BESCHREIBUNG DES ZERTIFIZIERUNGS-VERFAHRENS Trusted Site Data Privacy (TSDP)

INHALT

Haben Sie Fragen zu der Leistungsbeschreibung? Wir helfen Ihnen gern weiter.

Webseite zur Datenschutz-Zertifizierung gemäß Art. 42 DSGVO:
Datenschutz-Zertifizierung gemäß Art. 42 DSGVO

TÜV NORD CERT GmbH
Business Entity IT
Am TÜV 1
45307 Essen
www.tuev-nord-cert.de

1. ZWECK

Die Datenschutz-Zertifizierung stellt ein Verfahren dar, mit dem Verarbeitungsvorgänge bei IT-Produkten, Dienstleistungen oder im Unternehmen im Hinblick auf die Einhaltung der gesetzlichen Datenschutzanforderungen überprüft werden können.
Das Ergebnis ist ein Datenschutz-Zertifikat, das die Umsetzung der datenschutzrechtlichen Standards der DSGVO belegt.
Den Rahmen für die Zertifizierung schafft Art. 42 DSGVO, mit dem die EU die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie die Vergabe von Datenschutzsiegeln und -prüfzeichen durch zertifizierte Stellen fördert.
Die DSGVO-Zertifizierung richtet sich grundsätzlich an alle Unternehmen, in denen mithilfe IT-gestützter Verarbeitungsvorgänge personenbezogene Daten verarbeitet und/oder gespeichert werden.

2. EVALUIERUNGSGEGENSTAND

Der Evaluationsgegenstand ist das konkrete Objekt einer Evaluation. Bei dem Evaluierungsgegenstand handelt es sich um eine Datenverarbeitung durch informationsverarbeitende Services (IVS). IVS können nur Verarbeitungsvorgänge gemäß Art. 42 Abs. 1 DSGVO sein. Zur Erbringung der IVS können dabei sowohl Software- als auch kombinierte Software- / Hardwarelösungen zum Einsatz kommen.
Neben dem IVS selbst wird in den nachfolgenden Kriterien auch seine Einsatzkonzeption[1] betrachtet. Diese wird als immanenter Bestandteil des IVS gesehen, denn sie beschreibt u. U. wichtige Voraussetzungen für die datenschutzkonforme Handhabung der technischen Komponenten des IVS. Entsprechend spielt die Dokumentation des IVS und seiner Einsatzvorgaben eine wesentliche Rolle für die Begutachtung.
Insgesamt sind im Hinblick auf den IVS folgende Komponenten Teil des Evaluierungsgegenstandes:

- A Der IVS in seiner technischen Ausprägung als Kombinationen von
  - A1 Hardware-,
  - A2 Software-, und
  - A3 Netzwerkkomponenten sowie
  - A4 durch diese Komponenten unterstützte Prozesse.
- B Die Dokumentation des IVS mit der Beschreibung:
  - B1 Eigenschaften des IVS (Prozessdokumentation fachlich/technisch),
  - B2 Benutzungshinweise des IVS (Benutzerdokumentation fachlich/technisch),
  - B3 ggf. separate Einsatzkonzeption/Betriebskonzept (sofern nicht in B1/B2 enthalten),
  - B4 Änderungsinformationen.
- C Dokumente und sonstige Informationen, die zur Nutzung mit dem IVS bereitgestellt werden:
  - C1 Formulare,
  - C2 Informationstexte (z. B. Einwilligungstexte),
  - C3 Internetseiten,
  - C4 Vertragstexte (z. B. Vertrag zur Auftragsverarbeitung).

Zur Bestimmung des Evaluierungsgegenstandes ist seitens des Antragsstellers eine vollständige Datenflussanalyse des IVS unter Berücksichtigung aller an der Verarbeitung personenbezogener Daten

1Hier wurde der Begriff "Einsatzkonzeption" verwendet. Alternative Begriffe wären "Einsatzkonzept", "Betriebskonzept" oder auch "Nutzungskonzeption".

beteiligten Akteure, z. B. Auftragsverarbeiter, Subauftragsverarbeiter, gemeinsam Verantwortliche, vorzunehmen und sodann eine im Hinblick auf die Verantwortlichkeit qualifizierte Darstellung des gesamten nach Phasen geordneten Verarbeitungsprozesses inklusive Beschreibung des jeweiligen Akteur- und Rollenmodells (Akteure, Rollen, Beziehungen) für jede Verarbeitungsphase zu erstellen und vorzulegen. Die Darstellung kann entweder durch eine grafische Darstellung (z. B. anhand standardisierter Darstellung wie Business Process Modeling (BPM) oder Unified Modelling Language (UML) oder in textlicher Form erfolgen.
Die qualifizierte Darstellung des Verarbeitungsprozesses muss dabei den vollständigen Lebenszyklus der Verarbeitung von personenbezogenen Daten innerhalb des IVS abbilden.
Die Begriffsbestimmung zur „Verarbeitung“ in Art. 4 Abs. 2 DSGVO listet hierbei nicht abschließend einzelne Verarbeitungsvorgänge auf.
Zudem muss bestimmt und dokumentiert werden, welche Datenverarbeitungsschritte dem erweiterten Verantwortungsbereich des Antragstellers zuzuordnen sind. Hierbei ist auch eindeutig darzulegen, wie die Zugriffsmöglichkeiten der Verantwortlichen und Auftragsverarbeiter in den jeweiligen Datenvorgängen ausgestaltet sind. Alle Datenverarbeitungsschritte und relevante Schnittstellen sind vollständig zu erfassen. Der Antragssteller muss zudem die zu zertifizierenden Verarbeitungsvorgänge, welche Gegenstand der Evaluierung sind, kennzeichnen, sodass dann in Abstimmung mit der Zertifizierungsstelle und unter Berücksichtigung der Angaben gemäß 1.7 bis 1.17 des Kriterienkataloges [D503-10VA02A01_Kriterienkatalog TSDP_2.12] der jeweilige Evaluierungsgegenstand festgelegt werden kann.
Der Antragssteller muss für die Abgrenzung des Evaluierungsgegenstandes vor Aufnahme des Evaluierungsverfahrens ausführliche Angaben gemäß 1.7 bis 1.17 des Kriterienkataloges [D503-10VA02A01_Kriterienkatalog TSDP_2.12] machen. Ausgehend von diesen Angaben wird sodann der Evaluierungsgegenstand ermittelt und entsprechend im Evaluierungsbericht Trusted Site Data Privacy [D503-10VA02F002_Evaluierungsbericht_Vorlage_TSDP] dokumentiert.

3. ÜBERBLICK ÜBER DEN ZERTIFIZIERUNGSPROZESS

Die Überprüfung der Anforderungen wird anhand des Kriterienkataloges „Trusted Site Data Privacy“ der TN CERT vorgenommen.
In den nachfolgenden Abschnitten werden die verschiedenen Phasen des Zertifizierungsverfahrens beschrieben.

3.1. Angebotsanfrage und Zertifizierungsvereinbarung

Der Kunde für die Zertifizierung richtet seine Anfrage zum Zertifizierungsvorgang an die Zertifizierungsstelle. Die Zertifizierungsstelle informiert über das Zertifizierungsverfahren und der Kunde erhält auf Wunsch folgende Unterlagen:

- „Anfrageformular Datenschutz Zertifizierung nach Artikel 42 DSGVO – Trusted Site Data Privacy“
- ein „Kickoff“ (Workshop) Angebot,
- ein Zertifizierungsangebot,
- das Formblatt Zertifizierungsvereinbarung mit den Zertifizierungsbedingungen,
- Beschreibung des Zertifizierungsverfahrens.

Für die Angebotserstellung liefert der Kunde eine Beschreibung des Zertifizierungsgegenstandes (Scope). Dazu muss dieser das „Anfrageformular Datenschutz Zertifizierung nach Artikel 42 DSGVO – Trusted Site Data Privacy“ [D503-10F100] ausfüllen. Bei Bedarf werden Fragen zur Festlegung des Zertifizierungsgegenstandes oder zum Zertifizierungsverfahren in einem Vorgespräch geklärt.
Anschließend wird geprüft, ob der angestrebte Evaluierungsgegenstand generell zertifizierbar ist.
Anschließend wird ein Angebot für ein „Kickoff“-Workshops erstellt. Dieses entfällt ggf., bspw. bei einer Re-Zertifizierung, da hier der Zertifizierungsgegenstand bereits bekannt ist. Im Rahmen des „Kickoff“-Angebotes / -Workshops wird das Zertifizierungsverfahren und (durch den Kunden) der jeweilige Evaluierungsgegenstand vorstellt. Ziel ist es ein gemeinsames Verständnis zu erlangen, alle Fragen zu klären sowie und den konkreten Scope der Zertifizierung zu bestimmen. Sollte sich in diesem Schritt herausstellen, dass der angestrebte Evaluierungsgegenstand nicht zertifizierbar ist, endet in diesem Fall der Prozess an dieser Stelle. Im positiven Falls wird abschließend der Aufwand kalkuliert und ein Zertifizierungsangebot erstellt.
Anschließend erteilt der Kunde, auf der Grundlage des Zertifizierungsangebots der Zertifizierungsstelle, den Auftrag zur Zertifizierung und erkennt durch Unterzeichnung des Formblatts Zertifizierungsvereinbarung die Zertifizierungsbedingungen an. Der Antrag wird dann angenommen und es erfolgt die Bestätigung des Auftrags mit Mitteilung des verantwortlichen Evaluationsleiters.

3.2. Vorbereitung der Evaluierung

Die Evaluierung wird von einem Evaluierungsteam unter Verantwortung des Evaluationsleiter gemäß den Anforderungen und Vorgaben der Zertifizierungsstelle durchgeführt. Das Evaluierungsteam plant mit dem Kunden den zeitlichen Ablauf der Evaluierung und räumt bei Bedarf in Vorgesprächen letzte Unklarheiten bezüglich des Evaluierungs- und Zertifizierungsablaufs aus.
Die Evaluierung umfasst alle Tätigkeiten, um zu vollständigen Informationen über die Erfüllung der festgelegten Anforderungen durch den Zertifizierungsgegenstand zu gelangen. Dies schließt planende und vorbereitendende Tätigkeiten mit ein. Grundlage der Evaluierung ist der vom Kunden ausgefüllte TSDP-Kriterienkatalog mit ggf. weiterführenden Dokumenten.
Die Sprache für die Evaluierung und die Evaluierungs-Dokumentation wird vor der Evaluierung mit dem Kunden abgestimmt. Hierbei wird die deutsche oder englische Sprache/Schrift angeboten.
Der Evaluationsleiter trifft die endgültige Entscheidung darüber, welche Elemente des Evaluierungsgegenstandes und welche organisatorischen Tätigkeiten innerhalb eines festgelegten zeitlichen Rahmens evaluiert und welche technischen Tests innerhalb eines festgelegten zeitlichen Rahmens durchgeführt werden sollen. Der Kunde wird durch den Evaluationsleiter über den Umfang der Evaluierung informiert.
Die Evaluierung erfolgt anhand von verschiedenen Evaluierungsmethoden. Diese sind ausführlich im TSDP-Kriterienkatalog beschrieben.

3.3. Evaluierung

Die Evaluierung wird von Evaluierenden durchgeführt, die Mitarbeiter der Zertifizierungsstelle sind oder durch die Zertifizierungsstelle zugelassen sind und die Kompetenzanforderungen des o. g. Dokumentes in der aktuell gültigen Fassung erfüllen.
Die Evaluierenden untersuchen die zu zertifizierenden Verarbeitungsvorgänge in Hinblick auf die Konformität mit den oben genannten relevanten Normen. Im Rahmen der Evaluierung wird festgestellt, ob die Verarbeitungsvorgänge des Antragsstellers den europarechtlichen Vorgaben der DSGVO

genügen und ob der Antragsteller die von ihm eingeforderten technisch-organisatorischen Maßnahmen getroffen hat, um eine dauerhafte Konformität der eigenen Handlungen mit den Vorgaben der DSGVO sicherzustellen.
Die Evaluierung der Verarbeitungsvorgänge unterteilt sich in drei Phasen:

- die Dokumentationsprüfung
- technischen Evaluierungstätigkeiten
- Evaluierung.

Bei der Bewertung der Prüfkriterien ist zu unterscheiden zwischen „Erfüllt“, „Erfüllt mit Empfehlung“ und „Nicht erfüllt“. „Erfüllt mit Empfehlung“ bescheinigt die Konformität, zeigt jedoch einen Verbesserungsvorschlag auf, den der Kunde bis zur nächsten Überwachung oder Rezertifizierung analysiert haben sollte.
„Nicht erfüllt“ definiert eine Nichtkonformität, was dazu führt, dass das Zertifikat nicht ausgestellt oder bei einem bereits bestehenden Zertifikat ausgesetzt wird.
Die Konformitäten müssen innerhalb einer vorgesehenen Frist, die der Evaluator festlegt, jedoch 6 Monate nicht überschreiten darf, hergestellt werden, sonst wird das Zertifikat definitiv nicht ausgestellt bzw. final entzogen.

3.4. Evaluierungsbericht

Nach erfolgter Evaluierung erstellen die Evaluatoren auf Grundlage der Ergebnisse der Dokumentenprüfung und der technischen Evaluierung einen Evaluierungsbericht. Dieser Bericht wird dem Kunden zur Verfügung gestellt und bildet die Grundlage für die Bewertung und Zertifizierungsentscheidung.

3.5. Zertifikaterteilung

Seitens der Zertifizierungsstelle erfolgt eine Bewertung der Evaluierung anhand des erstellten Evaluierungsberichtes, der gesammelten Nachweise und der Überprüfung der Einhaltung der Verfahrensvorgaben der Zertifizierungsstelle. Nach Freigabe wird der Evaluierungsbericht dem Kunden als Entwurf zur Verfügung gestellt.
Im Fall einer negativen Zertifizierungsentscheidung wird der Kunde über die Gründe der Entscheidung schriftlich informiert. Dem Kunden wird eine Frist von 4 Wochen gewährt, gegen diese Entscheidung schriftlich Widerspruch zu erheben.
Im Fall einer positiven Zertifizierungsentscheidung wird das Zertifikat mit einer Gültigkeitsdauer von maximal drei Jahren ausgestellt. Das Zertifikat wird vor der Ausstellung zur Freigabe an den Kunden gesendet. Im Laufe des Gültigkeitszeitraums der Zertifizierung von 3 Jahren sind mindestens zwei Überwachungen durchzuführen.
Zur Unterstützung der Transparenz der Zertifizierungen führt die Zertifizierungsstelle eine Liste der zertifizierten Produkte, die der Öffentlichkeit zur Verfügung gestellt wird. Neue Zertifikate werden nach positiver Zertifizierungsentscheidung auf den Web-Seiten veröffentlicht.

4. ZERTIFIKATSLAUFZEIT UND ÜBERWACHUNG

Innerhalb der Zertifikatslaufzeit (von 3 Jahren) führt die Zertifizierungsstelle anlasslose Überwachungen durch. Diese soll jährlich innerhalb der jeweils letzten sechs Monate des abgelaufenen Jahres stattfinden, um die Zertifikatsgültigkeit zu erhalten.
Die zeitliche Planung für die Überwachung richtet sich nach dem Zertifikatsdatum. Die Überwachung muss immer spätestens am Tag des ein bzw. zwei Jahre auf das Zertifikatsdatum folgenden Tag abgeschlossen sein. Frühester Beginn für die Überwachung ist sechs Monate vor diesem Tag. Ebenso darf die Rezertifizierung frühestens sechs Monate vor Zertifikatslaufzeitende begonnen werden. Es sind maximal zwei Überwachung möglich. Spätestens nach 3 Jahren ist eine vollständige Evaluierung notwendig, um die Zertifikatsgültigkeit zu verlängern.
Im Rahmen der Überwachung werden die Tätigkeiten wie bei der Erst-Zertifizierung gemäß diesem Dokument ausgeführt. Inhaltlich wird festgestellt, ob die in der Zertifizierung dargelegten Sachverhalte weiterhin Bestand haben bzw. ob Änderungen konform zur Zertifizierung sind. Darüber hinaus werden ggf. aktualisierte oder neue Standards berücksichtigt. Die Überprüfung kann anhand einer repräsentativen Stichprobe.
Sofern im Rahmen der Überwachung Nichtkonformitäten festgestellt werden, so ist mit dem Kunden ein Plan zur Behebung dieser Nichtkonformitäten innerhalb einer gesetzten Frist zu vereinbaren. Diese Frist soll im Regelfall 3 Monate nach Bekanntgabe der Nichtkonformität im Evaluierungsbericht nicht überschreiten. Sofern die Komplexität der vorgesehenen Behebungsmaßnahme dies erfordert, kann die Frist auf bis zu 6 Monate nach Bekanntgabe der Nichtkonformität im Evaluierungsbericht verlängert werden.
Der Kunde muss während der Zertifikatslaufzeit die datenschutzkonforme Verarbeitung seiner Prozesse gewährleisten. Im Falle von Auffälligkeiten, die eine Nichteinhaltung der Zertifizierungsanforderungen befürchten lässt, erfolgt eine anlassbezogene Überwachung.

5. ÄNDERUNGEN IN DER ZERTIFIZIERUNG

Im Falle von Änderungen tatsächlicher oder rechtlicher Umstände, welche imstande sind, die Konformitätsbewertung des Prüfgegenstands zu verändern, nachdem das Zertifikat bereits im Rahmen einer Zertifizierung oder Rezertifizierung ausgestellt wurde, sind die Zertifizierungsstelle oder der Kunde verpflichtet, die jeweils andere Partei unverzüglich über den Eintritt des jeweiligen Umstands zu informieren. Falls der Eintritt eines solchen Umstands bereits sicher vorhergesagt werden kann (z. B.: Verabschiedung eines Gesetzes, welches zu einem Stichtag in Kraft tritt; geplante Umstellung eines betriebsinternen Ablaufes), sind beide Parteien verpflichtet, die jeweils andere innerhalb von drei Monaten schriftlich von dem Umstand in Kenntnis zu setzen.
In diesem Fall entscheidet die Zertifizierungsstelle darüber, welche Maßnahmen nötig sind, um angesichts der Änderungen die Zertifizierung weiterhin aufrecht erhalten zu können. Als Folge dieser Entscheidung können eine erneute Evaluierung, Bewertung, Entscheidung oder Erstellung überarbeiteter formeller Zertifizierungsdokumentation für nötig befunden werden. Zudem kann die Leitung des Zertifizierungsfachbereichs auch entscheiden, den Geltungsbereich der Zertifizierung zu erweitern oder einzuschränken.
Falls eine Aufrechterhaltung des Zertifikats die Umsetzung von bestimmten Maßnahmen erfordert, so sind diese vom Kunden innerhalb von drei Monaten umzusetzen.
Änderungen in der Zertifizierung, welche durch den Kunden initiiert werden, umfassen:

- wesentliche Änderungen in der TSDP-Dokumentation,
- sicherheitsrelevante Änderungen.

Eine vollständige neue Bewertung des Evaluierungsgegenstandes erfolgt bei

- wesentlichen Änderungen des Geltungsbereichs,
- wesentlichen Änderungen in den bereit gestellten Services im Geltungsbereich,
- Aufnahme neuer Services in den Geltungsbereich,
- wesentlichen Änderungen der IT-Systeme oder der Geschäftsprozesse des TSDP und / oder
- bei Umzug eines wesentlichen Teils der Services an einen anderen Ort.

Die Zertifizierungsstelle entscheidet anhand der Beschreibung, ob eine erneute Dokumentenprüfung oder eine erneute technische Evaluierung notwendig ist oder ob die Änderungen im Rahmen der nächsten Überwachungs- bzw. Re-Zertifizierungsevaluierung überprüft werden können. Im Fall einer erneuten Dokumentenprüfung oder Evaluierung erstellen die Evaluatoren einen entsprechenden Evaluierungsbericht, der dem Kunden zur Verfügung gestellt wird.
Sofern im Rahmen der Prüfung von Änderungen Nichtkonformitäten festgestellt werden, so ist mit dem Kunden ein Plan zur Behebung dieser Nichtkonformitäten innerhalb einer gesetzten Frist zu vereinbaren. Diese Frist soll im Regelfall 3 Monate nach Bekanntgabe der Nichtkonformität im Evaluierungsbericht nicht überschreiten. Sofern die Komplexität der vorgesehenen Behebungs-maßnahme dies erfordert, kann die Frist auf bis zu 6 Monate nach Bekanntgabe der Nichtkonformität im Evaluierungsbericht verlängert werden.
Nach jeder Änderung wird die Zertifizierungsentscheidung getroffen, ob ein aktualisiertes Zertifikat mit den Änderungen ausgestellt werden kann.