Datenschutzinformationsblatt für Kunden der CertMe GmbH gemäß Artikel 13 und 14 Datenschutzgrund-verordnung („DSGVO“)

Im Folgenden informiert die CertMe GmbH Sie über die Erhebung (durch die CertMe GmbH selbst oder in Form der Übermittlung an die CertMe GmbH durch die Kunden der CertMe GmbH) Ihrer personenbezogenen Daten (alle Informationen, die sich direkt oder indirekt auf natürliche Personen beziehen und diese identifizieren oder identifizierbar machen) und wie diese verarbeitet werden.

Änderungs-Historie (Revision Board)

Rev.	Beschreibung	Datum	Klassifizierung
001	Erstfassung des Dokumentes	09.02.2024	Public

Inhaltsverzeichnis

I. Präambel

Dieses Datenschutzinformationsblatt richtet sich an unsere bestehenden, ehemaligen und potenziell zukünftigen Kunden, ihre jeweiligen Gesellschafter, Organe und sonstigen Mitarbeiter*innen oder vertretungsbefugte Personen sowie an jede Person, über die wir im Rahmen einer Informationserteilung durch unsere Kunden personenbezogene Daten erhalten oder deren personenbezogene Daten wir selbst aus anderen Datenquellen erheben (alle genannten Personen im Folgenden kurz gemeinsam „Kunden“).

Da die CertMe GmbH Ihre Leistungen in Abhängigkeit von den einzelnen Bereichen (Consulting, Zertifizierung, CISO as a Service) und dem Ort der Beauftragung jeweils durch unterschiedliche (verbundene) Gesellschaften erbringt, gilt dieses Datenschutz-informationsblatt für alle nachfolgenden Gesellschaften gleichermaßen im maßgeblichen Auftrag bzw. Ausmaß.

- CertMe GmbH (Erbringung von Consultingdienstleistungen und Audits)
- TEMS Security Services GmbH (PEN- und Securitytesting)
- TEMS GmbH (Beratungsdienstleistungen IT, IT-Security)
- Condignum GmbH (Informationssicherheitsmanagementsysteme, PEN-Testing)

II. Datenverarbeitungen

Allgemeine Datenverarbeitung im Rahmen der Geschäftsbeziehung

Die Verarbeitung und Übermittlung der personenbezogenen Daten des Kunden (z.B. Stammdaten; Vertragsdaten; Kontaktdaten) erfolgt zur Durchführung der vertraglich vereinbarten Leistungen (Begründung, Verwaltung und Abwicklung der Geschäfts-beziehung) sowie der Erfüllung der steuerlichen- und unternehmensrechtlichen Pflichten. Dies schließt auch Verarbeitungen zur Vermeidung von Interessenskonflikten sowie Maßnahmen zur Qualitätssicherung und zum Risikomanagement mit ein.

Rechtsgrundlage:

- Erfüllung rechtlicher Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO);
- Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO).

Etwaige Übermittlungsempfänger:

- Externe Lieferanten, Kooperationspartner und Dienstleister;
- Empfänger gemäß zwingenden gesetzlichen Vorschriften;
- Rechtsvertreter;
- Versicherungen.

Datenverarbeitung zur Erfüllung des konkreten Auftrags

Der Zweck der jeweiligen Verarbeitungen ist abhängig vom konkreten Auftrag findet sich in den Punkten 1.2.1 bis 1.2.6.

Rechtsgrundlage:

- Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO);
- Überwiegendes berechtigtes Interesse, um die unter den Punkten 1.2.1 bis 1.2.6 genannten Zwecke zu erreichen (Art. 6 Abs 1 lit. f DSGVO);

- Externe Lieferanten, Kooperationspartner und Dienstleister;
- Factoring-Unternehmen, Zessionare und Leasingunternehmen;
- Gerichte und Behörden;
- Inkassounternehmen;
- Körperschaften des öffentlichen Rechtes;
- Rechtsvertreter;
- sonstige, einzelvertraglich bestimmte Empfänger (z.B. Konzerngesellschaften des Kunden);
- Versicherungen.

Audit Aufträge (Informationssicherheit nach ISO 27001)

Die Verarbeitung und Übermittlung der in Punkt (Allgemeine Datenverarbeitung) genannten Kategorien von personenbezogenen Daten des Kunden erfolgt

- zur selbständigen Durchführung von sonstigen Prüfungen (Internen Audits) und vereinbarten Untersuchungshandlungen (Pen-Tests im Zuge interner Audits),
- Der Beratung auf den Gebieten der Cyber- und Informationssicherheit nach ISO/IEC 27001 und der EU NIS2 Richtlinie bzw. deren nationaler Umsetzung
- zur Erbringung sämtlicher Beratungsleistungen und Tätigkeiten im Zusammenhang mit Cyber- und Informationssicherheit,
- zur Beratung betreffend Einrichtung und Organisation eines Informationssicherheitsmanagementsystems (ISMS).

Consulting Aufträge

Die Verarbeitung und Übermittlung der in Punkt (Allgemeine Datenverarbeitung) genannten Kategorien von personenbezogenen Daten des Kunden erfolgt

- zur Erbringung von Beratungsleistungen insbesondere in den Bereichen Cyber- und Informationssicherheit nach ISO/IEC 27001 und EU NIS2 Richtlinie (NISG),
- zur Erbringung von Beratungsleistungen im Bereich Organisation, Prozess- und Risikomanagement,

- zur Erbringung von Beratungsleistungen zur Optimierung und Sicherheit der Supply Chain im Kontext der EU NIS2 Richtlinie und deren nationaler Umsetzung,
- zur Beratung und Unterstützung von Unternehmen und Führungskräften bei der Entwicklung und Umsetzung von IT-Strategien, bei der Integration von IT-Systemen,
- zur Erbringung von Leistungen im Bereich Business Intelligence, Data Management, Technologie, Next-Generation Analytics, Big Data, Cloud und Machine Learning sowie Digital.

Forensik Aufträge

Die Verarbeitung und Übermittlung der in Punkt (Allgemeine Datenverarbeitung) genannten Kategorien von personenbezogenen Daten des Kunden erfolgt zur Durchführung von Datenanalysen

- bei wirtschaftskriminellen Verdachts- und Anlassfällen,
- bei Compliance Beratungsprojekten sowie
- bei gutachterlichen Tätigkeiten.

Aufträge in dem oben genannten Bereich werden von der CertMe GmbH an das verbundene Unternehmen, die TEMS Security Services GmbH, weitergegeben.

Risk Advisory Aufträge

Die Verarbeitung und Übermittlung der in Punkt (Allgemeine Datenverarbeitung) genannten Kategorien von personenbezogenen Daten des Kunden erfolgt

- zur Beratung in strategischen Entscheidungen,
- zur Durchführung von Risikobewertungen,
- zur Beratung bei der Antizipation von Änderungen im regulatorischen Umfeld und deren korrekte Umsetzung (EU NIS2 Richtlinie),
- zur Beratung und Unterstützung bei der operativen Risikosteuerung und
- zur Unterstützung um Cyber-Angriffe zu verhindern und Vermögenswerte zu schützen.

Datenverarbeitungen für Zwecke der Zusammenarbeit (Collaboration Systeme)

Die Collaboration Systeme stellen Kommunikations- und Informationsdienste zur Verbesserung der Zusammenarbeit zwischen der CertMe GmbH und Kunden zur Verfügung, um dadurch geschäftliche Prozesse zu beschleunigen und eine effiziente Kommunikation sowie einen laufenden Informationsaustausch zu gewährleisten. Die Collaboration Systeme greifen dabei auf Kontaktdaten sowie die ggf. hochgeladenen Daten zurück.

Rechtsgrundlage:

- Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO).
- Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO), denn ohne diese Datenverarbeitung ist eine effiziente und flexible Zusammenarbeit zwischen der CertMe GmbH und Kunden nicht möglich.

Etwaige Übermittlungsempfänger:

- Externe Lieferanten, Kooperationspartner und Dienstleister;
- sonstige, einzelvertraglich bestimmte Empfänger (z.B. Konzerngesellschaften des Kunden);
- Potenzielle oder bestehende Kunden (inkl. Ansprechpersonen bzw. Kontaktpersonen derselbigen)

Marketing im Rahmen der Geschäftsbeziehung

Zur Stärkung der bestehenden Kunden Beziehung bzw. zum Aufbau einer neuen Kunden Beziehungen sowie um Kunden über aktuelle Rechtsentwicklungen und das CertMe Dienstleistungsangebot zu informieren, verarbeiten wir Kontaktdaten der Kunden, um Information und/oder Werbenewsletter zu versenden.

Rechtsgrundlage:

- Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), soweit keine aufrechte Geschäftsbeziehung besteht;
- Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) iVm § 174 Abs 4 Telekommunikationsgesetz, soweit eine aufrechte Geschäftsbeziehung besteht und der Informations- und/oder Werbenewsletter im Zusammenhang mit dieser Geschäftsbeziehung steht), denn ohne diese Datenverarbeitung wäre die Stärkung bzw. der Aufbau der Kunden Beziehungen nicht oder nur eingeschränkt möglich.

Etwaige Übermittlungsempfänger:

- Externe Kooperationspartner und Dienstleister;

Datenverarbeitung im Falle von Vertragsstreitigkeiten

Zur Geltendmachung oder Abwehr von Rechtsansprüchen aus dem Vertragsverhältnis während des aufrechten Vertragsverhältnisses oder nach dessen Beendigung können die in Punkt (Allgemeine Datenverarbeitung) genannten Kategorien von personenbezogenen Daten des Kunden verarbeitet werden.

Rechtsgrundlage:

- Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO), denn ohne diese Datenverarbeitung wäre die Geltendmachung oder Abwehr von Rechtsansprüchen nicht oder nicht im ausreichenden Ausmaß möglich bzw. gewährleistet.

Etwaige Übermittlungsempfänger:

- Gerichte, Verwaltungsbehörden, Staatsanwaltschaften und polizeiliche Dienststellen;
- Gutachter und Sachverständige;

- Rechtsvertreter.

Datenverarbeitung für Zwecke der Verwaltung, Systemsicherheit und Zutrittskontrollen

Aufgrund der geltenden gesetzlichen Datensicherheitsbestimmungen (Art. 32 DSGVO) können personenbezogene Daten der Kunden (Stammdaten, IT-System und Protokoll Daten) für die Verwaltung und Systemsicherheit verarbeitet werden, wie etwa zur Verwaltung von Benutzerkennzeichen, zur Zuteilung von Hard- und Software an Benutzer von Systemen sowie zur Sicherheit der Systeme. Weiters können zum Zweck der Einhaltung gesetzlicher Datensicherheitsbestimmungen und zum Schutz von Eigentum und Betriebs- und Geschäftsgeheimnissen personenbezogene Daten der Kunden für Zutrittssysteme (Schlüssel, Chips, Berechtigungssysteme) verarbeitet werden.

Rechtsgrundlage:

- Erfüllung rechtlicher Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO);
- Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO), denn ohne diese Datenverarbeitung ist ein sicherer Betrieb des Systems und somit die Wahrung eines angemessenen technischen und organisatorischen Schutzniveaus nicht möglich.

Etwaige Übermittlungsempfänger:

- Externe Lieferanten, Kooperationspartner und Dienstleister;

Datenaustausch innerhalb CertMe und verbundenen Unternehmen

Für interne Verwaltungszwecke können die in Punkt (Allgemeine Datenverarbeitung) genannten personenbezogene Daten der Kunden innerhalb der CertMe und ihren verbundenen Unternehmen ausgetauscht und durch diese verarbeitet werden. Dies jedoch nur soweit der Datenaustausch sowie die Verarbeitung zur Wahrnehmung unserer berechtigten Interessen erforderlich ist.

Rechtsgrundlage:

- Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO), dieses Interesse liegt in der effizienten internen Verwaltungszusammenarbeit sowie dem Erhalt der Wettbewerbsfähigkeit.

Etwaige Übermittlungsempfänger:

- Empfänger außerhalb Österreichs. Sollte sich einer der oben genannten Empfänger außerhalb Österreichs befinden oder die personenbezogenen Daten außerhalb Österreichs verarbeiten. Wird sichergestellt dass das Datenschutzniveau in anderen Ländern jenem Österreichs entspricht. Eine Verarbeitung außerhalb der Europäischen Union schließen wir grundsätzlich aus.

III. Speicherdauer

Die personenbezogenen Daten der Kunden werden grundsätzlich bis zur Beendigung der Vertragsbeziehung oder bis zum Ablauf der anwendbaren gesetzlichen Verjährungs- und Aufbewahrungsfristen, darüber hinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden, gespeichert. Soweit die Datenverarbeitung auf einer Einwilligungserklärung beruht, erfolgt die Speicherung bis auf Widerruf, sofern danach keine andere gesetzliche Rechtfertigungsgrundlage zur Speicherung der Daten besteht.

IV. Rechte im Zusammenhang mit personenbezogenen Daten

Sie sind unter anderem berechtigt

- zu überprüfen, ob und welche personenbezogenen Daten wir über Sie verarbeiten und Kopien dieser Daten zu erhalten,

- die Berichtigung, Ergänzung, oder Löschung Ihrer personenbezogenen Daten zu verlangen, soweit diese falsch sind oder nicht rechtskonform verarbeitet werden,
- von uns zu verlangen, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken,
- unter bestimmten Umständen der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen oder die für die Verarbeitung zuvor gegebene Einwilligung zu widerrufen, wobei ein Widerruf die Rechtsmäßigkeit der vor dem Widerruf erfolgten Verarbeitung nicht berührt,
- Datenübertragbarkeit zu verlangen
- die Identität von Dritten, an welche Ihre personenbezogenen Daten übermittelt werden, zu kennen und
- bei der Datenschutzbehörde Beschwerde zu erheben.

V. Weitere Informationspflichten nach Artikel 13 DSGVO

Sollten Sie zu dieser Erklärung Fragen haben oder Anträge stellen wollen, wenden Sie sich bitte an uns über: datenschutz@certme.at bzw. Heiligenstädter Straße 29/OG.2/209, 1190 Wien.

Widerrufsmöglichkeit: Sofern und soweit die Datenverarbeitung durch die CertMe GmbH auf einer Einwilligung beruht, steht es Ihnen jederzeit offen, die erteilte Einwilligung gegenüber der CertMe GmbH mittels E-Mail an datenschutz@certme.at oder mittels Briefs an die Postadresse der CertMe GmbH ohne Angabe von Gründen und ohne daraus einen wie immer gearteten Nachteil zu befürchten, zu widerrufen. Durch den Widerruf der erteilten Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Sofern und soweit kein gesetzlich gerechtfertigter Grund vorliegt, die Daten trotz erfolgten Widerrufs weiterzuverarbeiten, werden die Daten nach erfolgtem Widerruf unverzüglich und zur Gänze gelöscht.

Soweit personenbezogene Daten, die zur Erfüllung unseres konkreten Auftrags oder zur jeweiligen Zweckerreichung erforderlich sind, nicht oder unvollständig bereitgestellt

werden, kann ohne diese Daten der Auftrag und/oder jeweilige Zweck nicht oder nicht vollständig erfüllt bzw. erreicht werden. Eine vollautomatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO findet nicht statt.

Wien am, 9. Februar 2024

CertMe GmbH