

dsc-White Paper  
27.01.2026

## **DSGVO-Zertifizierung als Wettbewerbsvorteil für HR-Dienstleister: Compliance nachweisen und Reputation stärken mit dem Zertifizierungsstandard „DSGVO – information privacy standard“**

### **1. Executive Summary**

HR-Dienstleister – von spezialisierten SaaS<sup>1</sup>-Anbietern über Recruiting- und Payroll-Provider bis hin zu Personalvermittlungen, Jobportalen und beruflichen Netzwerken – verarbeiten entlang des Employee-Lifecycles in großem Umfang sensible personenbezogene Daten. Je nach konkret erbrachter Dienstleistung werden etwa Gesundheitsdaten, Gehaltsinformationen sowie Daten zur Gewerkschafts- und Religionszugehörigkeit verarbeitet. Dies erfolgt vermehrt unter Zuhilfenahme von KI (so z. B. bei der Automatisierung von Recruitingprozessen). Aufgrund der mit der Verarbeitung verbundenen Risiken drohen bei DSGVO-Verstößen im HR-Kontext hohe Bußgelder von bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes und Schadensersatzansprüche betroffener Personen. Vor diesem Hintergrund verlangen Auftraggeber von HR-Dienstleistern zunehmend objektive, unabhängige Nachweise zur Einhaltung des Datenschutzes, bevor sie sich für eine Zusammenarbeit mit ihnen entscheiden. Auch im Rahmen von Ausschreibungen spielen solche Nachweise eine immer größere Rolle.

Hier bietet die DSGVO mit der genehmigten Zertifizierung nach Artikel 42 ein optimales, passgenaues Tool zum Nachweis von Compliance. Der Zertifizierungsstandard „DSGVO – information privacy standard“ ist eine solche genehmigte Zertifizierung, mit der Verantwortliche und Auftragsverarbeiter den Nachweis erbringen können, dass ihre IT-gestützten Verarbeitungsvorgänge DSGVO-konform sind. Ein Zertifizierungsverfahren nach „DSGVO – information privacy standard“ erfolgt unparteilich, transparent und qualitätsgesichert in einem zweistufigen Verfahren. Ein erteiltes Zertifikat ist drei Jahre gültig und kann im Rahmen von Rezertifizierungen um jeweils drei weitere Jahre verlängert werden. Zertifizierte HR-Dienstleister profitieren von Wettbewerbsvorteilen, der Reduktion von Haftungsrisiken, einem gesteigerten Vertrauen ihrer Kunden und einem Reputationszuwachs.



#### **Hinweis:**

Dieses White Paper richtet sich nicht direkt an HR-Verantwortliche / Personalabteilungen in Unternehmen. Auch für sie ist eine DSGVO-Zertifizierung aber durchaus interessant. So kann diese ein wirksamer Baustein eines erfolgreichen Employer Brandings und Candidate Trusts sein und durch den mit ihr verbundenen Vertrauenszuwachs auch einen wichtigen Beitrag zur Mitarbeiterbindung leisten.

---

<sup>1</sup> Software-as-a-Service

## 2. Ausgangslage: HR als Datenschutz-Hochrisikobereich

Im HR-Kontext wird eine Vielzahl personenbezogener Daten verarbeitet, womit oftmals ein hohes Risiko verbunden ist. Als Beispiele hierfür können Aktivitäten zur Leistungs- und Verhaltenskontrolle, der Einsatz biometrischer Identifikationssysteme, KI-gestützte Entscheidungsfindungen und die dauerhafte Videoüberwachung von Beschäftigten genannt werden. Verarbeitet werden so sensible Informationen wie individuelle Produktivitätskennzahlen, Angaben zu Fehlverhalten und Abmahnungen, Arbeitsunfähigkeitsgründe, Schwerbehinderteneigenschaft, Persönlichkeits- und Bewegungsprofile sowie Gesprächsprotokolle und E-Mail-Inhalte.



Neben den jeweiligen Arbeitgebern selbst sind hier auch die von diesen beauftragten HR-Dienstleister in der Pflicht: Je nach Art der von ihnen konkret erbrachten Dienstleistung werden diese als Auftragsverarbeiter oder Verantwortliche im Sinne der DSGVO tätig und sind deshalb selbst Adressaten datenschutzrechtlicher Pflichten.

So müssen Auftragsverarbeiter u.a. den folgenden Rechtspflichten nachkommen:

- Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen (Auftraggebers) – Artikel 29 DSGVO;
- Treffen geeigneter technischer und organisatorischer Maßnahmen zur Sicherheit der Verarbeitung – Artikel 32 DSGVO;
- Inanspruchnahme weiterer Auftragsverarbeiter nur nach vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Verantwortlichen – Artikel 28 Abs. 2 DSGVO;
- Beachtung der Regeln für Übermittlungen personenbezogener Daten in Drittländer außerhalb EU/EWR – Artikel 44 ff. DSGVO;
- Unverzügliche Meldung an den Verantwortlichen bei einer Verletzung des Schutzes personenbezogener Daten („Data Breach“) – Artikel 33 Absatz 2 DSGVO.

HR-Dienstleister, die ihre Leistungen als Verantwortliche erbringen, treffen noch sehr viel weitergehende Pflichten, z. B.:

- Rechenschaftspflicht: Verantwortliche müssen nachweisen können, dass sie die Grundsätze für die Verarbeitung personenbezogener Daten einhalten – Artikel 5 Abs. 2 DSGVO;
- Treffen von Maßnahmen zur Umsetzung von Privacy by Design and by Default – Artikel 25 DSGVO;
- Gewährleistung von Transparenz: Informationspflichten und Auskunftsrecht gegenüber den von der Verarbeitung betroffenen Personen – Artikel 13 ff. DSGVO;
- Beachtung der rechtlichen Vorgaben der DSGVO zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling – Artikel 22 DSGVO;
- Durchführung einer Datenschutzfolgen-Abschätzung bei Verarbeitungen mit hohem Risiko für Rechte und Freiheiten natürlicher Personen – Artikel 35 DSGVO.

Die Durchführung einer Datenschutzfolgen-Abschätzung wird im HR-Kontext u.a. auch dann oftmals erforderlich sein, wenn KI verwendet wird. Als Beispiel sei insoweit der Einsatz eines KI-gestützten Bewerber-Scorings genannt. Vielfach wird beim Einsatz von KI auch ein besonderes Augenmerk auf die Einhaltung der Vorgaben von

Artikel 22 DSGVO zu legen sein. Ist diese Vorschrift anwendbar, trifft den Verantwortlichen zudem die Pflicht, den betroffenen Personen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zur Verfügung zu stellen.<sup>2</sup>

### 3. Risiko: Bußgelder, Schadensersatzansprüche und Vertrauensverlust

Bekanntermaßen drohen Verantwortlichen und Auftragsverarbeitern bei DSGVO-Verstößen Bußgelder von bis zu 20 Mio. € oder 4 % des welt- und konzernweiten Jahresumsatzes. Auf dem Vormarsch sind außerdem Schadensersatzansprüche von Personen, denen wegen eines Verstoßes ein materieller oder immaterieller Schaden entstanden ist.

So sind im HR-Kontext auch bereits Bußgelder in Millionenhöhe verhängt worden: Zu nennen ist hier etwa ein Bußgeld in Höhe von 35,3 Mio. €, das einem Unternehmen auferlegt wurde, welches umfangreiche und fortlaufend aktualisierte Aufzeichnungen über private Lebensumstände, Gesundheitsangaben und Tätigkeiten von Beschäftigten ohne Rechtsgrundlage verarbeitet hatte.<sup>3</sup> In einem anderen Fall wurde die flächendeckende, anlasslose Videoüberwachung von Arbeitsplätzen, Lagern und Aufenthaltsbereichen mit einem Bußgeld in Höhe von 10,4 Mio. € sanktioniert.<sup>4</sup> Erfolgreich gerichtlich geltend gemachte Schadensersatzansprüche betrafen bislang insbesondere den Bereich der unzulässigen Videoüberwachung am Arbeitsplatz, die uninformierte Google-Recherche eines Bewerbers, die heimliche Observation eines arbeitsunfähigen Mitarbeiters durch eine Detektei sowie die Übermittlung von Echtdateien zu Beschäftigten zwischen Konzerngesellschaften, um die HR-Cloud eines spezialisierten Dienstleisters zu testen<sup>5</sup>.



Auch wenn sich die Bußgelder und Schadensersatzansprüche bislang überwiegend gegen die jeweiligen Arbeitgeber der betroffenen Beschäftigten richteten, zeigt beispielsweise ein Fall aus dem Jahr 2025, dass durchaus auch HR-Dienstleister hiervon betroffen sein können. Konkret wurde ein Bußgeld gegen eine Personalvermittlung verhängt, weil sie die Datenschutzrechte von Arbeitssuchenden ignoriert hatte.<sup>6</sup> In einem anderen Fall (ebenfalls aus 2025) wurde eine mit der Verwaltung von Mitarbeiter-Schichtplänen beauftragte Agentur mit einem Bußgeld belegt: Hier waren Beschäftigtendaten wegen einer Fehlkonfiguration und unzureichender technischer und organisatorischer Maßnahmen öffentlich zugänglich geworden.<sup>7</sup>

Sei es durch ein Bußgeld, Schadensersatzansprüche von betroffenen Personen oder einen Data Breach: Häufig wiegen der Vertrauensverlust bei Kunden und sonstigen Stakeholdern sowie der daraus resultierende Reputationsschaden mindestens ebenso schwer wie der unmittelbare finanzielle Schaden.

---

<sup>2</sup> Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO.

<sup>3</sup> <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-h&m-hennes-2020-10-01-DE-651.php>

<sup>4</sup> <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-notebooksbilliger.de-ag-2021-01-08-DE-823.php>

<sup>5</sup> <https://www.bundesarbeitsgericht.de/presse/schadenersatz-nach-datenschutz-grundverordnung-dsgvo-betriebsvereinbarung-workday/>

<sup>6</sup> [https://www.lidi.nrw.de/bussgeld\\_2025](https://www.lidi.nrw.de/bussgeld_2025)

<sup>7</sup> <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-mcdonald's-polska-2025-06-23-PL-4556.php>

#### 4. Lösung: Zertifizierung nach Artikel 42 DSGVO

Mit der Zertifizierung gemäß Artikel 42 stellt die DSGVO ein verlässliches und praktisches Instrument zum Nachweis von Datenschutz-Compliance zur Verfügung. Zertifiziert werden können Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern. Das bedeutet im Umkehrschluss, dass reine IT-Produkte wie etwa Software, die erst noch „on-prem“ installiert werden muss, Personen und Management-Systeme nicht in den Anwendungsbereich dieser Vorschrift fallen. So handelt es sich beispielsweise bei der Zertifizierung eines Datenschutz-Managementsystems nach ISO/IEC 27701 oder bei einer Personenzertifizierung, durch die die Fachkunde eines betrieblichen Datenschutzbeauftragten (bDSB) bescheinigt wird, gerade nicht um eine DSGVO-Zertifizierung.

Eine Zertifizierung nach Artikel 42 DSGVO wird durch hierfür akkreditierte Zertifizierungsstellen, die ihre Unabhängigkeit und ihr Fachwissen nachgewiesen haben, und auf der Grundlage eines durch die zuständigen Behörden genehmigten Zertifizierungsprogramms wie etwa des „DSGVO – information privacy standard“ erteilt. Bei Datenschutzsiegeln oder sonstigen Nachweisen, die diese Voraussetzungen nicht erfüllen, handelt es sich also ebenfalls nicht um eine DSGVO-Zertifizierung, auch wenn hier oftmals ein anderer Anschein erweckt wird.

Eine Zertifizierung wird nach erfolgreichem Abschluss eines transparenten Zertifizierungsverfahrens für eine Höchstdauer von drei Jahren erteilt und kann jeweils um drei weitere Jahre verlängert werden, sofern die einschlägigen Kriterien weiterhin erfüllt werden.



Zertifizierte Organisationen profitieren insbesondere von Wettbewerbsvorteilen und einer Haftungsreduktion:

Unternehmen können sich gegenüber ihren Mitbewerbern abheben, indem sie mit einem DSGVO-Zertifikat nachweisen, dass bestimmte Verarbeitungsvorgänge die gesetzlichen Anforderungen erfüllen. Gerade im Bereich der Auftragsverarbeitung ist davon auszugehen, dass sich solche Zertifikate in wenigen Jahren zum Must-Have entwickeln werden (vergleichbar mit ISO/IEC 27001 bei Rechenzentren). Aber auch Dienstleister, die als Verantwortliche im Sinne der DSGVO agieren, können sich durch ein Zertifikat nach Artikel 42 DSGVO vom Wettbewerb hervorheben. Ein Zertifikat kann nicht zuletzt auch im Rahmen von Ausschreibungen (RFP<sup>8</sup>) das entscheidende Alleinstellungsmerkmal (USP<sup>9</sup>) sein, das zum Zuschlag führt.

Über ein unabhängiges Zertifikat können zudem die in der DSGVO verankerten Nachweispflichten optimal erfüllt werden, was im Ergebnis auch zu einer Haftungsreduktion führt. So ist eine Zertifizierung bei der Entscheidung darüber, ob ein Bußgeld verhängt wird, von der zuständigen Aufsichtsbehörde gebührend zu berücksichtigen<sup>10</sup> – sie kann sich also positiv auf eine solche Entscheidung auswirken. Gleiches gilt für die Entscheidung über die Höhe eines etwaigen Bußgeldes. Dies kann auch bilanziell

---

<sup>8</sup> Request for Proposal

<sup>9</sup> Unique Selling Proposition

<sup>10</sup> Art. 83 Abs. 2 S. 2 lit. j DSGVO

interessant sein (Stichwort: Rücklagen, KonTraG<sup>11</sup>, aber auch Versicherungen – gegebenenfalls kann eine DSGVO-Zertifizierung die Höhe einer Versicherungsprämie reduzieren).

## 5. Best Practice-Ansatz: Der „DSGVO – information privacy standard“

„DSGVO – information privacy standard“ ist ein offiziell genehmigter<sup>12</sup>, generischer Zertifizierungsstandard für Artikel 42 DSGVO-Zertifikate, mit dem IT-gestützte Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern auf DSGVO-Konformität geprüft werden können. Programmeignerin dieses Standards ist die datenschutz cert GmbH, die auch als Zertifizierungsstelle für „DSGVO – information privacy standard“ agiert. Sie ist hierfür von der Deutsche Akkreditierungsstelle GmbH (DAKkS) akkreditiert worden<sup>13</sup> und hat vom Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) Bremen die Befugnis zur Tätigkeit als Zertifizierungsstelle erhalten.



Bei „DSGVO – information privacy standard“ ist ein qualitätsgesichertes, zweistufiges Verfahren etabliert, wonach ein Evaluationsteam – bestehend aus juristischen und technischen Experten\*innen – den Verarbeitungsvorgang prüft, bevor die Zertifizierungsstelle die Ergebnisse der Evaluierung bewertet und im Erfolgsfall das Zertifikat erteilt.

Ein Zertifikat gemäß „DSGVO – information privacy standard“ ist drei Jahre gültig. Nach der Erst- und Re-Zertifizierung sind jeweils jährliche Überwachungen vorgesehen.

Ein zentrales Dokument des „DSGVO – information privacy standard“ ist der Kriterienkatalog: Dieser stellt die verbindlichen inhaltlichen Anforderungen für die Prüfung und Beurteilung einer IT-gestützten Verarbeitung personenbezogener Daten dar. Der Kriterienkatalog sieht 50 Kriterien vor, die in acht Bereiche gruppiert sind:

---

<sup>11</sup> Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

<sup>12</sup> [https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks/dsgvo-information\\_de](https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks/dsgvo-information_de)

<sup>13</sup> <https://www.dakks.de/de/akkreditierte-stelle.html?id=D-ZE-16077-02-00>

- 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

## 6. Anwendungsbeispiele: Typische Use Cases im HR-Kontext

Mit Blick auf HR-Dienstleister lassen sich beispielsweise die folgenden Arten von Verarbeitungsvorgängen nennen, die nach „DSGVO – information privacy standard“ zertifiziert werden können:

- Zur Personalbeschaffung durchgeführte Verarbeitungsvorgänge durch einen externen RPO<sup>14</sup>-Spezialisten;
- Verarbeitungsvorgänge beim Betrieb eines ATS<sup>15</sup>-Bewerbermanagements im Auftrag eines Kunden;
- SaaS-Lösung für Employee Experience, People Analytics & Performance;
- Payroll-SaaS-Verarbeitung (Datenverarbeitung bei der Lohnbuchhaltung);
- Verarbeitungsvorgänge beim Einsatz der Matching/Recommendation-Engine eines Jobportals;
- Aufbau und Pflege eines Talentpools durch eine Personalvermittlung sowie Weitergabe personenbezogener Daten zu Talenten an deren Kunden;
- Time and Attendance-Verarbeitung (Arbeits-/Fehlzeiten) in Workforce- Management-SaaS;
- Betrieb einer telefonischen Whistleblowing-Hotline oder eines webbasierten Hinweisgebersystems;
- Verarbeitungsvorgänge bei LMS<sup>16</sup>-Enrollment und Teilnehmerverwaltung (Kursbuchung bis Teilnahmebestätigung);
- Verarbeitungsvorgänge im Zusammenhang mit der Anmeldung auf sowie der Verwaltung einer Benefits-/Compensation-Plattform.



### Hinweis:

Hierbei handelt es sich lediglich um eine beispielhafte Aufzählung. Nach „DSGVO – information privacy standard“ zertifiziert werden können jegliche Verarbeitungsvorgänge, die von HR-Dienstleistern als Verantwortliche oder Auftragsverarbeiter erbracht werden.

<sup>14</sup> Recruitment Process Outsourcing

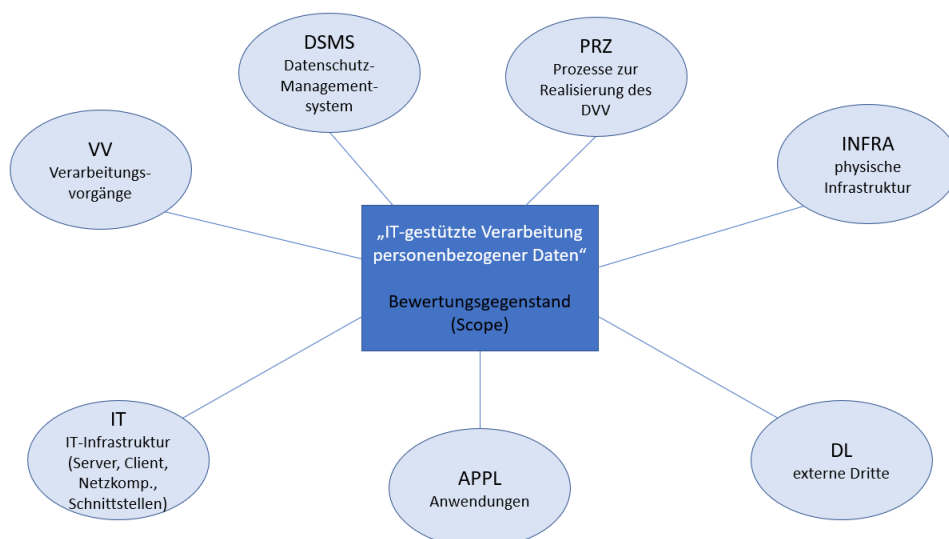
<sup>15</sup> Applicant Tracking System

<sup>16</sup> Learning Management System

## 7. Expertentipp: Scope präzise definieren – der Schlüssel zum Erfolg

An dieser Stelle soll das Thema „Scoping“ näher beleuchtet werden, da es von fundamentaler Bedeutung für ein erfolgreiches Zertifizierungsverfahren ist. Scoping meint, den Geltungsbereich – also den Umfang der Zertifizierung – klar zu benennen, um zu definieren, was im Rahmen des Zertifizierungsverfahrens geprüft wird und was außerhalb der Betrachtungsgrenzen liegt. Dazu muss eindeutig beschrieben werden, welche Verarbeitungsvorgänge im Einzelnen zum Bewertungsgegenstand gehören, an welchen Standorten diese Tätigkeiten erbracht werden, welche externen Dritten (z. B. Dienstleister) ggf. einbezogen sind, welche IT-Komponenten erforderlich sind und auch welche Prozesse in einer Organisation etabliert sind, um die Datenverarbeitung insgesamt darstellen zu können. Konkret müssen also die folgenden Elemente (Zielobjektkategorien) charakterisiert werden:

- Verarbeitungsvorgänge (VV) zur Konkretisierung der zu zertifizierenden Datenverarbeitung;
- Datenschutz-Managementsystem (DSMS) mit den internen Prozessen zur Steuerung der Datenschutz-Konformität;
- Prozesse (PRZ) mit den Tätigkeiten, die für die konkrete Datenverarbeitung benötigt werden;
- Physische Infrastruktur (INFRA) mit Standorten und Räumen;
- IT-Infrastruktur (IT) mit allen relevanten Komponenten (z. B. Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen);
- Applikationen (APPL), über die die Datenverarbeitung realisiert wird;
- Externe Dritte (DL), z. B. Dienstleister, Auftragsverarbeiter, Behörden oder Schwes-tergesellschaften, die für die Realisierung der Datenverarbeitung benötigt werden oder an die personenbezogene Daten übermittelt werden.





### **Empfehlung:**

Es ist ratsam, mit einem kleinen Scope zu beginnen, also mit einer eher übersichtlichen Datenverarbeitung. Später den Scope zu erweitern, ist erfahrungsgemäß sehr viel einfacher, als gleich zu Beginn mit einem mächtigen und komplexen Scope loszulegen. So könnte man etwa in dem in Kapitel 4 genannten Beispiel „Anmeldung auf sowie Verwaltung einer Benefits/Compensation Plattform“ zunächst nur die Datenverarbeitung bezüglich der Anmeldung zertifizieren lassen und den Bewertungsgegenstand dann zu einem späteren Zeitpunkt um zusätzliche Verarbeitungsvorgänge erweitern.



### **Achtung:**

Unzulässig ist es hingegen, bewusst relevante, risikoreiche Bestandteile einer Datenverarbeitung auszusparen (Verbot des „Cherry Picking“).

## **8. Anleitung: In fünf Schritten zur Zertifizierung nach „DSGVO – information privacy standard“**

Der Weg zum Zertifikat führt über die folgenden fünf Schritte:

### **8.1. Scoping**

Im ersten Schritt ist die Datenverarbeitung, für die ein DSGVO-Zertifikat angestrebt wird, zu identifizieren und abzugrenzen, wie bereits im vorangegangenen Kapitel erläutert.

### **8.2. Vertraut werden mit „DSGVO – information privacy standard“**

Wie der Zertifizierungsstandard „DSGVO – information privacy standard“ funktioniert, lässt sich auf der Website zum Zertifizierungsstandard<sup>17</sup> oder direkt in dem dort verlinkten, öffentlich zugänglichen Kriterienkatalog nachlesen.

### **8.3. Angebot einholen**

Die Kosten für ein DSGVO-Zertifikat orientieren sich an der Komplexität und dem Umfang der Datenverarbeitung, die im Scope ist. Deshalb werden einige Informationen benötigt, um den Aufwand zu kalkulieren. Nach dem bereits im ersten Schritt durchgeführten Scoping bedeutet die Zusammenstellung dieser Informationen allerdings nur noch einen verhältnismäßig geringen Aufwand.

### **8.4. Evaluierung**

Von zentraler Bedeutung für die Evaluierung sind die folgenden Meilensteine:

- Übergabe der Referenzdokumentation (Scope-Beschreibung und weitere, vom Kunden zu erstellende Dokumente);
- Basisprüfung;

---

<sup>17</sup> <https://www.ips-dsgvo-zertifikat.de/>

- Prüfung (rechtlich);
- Prüfung (technisch);
- Auditierung/Inspektion als Site Visit (Vor-Ort-Termin).

Wenn alle Evaluierungsschritte absolviert sind und die zu zertifizierende Datenverarbeitung sämtliche relevanten Anforderungen erfüllt, erstellen die Evaluatoren\*innen ihre Berichte und reichen die gesamte Dokumentation in der Zertifizierungsstelle ein.

### 8.5. Zertifikat

Wenn auch die Zertifizierungsstelle zu dem Schluss kommt, dass alle einschlägigen Anforderungen des Kriterienkatalogs angemessen umgesetzt sind, wird eine positive Zertifizierungsentscheidung getroffen und das Zertifikat ausgestellt.



### 9. Fazit

Durch eine Zertifizierung nach dem „DSGVO – information privacy standard“ können HR-Dienstleister Risiken minimieren, Compliance nachweisen, Wettbewerbsvorteile erlangen und Vertrauen und Reputation ausbauen sowie Due Diligence-Prozesse ihrer Kunden beschleunigen.

Wir freuen uns, wenn wir durch dieses White Paper Ihr Interesse an einer Zertifizierung geweckt haben. Bei Fragen zögern Sie bitte nicht, uns anzusprechen. Als unabhängige Zertifizierungsstelle dürfen wir Sie zwar nicht beraten, wir dürfen aber selbstverständlich unsere Methodik erläutern und freuen uns, Ihre Fragen dazu zu beantworten.



**Sie erreichen uns unter:**

datenschutz cert GmbH  
Konsul-Smidt-Straße 88a • 28217 Bremen  
Tel.: +49 (0) 421 69 66 32 50  
E-Mail: office@datenschutz-cert.de

**A. Anhang 1: Kategorien von HR-Dienstleistern und ihre datenschutzrechtlichen Rollen (Verantwortlicher / Auftragsverarbeiter)**

ART DER HR-DIENSTLEISTUNG	TYPISCHE DATENSCHUTZRECHTLICHE ROLLE
HR-Software und Digitalisierung (z.B. SaaS-HR-Tools)	Auftragsverarbeiter
Recruiting Process Outsourcing	Auftragsverarbeiter
Payroll Services (Entgeltabrechnung)	Auftragsverarbeiter oder Verantwortlicher (vgl. § 11 Abs. 2 StBerG)
Benefits und Compensation-Management	Auftragsverarbeiter oder Verantwortlicher
Personalvermittlung und Executive Search	Verantwortlicher
Arbeitnehmerüberlassung (Zeitarbeit)	Verantwortlicher
Weiterbildung und Training	Verantwortlicher
HR-Consulting und Strategieberatung	Verantwortlicher
Employer Branding und Personalmarketing	Verantwortlicher
Outplacement / Newplacement	Verantwortlicher
Jobportale	Verantwortlicher
Arbeitgeberbewertungsportale	Verantwortlicher
Berufliche Netzwerke	Verantwortlicher



**Hinweis:**

In dieser Übersicht werden die typischerweise einschlägigen datenschutzrechtlichen Rollen aufgelistet. Im konkreten Einzelfall muss aber stets unter Berücksichtigung aller relevanten Aspekte geprüft werden, ob eine Datenverarbeitung als Verantwortlicher oder als Auftragsverarbeiter durchgeführt wird.