Zweck der Managementzertifizierung hervorgehen.