***Antrag***

**Antrag auf GDPR CC- Zertifizierung eines Cloud-Services durch die**

**PwC Certification Services**

**GmbH**

|  |  |
| --- | --- |
| Dokumentenart: | Formblatt |
| Mandant: | Zertifizierungsstellen-intern, potenzielle Mandanten |
| Autor: | Leitung der Zertifizierungsstelle-DL |
| Editor: | Sören Scholz |
| QS: | Stellv. Leitung der Zertifizierungsstelle-DL |
| Version: | 4.0 |
| Status: | Freigegeben |
| Verschwiegenheit: | ÖFFENTLICH |
| Verteiler: | Mitarbeiter der Zertifizierungsstelle und potentielle Mandanten |

***Antrag auf GDPR CC-Zertifizierung eines Cloud-Services durch die PwC Certification Services GmbH***

Hiermit beantragen wir als Cloud-Anbieter in der Rolle des Auftragsverarbeiters eine GDPR CC-Zertifizierung bei der PwC Certification Services GmbH und bitten um Bewertung, ob eine Zertifizierung für den angegebenen Geltungsbereich durchgeführt werden kann sowie um die kostenfreie und unverbindliche Erstellung eines entsprechenden Angebotes.

Mit diesem Antrag entsteht kein rechtsverbindliches Vertragsverhältnis.

1. ***Angaben zum Antragsteller***

| **Frage** | **Antwort** | |
| --- | --- | --- |
| **Name der antragstellenden Organisation** |  | |
| **Anschrift** |  | |
| **Allg. Kontaktdaten des Antragstellers** | Telefon |  |
| Telefax |  |
| E-Mail |  |
| Internet |  |
| **Rechnungsanschrift**  **(sofern abweichend)** |  | |
| **Lieferanschrift**  **(sofern abweichend)** |  | |
| **Weitere Standorte [Name(n) und**  **Anschrift(en)]** |  | |
| **Kontaktperson** | Anrede |  |
| Vorname Name |  |
| Funktion |  |
| Telefon |  |
| Telefax |  |
| E-Mail |  |
| **Verantwortliches**  **Mitglied der Geschäftsführung/ Leitungsebene** | Anrede |  |
| Vorname Name |  |
| Funktion |  |
| Telefon |  |
| Telefax |  |
| E-Mail |  |

1. ***Basisangaben zur beantragten Zertifizierung***

| **Frage** | **Antwort** |
| --- | --- |
| **Die Zertifizierung wird beantragt auf Basis folgender Normen/Standards (in der jeweils aktuell gültigen Fassung)** | ☒ GDPR CC (AUDITOR-Konformitätsbewertungsprogramm und AUDITOR-Kriterienkatalog inkl. der mitgeltenden Dokumente) |
| **Verfahrensart (Art des Audits)  (Mehrfachauswahl möglich)** | ☐ Erstzertifizierung  ☐ Rezertifizierung  ☐ Erweiterung/Änderung des  Geltungsbereiches |
| **Beantragte Schutzklasse** | ☐ Schutzklasse 1  ☐ Schutzklasse 2  ☐ Schutzklasse 3 |
| **Beantragte Wiederherstellbarkeitsklasse** | ☐ Wiederherstellbarkeitsklasse 1  ☐ Wiederherstellbarkeitsklasse 2 ☐ Wiederherstellbarkeitsklasse 3 |
| **Branche** |  |
| **Tätigkeiten** |  |
| **Beschreibung der Marktausrichtung**  **(z. B. national, EU, international, ausgewählte Märkte in Ländern etc.)** |  |
| **Personelle Ressourcen**  **(Anzahl aller Mitarbeiter im Geltungsbereich, welche an der Erbringung des Datenverarbeitungs­vorgangs oder der Datenverarbeitungs­vorgänge mitwirken)** |  |
| **Technische Ressourcen** |  |
| **Organigramm** | Bitte relevante Organigramme als Anlage beifügen |
| **Beziehungen in einer größeren**  **Körperschaft** |  |
| **Anzahl der Cloud-Kunden** |  |
| **Wurden Beratungsleistungen bezüglich der zu zertifizierenden Datenverarbeitungsvorgänge in Anspruch genommen?  Wenn ja, von wem und wann?** |  |

1. ***Beschreibung und Festlegung des Zertifizierungsgegenstandes  
   gemäß § 5.1.4 GDPR CC***

Wir beantragen hiermit die Zertifizierung des bzw. der nachfolgenden personenbezogenen Datenverarbeitungsvorgangsvorgänge in unserem(n) Cloud-Dienste(n) gemäß GDPR CC-Kriterienkatalog (Zertifizierungsgegenstand).

<Bitte hier die detaillierte Beschreibung des Zertifizierungsgegenstandes einfügen und/oder ergänzende Dokumente dem Antrag beifügen.>

**Hinweis:** Die Beschreibung des Zertifizierungsgegenstandes sollte mindestens die folgenden Themen abdecken:

* die Benennung und detaillierte (Funktions-)Beschreibung des Datenverarbeitungsvorgangs oder der Datenverarbeitungsvorgänge innerhalb eines entsprechenden Cloud-Dienstes, der zertifiziert werden soll;
* detaillierte Beschreibung aller Bestandteile der relevanten Datenverarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur ersichtlich und gewährleistet wird;
* Dokumentation Ihrer internen Verantwortlichkeiten im Datenverarbeitungsvorgang;
* Welche Daten im Zusammenhang mit dem Zertifizierungsgegenstand verarbeitet werden (siehe DSK ADZ Tz. 2.1.2) und
  + welche Daten davon besondere Kategorien personenbezogener Daten gemäß Art 9 sind;
  + welche Daten sich auf strafrechtliche Verurteilungen und Straftaten nach Art. 10 beziehen;
* Benennung und Informationen zu Standorten bei denen Datenverarbeitungsvorgänge durchgeführt werden (darunter Nennung Zentralstelle und weiterer Standorte und Beschreibung der Tätigkeiten, Risiken pro Standort, rechtliche und vertraglichen Regelungen für jeden Standort, den Grad der Zentralisierung der Prozesse/Tätigkeiten, die für alle Standorten erbracht werden, die Schnittstellen zwischen den verschiedenen Standorten;
* Informationen bezüglich aller ausgegliederten Vorgänge, die von Ihnen im Rahmen des Datenverarbeitungsvorgangs genutzt werden und die Konformität mit den Zertifizierungskriterien beeinflussen. Dabei müssen insbesondere Subauftragsverarbeiter und die von diesen übernommenen Zuständigkeiten und damit verbundenen Aufgaben benannt werden;
* die Darstellung der Schnittstellen und Übergänge zu anderen Systemen und Organisationen/Subauftragsverarbeitern (bspw. in Form eines Netzplans). Hierbei sind auch die zugrundeliegenden Protokolle (bspw. Überwachungsprotokolle, (Muster-)Verträge, Vereinbarungen, Garantien) und sonstige Zusicherungen darzulegen;
* Angabe, ob eine Übermittlung personenbezogener Daten
  + außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder
  + an internationale Organisationen erfolgt

Dabei muss beachtet werden, dass es in der Praxis häufig zu derartigen Drittlandtransfers bei der Übermittlung von Daten im Rahmen von Wartung, Pflege und Supports kommt (siehe DSK ADZ Tz. 2.10). Insbesondere kann dies auch in Ausnahmefällen erforderlich sein und muss daher berücksichtigt werden.

* Ihre technischen und organisatorischen Maßnahmen (TOM) i. S. d. Art. 28 DS-GVO;
* eingesetzte Technik und IT-Landschaft, dazu zählen insbesondere relevante IT-Systeme und das Zusammenspiel zwischen Technik und organisatorische Prozesse;
* organisatorische Prozesse zur Durchführung der Datenverarbeitungsvorgänge;
* welche spezifischen Datenschutzrisiken die zu zertifizierenden Datenverarbeitungsvorgänge aufweisen.

1. ***Stellungnahme zur Erfüllung der Zertifizierungskriterien   
   gemäß § 5.1.6 GDPR CC***

Nachfolgend geben wir als Antragssteller dediziert für jedes Zertifizierungskriterium unsere Stellungnahme hinsichtlich der Erfüllung des jeweiligen Zertifizierungskriteriums ab und erläutern die Umsetzung ggf. unter Referenz zur entsprechenden Dokumentation. Durch die Abgabe dieser Stellungnahme versichern wir gegenüber der PWC Certification Services GmbH, die in der Stellungnahme genannten Maßnahmen vollständig umgesetzt zu haben.

<Bitte Excel-Formblatt „Erläuterung zur Erfüllung der Zertifizierungskriterien gemäß § 5.1.6 GDPR CC“ ausfüllen und als Anlage beifügen.>

**Hinweis:** Bitte nutzen Sie die beigefügte Excel-Tabelle als Hilfestellung zur Abgabe der Stellungnahme zur Erfüllung der Zertifizierungskriterien. Darüber hinaus dient die Excel-Tabelle ebenfalls zur Erläuterung der Nichtanwendbarkeit von einzelnen Zertifizierungskriterien sowie derjenigen Zertifizierungskriterien, welche durch Anerkennung bereits vorliegender Zertifizierungen.

1. ***Erläuterung zur Nichtanwendbarkeit von Zertifizierungskriterien gemäß § 5.1.5 GDPR CC***

Für die von uns beschriebenen erbrachten personenbezogenen Datenverarbeitungsvorgänge in unseren Cloud-Diensten (Zertifizierungsgegenstand) schätzen wir die im Anhang (Excel-Dokument) genannten Zertifizierungskriterien als nichtanwendbar ein. Die Dokumentation erfolgt im beigefügten Excel-Dokument (siehe „Erläuterung zur Erfüllung der Zertifizierungskriterien gemäß § 5.1.6 GDPR CC).

**Hinweis:** Im Weiteren ist es möglich, dass der Antragssteller oder die PwC Cert z. B. im Rahmen der Festlegung des Zertifizierungsgegenstandes oder der Ermittlungs- und Bewertungstätigkeiten eine Nichtanwendbarkeit von Zertifizierungskriterien aufgrund besonderer Umstände und Eigenschaften des Datenverarbeitungsvorgangs feststellen kann, die entsprechend begründet wird.

**Hinweis:** Nicht anwendbar sind Kriterien insbesondere dann (vgl. § 5.1.5 (5) GDPR CC), wenn:

* der Cloud-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der Cloud-Anbieter bspw. nach dem Zertifizierungskriterium Nr. 6.2 zur Unterstützung des Cloud-Nutzers bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des Cloud-Anbieters nicht anwendbar und der Cloud-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt (bspw. im Falle eines Infrastructure-as-a-Service). Das Gleiche gilt, wenn nicht der Cloud-Anbieter, sondern Subauftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach dem Zertifizierungskriterium Nr. 2.3 verantwortlich sind. In diesem Fall ist das Zertifizierungskriterium Nr. 2.3 auf den Cloud-Anbieter nicht anwendbar. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass die Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (s. Zertifizierungskriterium Nr. 10.4) und somit ihrerseits das Zertifizierungskriterium Nr. 2.3 erfüllen.
* der Cloud-Anbieter die in den Zertifizierungskriterien adressierten Handlungen nicht vornimmt. Setzt der Cloud-Anbieter bspw. keine Subauftragsverarbeiter ein oder findet keine Datenverarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt, sind die Zertifizierungskriterien aus Kapitel V und VI des AUDITOR-Kriterienkatalogs nicht anwendbar.

1. ***Beantragung der Anerkennung von bestehenden Zertifizierungen gemäß § 5.1.7 GDPR CC***

Wir beantragen die Anerkennung der folgenden bereits bestehenden Zertifizierungen für Bestandteile der Datenverarbeitungsvorgänge (vgl. Excel-Dokument).

**Hinweis:** Grundsätzlich können nur Zertifikate der folgenden drei Kategorien anerkannt werden:

Das Zertifikat wurde von einer akkreditierten Zertifizierungsstelle ausgestellt (bspw. ein   
ISO/IEC 27001 Zertifikat durch eine akkreditierte Zertifizierungsstelle);

Das Zertifikat wurde von einer Stelle ausgestellt, die eine Begutachtung unter Gleichrangigen durchlaufen hat (gem. ISO/IEC 17040);

Das Zertifikat wurde durch eine staatliche Zertifizierungsstelle auf gesetzlicher Grundlage ausgestellt (z. B. Cyber Security Act).

Anzuerkennende Zertifikate sind vor der Antragsstellung durch die PwC Certification Services GmbH hinsichtlich ihrer Anerkennung zu bewerten. Sollten Sie die Anerkennung von Zertifikaten für Bestandteile des Zertifizierungsgegenstands wünschen, nehmen Sie bitte im Vorfeld Kontakt mit uns auf.

Gleichwohl ist die beantragte Anerkennung in diesen Antrag, als auch in die Stellungnahme zur Erfüllung der Zertifizierungskriterien aufzunehmen.

Hinweis: Die Frist zur Übermittlung aller für die Bearbeitung und Bewertung des Zertifizierungsantrags erforderlichen Informationen beträgt in der Regel 2 bis max. 3 Monate nach Antragseingang.

1. ***Erklärung zu den technischen Voraussetzungen für Remote-Techniken***

Im Rahmen der Ermittlungen können grundsätzlich anteilig Remote-Techniken wie Web-Meetings (Remote-Audits), Telefonkonferenzen oder elektronische Fernprüfung der Datenverarbeitungsvorgänge (bspw. Penetrationstests oder Schwachstellenanalysen) durch die PwC Cert genutzt werden. Hiermit erklären wir, dass gemäß den Anforderung IAF MD4 und DIN EN ISO/IEC 17021-1 mindestens die folgenden technischen Voraussetzungen gegeben sind bzw. zum Zeitpunkt der Ermittlung sichergestellt werden:

1. Stabile Internetverbindung

Eine ausreichend schnelle und stabile Internetverbindung ist vorhanden (mindestens 5 Mbit/s empfohlen), um Video- und Audioübertragungen ohne Unterbrechung zu ermöglichen.

1. Geeignete Hardware

Es stehen geeignete Endgeräte zur Verfügung (z. B. PC, Laptop, Tablet oder Mobilgerät) mit Kamera, Mikrofon und Lautsprecher bzw. Headset für eine störungsfreie Kommunikation.

1. Zugriff auf relevante Dokumente und Systeme

Die zur Auditierung relevanten Informationen, Dokumente und IT-Systeme können bei Bedarf digital freigegeben bzw. über Bildschirmfreigabe oder Dateizugriff zur Verfügung gestellt werden.

1. Virtuelle Besichtigung (sofern erforderlich)

Falls eine visuelle Begutachtung von Anlagen, Produktionsbereichen oder Tätigkeiten erforderlich ist, wird diese über mobile Geräte (z. B. Smartphone, Tablet) mit Kamera ermöglicht.

1. Datenschutz und Vertraulichkeit

Die eingesetzten technischen Systeme und Plattformen entsprechen den geltenden Datenschutzanforderungen. Der Zugang erfolgt kontrolliert und ausschließlich durch autorisierte Personen. Die Vertraulichkeit der übermittelten Inhalte wird gewährleistet.

1. Zugang zu Kommunikationsplattformen

Die Nutzung gängiger Kommunikationsmittel (z. B. Microsoft Team oder vergleichbare Lösungen) wird ermöglicht. Ggf. erforderliche Softwareinstallationen werden im Vorfeld abgestimmt.

Wir bestätigen, dass unser Unternehmen die oben genannten technischen Voraussetzungen erfüllt oder rechtzeitig vor dem Remote-Audit die notwendigen Maßnahmen zur Herstellung dieser Voraussetzungen trifft. Wir sind uns bewusst, dass fehlende technische Voraussetzungen zur Verzögerung oder zum Abbruch des Remote-Audits führen können oder der Verwendung von anderen geeigneten Ermittlungsmethoden.

|  |  |  |
| --- | --- | --- |
| Ort, Datum |  | Rechtsverbindliche Unterschrift |