BvD e.V.
Die Datenschützer

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsrechtstag 2017

Gemeinsame Veranstaltung von TeleTrusT und BvD

Berlin, 07.11.2017

Datenschutz Auditierung

Jörg Schließke

TÜV Informationstechnik GmbH

Datenschutz Auditierung

Datenschutz Auditierung im Kontext zur EU-DSGVO

Jörg Schließke, Produktmanager Datenschutzqualifizierung Business Security & Privacy

TÜV NORD GROUP

INHALT

1. Über TÜViT
2. Audit
3. Datenschutz Audit
4. Datenschutz Audit nach der EU DS-GVO
5. Umsetzung Audit
6. Datenschutz Zertifizierung

Über uns

VERTRAUEN IST DER GRUNDSTEIN UNSERES HANDELNS

TÜViT

- schafft Vertrauen in Technik, Funktion und Betrieb von IT-Systemen und IT-Prozessen durch objektive Prüfung und Zertifizierung sowie Beratung
- arbeitet hersteller- sowie produktneutral und unabhängig von Interessengruppen
- entwickelt, verkauft oder integriert keine Produkte
- ist mit über 100 Mitarbeitern weltweit tätig in den Bereichen IT-Sicherheit, IT-Qualität, Datenschutz und Zertifizierung

TÜViT IN DER TÜV NORD GROUP

TÜV NORD AG

Geschäftsbereich Industrie Service	Geschäftsbereich Mobilität	Geschäftsbereich Rohstoffe	Geschäftsbereich Bildung	Geschäftsbereich Aerospace	Geschäftsbereich IT	Konzernservice
TÜV NORD Systems	TÜV NORD Mobilität	DMT	TÜV NORD Bildung	ATN	TÜViT	TÜV NORD Service
weitere Gesellschaften	weitere Gesellschaften	weitere Gesellschaften	weitere Gesellschaften	weitere Gesellschaften		weitere Gesellschaften

UNSERE THEMEN, WAS UNS ANTREIBT

IT-Sicherheit und -Qualität – unabhängig geprüft

Security4Safety

Industrie 4.0: Vernetzung braucht Sicherheit

Cyber Security

Prüfung von IT-Systemen/Netzwerken und Applikationen

Automotive Security

Das sichere "Connected Car"

Mobile Security

Mobile Sicherheit durch "Trusted Mobile" Siegel

Datenschutz

Aus der "Pflicht" eine "Kür" machen

KRITIS

Umsetzung der Vorgaben aus IT-Sicherheitsgesetz

Sicherheitsevaluierungen

Schutz von sensitiven Daten für Hard- und Software

eIDAS

Elektronische Signaturen und Siegel

Data Center Security

300+ Zertifikate für sichere Rechenzentren

IT SERVICES ÜBER ALLE EBENEN

- Informationssicherheits-Management
- Datenschutz (externer Datenschutzbeauftragter)
- Projekt- und Qualitätsmanagement
- Prozessverbesserung

- Netzwerk- und Applikationssicherheit
- Webanwendungen
- Rechenzentren
- Mobile Security
- Sicherheitsanalysen und -konzepte
- Datenschutz-Qualifizierung

- Produktevaluationen nach Common Criteria
- Validierungstests nach FIPS140-2
- Tests und Sicherheitsanalysen im Hardware-Labor
- Bewertungen nach Bankenspezifikationen
- Konformitätsprüfungen

Audit

AUDIT

- Ein Audit ist "systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind." (Quelle: ISO 19011, Leitfaden zur Auditierung von Managementsystemen)
- Daraus ergeben sich folgende Anforderungen:
  - Systematischer Prozess
  - Unabhängigkeit der Auditoren
  - Dokumentierter Prozess
  - Erlangung von Auditnachweisen
  - Objektive Auswertung Feststellung
  - Auditschlussfolgerung ob diese erfüllt sind
- Grundlage ist in allen Fällen die Notwendigkeit, Abweichungen von Anforderungen (IST vom SOLL) zu erkennen und Verbesserungen herbeizuführen.

AUDIT

- Kategorisierung von Audits in:
  - interne Audits
    - Ziel: Erbringung von Nachweisen für eigene Zwecke, z.B. IT-Sicherheit, Umsetzung gesetzlicher Anforderungen, Überprüfung der technischen und organisatorische Maßnahmen
  - externe Audits
    - Ziel: Erbringung von Nachweisen für Stellen außerhalb der Organisation (z.B. Lieferanten- oder Kundenaudit, Audits im Rahmen von Zertifizierungen)
- Klassifikation von Audits:
  - Prozess-/Verfahrensaudits
  - Produktaudits
  - Systemaudits (z.B. DSMS)

GRUNDSÄTZE EINES AUDITS

- Unabhängigkeit des Auditors
- Objektivität des Auditors (z.B. keine Beeinflussung durch Sympathie)
- Sachlichkeit (Dokumentation durch Auditor richtig, genau und vor allem verständlich)
- Kompetenz (Fachwissen)
- Integrität (Einhaltung der rechtlichen Anforderungen und ehrliche Erbringung)
- Vertraulichkeit/Verschwiegenheit
- Methodischer Ansatz (Durchführung nach Schema und Dokumentation des Auditverlaufs)

Quelle: Datenschutz-Audit, Pachinger/Beham

Datenschutz Audit (bis 24.05.2018)

DATENSCHUTZAUDIT GEMÄß § 9A BDSG

- Zur Verbesserung des Datenschutzes und der Datensicherheit **können** Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch **unabhängige und zugelassene Gutachter** prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die **näheren Anforderungen** an die Prüfung und Bewertung, **das Verfahren** sowie die **Auswahl und Zulassung der Gutachter** werden durch **besonderes Gesetz geregelt**.
- Datenschutzauditgesetz auf Bundesebene gescheitert
- Aufgrund fehlender Anforderungen Audit oder Zertifizierung nach § 9a BDSG nicht möglich
- Datenschutzaudit verankert in:
  - Schleswig-Holstein (Datenschutz-Behördenaudit gemäß § 43 Abs. 2 LDSG)
  - Bremen(Datenschutzaudit gemäß § 7b BremDSG i.V.m. BremDSAuditV)

AUDIT VON DIENSTLEISTERN

- Kontrolle der Einhaltung der technischen und organisatorischen bei einem Dienstleister im Rahmen der Auftragsdatenverarbeitung
  - Kontrolle gemäß § 11 Abs. 2 Satz 4 BDSG
  - Kontrolle des Auftraggebers
    - vor Beginn der Datenverarbeitung und
    - sodann regelmäßig (ca. alle 2-3 Jahre)
  - von der Einhaltung der bei Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen

- Es gibt keine verbindlichen Vorgaben wie das Audit durchzuführen ist (z.B. durch Selbstauskunft oder Erbringung von Nachweisen/Zertifikaten)
- Das Ergebnis ist gemäß § 11 Abs. 2 Satz 5 BDSG zu **dokumentieren**

Datenschutz Audit im Rahmen der EU-DSGVO

AUDIT IM KONTEXT DER EU DS-GVO

- Begriff Audit in der dt. Fassung der DS-GVO nicht vorhanden, aber in der engl. Fassung
- Begriff Überprüfungen bzw. Inspektionen
- Art. 28 Abs. 3 lit. h DS-GVO "Auftragsverarbeiter"
  - Einhaltung der Pflichten aus Art. 28 einschließlich durchgeführter Überprüfungen und Inspektionen
- Art. 39 Abs. 1 lit. b DS-GVO "Aufgaben des Datenschutzbeauftragten"
  - Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen **Überprüfungen**
- Art. 47 Abs. 1 lit. j DS-GVO "verbindliche interne Datenschutzvorschriften"
  - Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften
- Art. 58 DS-GVO Abs. 1 lit. b DS-GVO "Befugnisse" (für Aufsichtsbehörden)
  - Aufsichtsbehörde hat Befugnisse Untersuchungen in Form von Audits durchzuführen

AUDIT DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

- Art. 24 Abs. 1 DS-GVO "Verantwortung des für die Verarbeitung Verantwortlichen"
  - Einsatz geeigneter TOM um den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DS-GVO erfolgt.
- Art. 32 Abs. 1 DS-GVO "Sicherheit der Verarbeitung"
  - Einsatz geeigneter TOM um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- Art. 25 "Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen"
- Art. 35 DS-GVO "Datenschutz-Folgenabschätzung"
  - Sicherstellung des Schutzes personenbezogener Daten
- Art. 30 DS-GVO "Verzeichnis von Verarbeitungstätigkeiten"
  - Einsatz geeigneter TOM

RECHENSCHAFTSPFLICHT (ACCOUNTABILITY) GEMÄß ART. 5 DS-GVO

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	**Verarbeitung** auf **rechtmäßige** Weise, nach dem Grundsatz von **Treu und Glauben** und in einer für den Betroffenen **nachvollziehbaren Weise**
Zweckbindung	Erhebung für **festgelegte**, **eindeutige** und **rechtmäßige Zwecke** und **Verbot** der **Weiterverarbeitung** in einer mit diesen **Zwecken** nicht zu vereinbarenden Weise
Datenminimierung	**Beschränkung** auf das für den **Zweck der Verarbeitung** angemessene und sachlich relevante sowie **notwendige Maß**
Richtigkeit	**Sachlich richtige** und ggf. **aktuellste** Daten; Vorsehen von Maßnahmen zur unverzüglichen **Löschung** oder **Berichtigung** von unzutreffenden Daten
Speicherbegrenzung	**Speicherung** mit Personenbezug **höchstens** so lange, wie es für die **Verarbeitungszwecke erforderlich** ist
Integrität und Vertraulichkeit	Geeignete **technisch-organisatorische Maßnahmen** (TOM) zum **Schutz der Daten**, insbes. vor **unbefugter** oder **unrechtmäßiger** Verarbeitung, zufälligem **Verlust**, zufälliger **Zerstörung** oder **Schädigung**

AUDIT IM KONTEXT DER EU DS-GVO

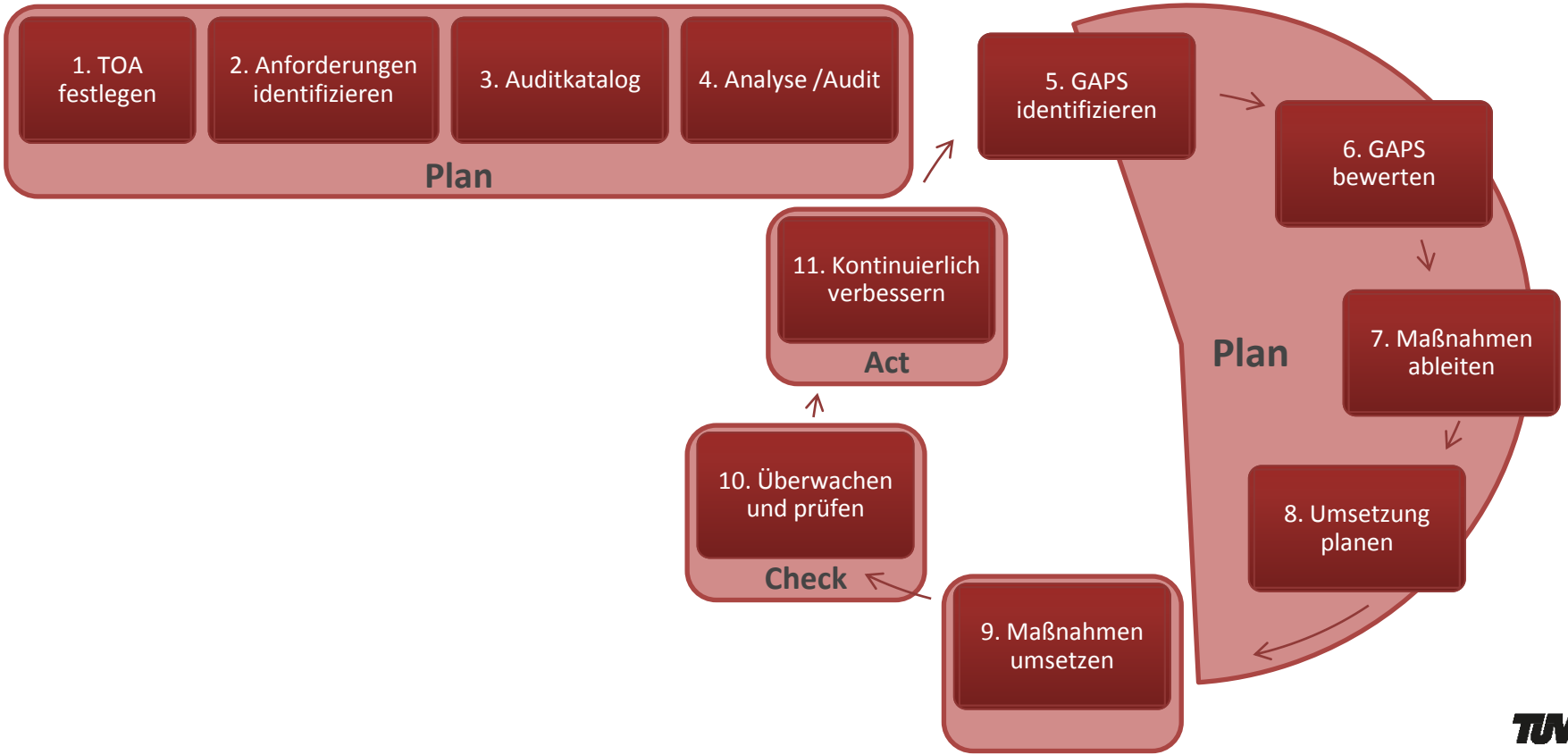
- hoher Fokus auf Kontroll- und Nachweisbarkeit (z.B. Art. 5 Abs. 2 DS-GVO zum Nachweis der Einhaltung der Verarbeitung von personenbezogenen Daten gemäß Art. 5 Abs. 1 DS-GVO)
- Pflicht zur Nachweisbarkeit betrifft nicht nur den Verantwortlichen sondern auch
- den Auftragsverarbeiter der die Einhaltung seiner technischen und organisatorischen Maßnahmen nachweisen muss
- z.Zt auch viele interne Audits zur GAP Analyse im Rahmen der Transformation zur DS-GVO
- oder DS-GVO Fragebogen des Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)
  - Fragen zum:
    - Verzeichnis von Verarbeitungstätigkeiten
    - Einbindung von Auftragsverarbeitern
    - Umsetzung von Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte
    - Prozess zum Umgang mit Datenschutzverletzungen

Umsetzung eines Audits

UMSETZUNG EINES AUDITS

Ziel	Risikoanalyse und Accountability zur Implementierung eines nachhaltigen DSMS im Rahmen der EU DS-GVO
Normen	u.a. EU DS-GVO (Datenschutzgrundverordnung) sowie DSAnpUG-EU (Datenschutz-Anpassungs- und Umsetzungsgesetz EU)
In Kraft treten	25. Mai 2016 Übergangsfrist bis 25. Mai 2018 (2 Jahre)
Umsetzung	Datenschutzaudit → GAP-Analyse Arbeitspaket, Umsetzung und Implementierung

ERWEITERTER PDCA-ZYKLUS ZUM AUDIT DSMS



AUDITPROZESS

- Ablauf eines Audits:
  - Initialisierung: Festlegung von Auditzielen, Definition des Auditgegenstands (Target of Audit – ToA), ggf. Pre-Audit
  - Auditplanung: Vorbereitungsmaßnahmen des Auditoren und des zu Auditierenden (ggf. Auskunft über zu vorliegende Dokumentationen durch Anforderungs- oder Fragenkatalog)
  - Durchführung des Audits
  - Bewertung der Auditergebnisse
  - Erstellung des Auditberichts

Quelle: Fotolia

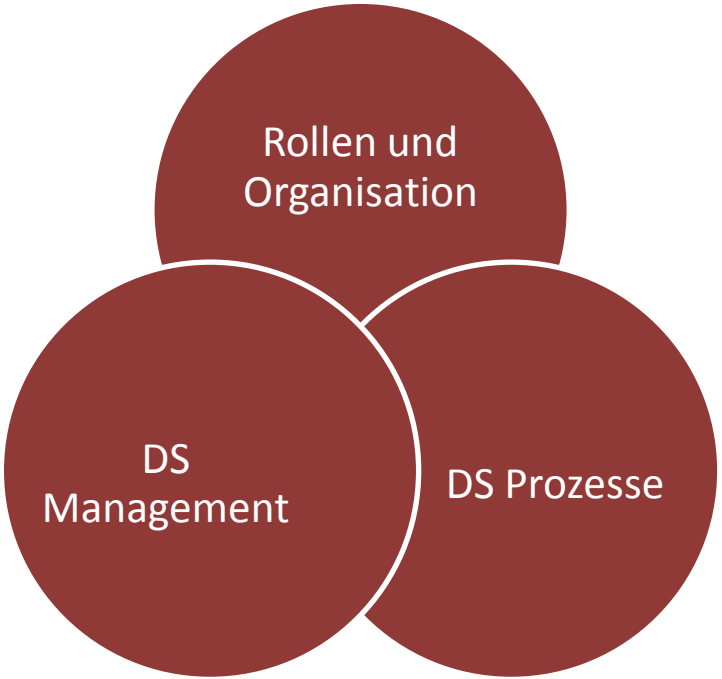
INITIALISIERUNG DES AUDITS

- Festlegung der Ziele:
  - Erkennung von Mängeln und Schwachstellen
  - GAP-Analyse im Rahmen des Transformationsprozesses
  - Sicherstellung der Nachweisbarkeit im Kontext der DS-GVO
  - weitere rechtliche Anforderungen
  - interne Anforderungen, z.B. gemäß der Datenschutzleitlinie (regelmäßige Audits)
  - Grundlage für eine Zertifizierung
- Definition des Prüfgegenstands:
  - klare Definition des Prüfgegenstands (ToA) und der zu überprüfenden Bereiche (z.B. Überprüfung der gesamten Organisation oder nur einzelner Systeme bzw. IT-Verfahren / Überprüfung der TOM im Rahmen eines Dienstleisteraudits)
  - evtl. vorab Scoping-Workshop zur gemeinsamen Festlegung des Prüfgegenstands oder internes Pre-Audit im Rahmen von Zertifizierungen

PLANUNG UND VORBEREITUNG

- Erstellen einer Audit Agenda mit Zeitplan, Ansprechpartnern und möglicher Zeitpuffer
- Audit Fragenkatalog erstellen ("roter Faden")
  - Kriterien festlegen
  - Auditnachweise
  - Feststellungen
  - Schlussfolgerungen
- Vorab dem zu auditierenden Fragenkatalog übermitteln zur Vorbereitung oder eine Übersicht der zu prüfenden Dokumente
- evtl. werden Dokumente vorab übermittelt (z.B. Datenschutzhandbuch oder Beschreibung der Datenschutzorganisation

BSP. PLANUNG UND VORBEREITUNG AUDIT DSMS



- Rollen und Organisation sowie Verantwortlichkeiten
- Einhaltung Accountability (Dokumentation)
- **Verzeichnis von Verarbeitungstätigkeiten als zentrales Organ**
- Einwilligungsmanagement
- Vertragsmanagement (Auftragsverarbeiter)
- Übermittlung in Drittländer
- Datenschutz-Folgenabschätzung
- Umsetzung von IT-Sicherheitsmaßnahmen
- Prozess zur Wahrung der Betroffenenrechte
- Prozess zur Meldung von Datenschutzverstößen
- .....

BSP. PLANUNG UND VORBEREITUNG AUDIT DSMS

- Identifizierung datenschutzrelevanter Dokumente
  - ADV Vereinbarungen
  - DS Policies
  - Datenschutzerklärungen
    - Internet
    - App
  - Grundsätzliche Einwilligungen
  - Betriebsvereinbarungen

BSP. PLANUNG UND VORBEREITUNG AUDIT DSMS

- DS Unterweisung DSGVO (Führungskräfte – Mitarbeiter – z.B. Hand-Out)
- Privacy Impact Assessment
- Meldung neuer Verfahren / Bewertung / Kontrolle
- Pflege Verzeichnis von Verarbeitungstätigkeiten
- IT Security – TOM‘s – Dokumentation - Schutzklassenkonzept
- Umsetzung Privacy by Design – Privacy by Default
- Löschkonzept und Prozess
- Prozess ADV (Ablage und Nutzung sowie Dokumentation)
- Prozess Datenpannen (vorhanden – Anpassen – Reaktionszeiten)
- Allgemeines DS Richtlinie / DS Handbuch (Zugriff für Führungskräfte)
- Prozess Auskunft von Betroffenen (vorhanden – Anpassen – Vorlagen erstellen)

DURCHFÜHRUNG DES AUDITS

- Einführungsgespräch (evtl. vorab Präsentationen)
- Durchführung des Audits:
  - Interviewtechnik anhand der Prüffragen und Erstellen von Gesprächsnotizen
  - Stichprobenartige Sichtung der bereitgestellten Unterlagen (z.B. Einsicht in die interne Verarbeitungsübersicht)
  - Besichtigung/Vor-Ort Begehung der relevanten Bereiche, z.B.
    - Sichtung der Serverräume
    - Sichtung der Arbeitsplätze
    - Sichtung optisch-elektronischer Einrichtungen
    - Einblick in zu prüfender Software
- Abschlussgespräch
  - evtl. Erläuterung erster relevanter Gap‘s
  - Erläuterung der weiteren Schritte

BEWERTUNG DER AUDITERGEBNISSE UND AUDITBERICHT

- Direkte Dokumentation bzw. Zusammenfassung der Ergebnisse, um keine wichtigen Informationen zu vergessen
- Einsicht in noch zur Verfügung gestellter Dokumente
- Auswertung der Ergebnisse und Schlussfolgerung von möglichen Abweichungen

- Erstellung des Auditberichts
  - Darstellung Auditgegenstand und Vorgehensweise
  - Übersicht der übermittelten Dokumente und möglicher Verweise
  - Management Summary
  - Darstellung der Prüfung und möglicher Abweichung
  - Gesamtergebnis
  - Empfehlungen (z.B. Maßnahmen)

Zertifizierungen gemäß DS-GVO

ZERTIFIZIERUNGEN GEMÄß DS-GVO

- Erfüllung des hohen Anteils an Nachweispflichten durch
  - genehmigte Verhaltensregeln (Code of Conduct) oder
  - genehmigte Zertifizierungsverfahren

- Förderung der Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und-prüfzeichen die dazu dienen, ***nachzuweisen****, dass diese Verordnung bei* ***Verarbeitungsvorgängen*** *von Verantwortlichen oder Auftragsverarbeitern eingehalten wird* gemäß Art. 42 DS-GVO
- Höchstdauer der Gültigkeit der Zertifizierung ist 3 Jahre
- Akkreditierung der Zertifizierungsstellen gemäß Art. 43 DS-GVO

MÖGLICHKEITEN DER ZERTIFIZIERUNG

- Erfüllung der datenschutzkonformen Verarbeitung des Verantwortlichen (Art. 24 DS-GVO)
- Datenschutz durch Technik (Art. 25 Abs. 1 DS-GVO; Umsetzung der Datenschutzgrundsätze, z.B. Datenminimierung)
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO; Umsetzung der Voreinstellungen, z.B. begrenzter Empfängerkreis)
- Auftragsverarbeitung; Nachweis hinreichender Garantien zur Einhaltung der DS-GVO (art. 28 DS-GVO)
- Sicherheit der Verarbeitung; Nachweis der Sicherheitsanforderungen gemäß Art. 32 DS-GVO
- Garantien zur Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f DS-GVO)
- Datenschutz-Folgenabschätzung (ErwGr. 90), Nachweis zur Einhaltung der DS-GVO

- Hinweis: Eine Zertifizierung mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters zur Einhaltung der DS-GVO (Art. 42 Abs. 4 DS-GVO)

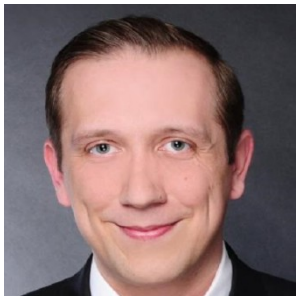
MÖGLICHKEITEN UND VORTEILE EINER ZERTIFIZIERUNG

- Zertifizierung von einzelnen Verfahren
- Zertifizierung eines Datenschutzmanagementsystems

- Vorteile einer Zertifizierung:
  - Sicherstellung der Nachweispflichten
  - Nachweis im Rahmen der Auftragsverarbeitung (Prüftourismus)
  - Marketinginstrument für
    - Auftraggeber
    - Geschäftskunden
    - Verbraucher (Betroffene)

Vielen Dank für Ihre Aufmerksamkeit!

Ihr(e) Ansprechpartner



Tobias Mielke, B.Sc.

Data Protection Consultant
Datenschutz-Qualifizierung
Business Security & Privacy
+49 201 8999-553
t.mielke@tuvit.de

TÜV NORD GROUP