EU Datenschutzgrundverordnung (DSGVO)

Workshop Teil:
technische und organisatorische Maßnahmen

Referent: Eric Drissler

Wer ist ED Computer & Design?

- 1998 gegründet
- herstellerneutrales bundesweites IT-Dienstleistungsunternehmen (Systemhaus)
- Unternehmenssitz: Köln
- Geschäftsbereiche:
  - EDit ➔ IT-Consulting, Hard- und Software, Netzwerke, Security
  - EDcom ➔ ITK-Consulting, Telekommunikation, Unified Communication, SoundSolution
  - EDmoiis ➔ EDmoiis immo, EDmoiis crm
  - EDweb ➔ Webentwicklungen, Webdesign, Webhosting
  - EDdesign ➔ Designkonzepte, Grafikdesign für Digital und Print
  - EDdatenschutz ➔ Stellung eDSB, Datenschutz-Audits, Schulungen
- Mitarbeiter: 12+1
- Ausbildungsbetrieb für IT-Systemkaufleute & Fachinformatiker
- seit 2001 mit Schwerpunkt in der Immobilienwirtschaft
- Partnerschaft mit allen IVD-Regionalverbänden

Allianz für Cyber-Sicherheit

Über mich

- Ausbildung in der Informationstechnik
- ITIL V2 Foundation Certificate 2008
- ITIL V3 Foundation Bridge Certificate 2009
- Datenschutzbeauftragter (TÜV)
- Datenschutzmanager (TÜV)
- externer Datenschutzbeauftragter (TÜV)
- Datenschutzauditor (TÜV)
- Extern bestellter Datenschutzbeauftragter für div. Mandaten
- Prozessbeteiligt bei der Zertifizierung gemäß ISO 27001 bei einem Hoster

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

„unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der Art, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Das heißt Sie müssen die Maßnahmen nicht nur dokumentieren, sondern Eintrittswahrscheinlichkeit und Schwere des Risikos bewerten vgl. Risikoanalyse

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

„Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob **unbeabsichtigt** oder **unrechtmäßig**, oder **unbefugte Offenlegung** von beziehungsweise **unbefugten Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.“

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

bisher technische und organisatorische Maßnahmen (TOM) gemäß §9 BDSG alt

- Zutrittskontrolle → physikalischer Zutritt in Büros, Serverräume etc.
- Zugangskontrolle → logischer Zugang zu den EDV-Systemen, mit dem personenbezogene Daten verarbeitet werden
- Zugriffskontrolle → Zugriff auf personenbezogene Daten
- Weitergabekontrolle → Weitergabe von personenbezogenen Daten
- Eingabekontrolle → Eingabe, Veränderung oder Entfernung personenbezogener Daten
- Auftragskontrolle → Verarbeitung durch einen Dritten im Auftrag
- Verfügbarkeitskontrolle → Schutz vor Verlust und Zerstörung
- Trennungskontrolle → Zweckbindung der Datenverarbeitung

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

- **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DSGVO);
  z.B. virtuelle Maschine für Server mit Offsitesicherung und passendem Hardware-Service-Vertrag, Active-Passive Systeme, HA-Cluster

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 DSGVO)

- **Datenschutz-Management**;
  Definition von Zuständigkeiten, Datenschutzbeauftragter, ggf. Datenschutzkoordinatoren, Verzeichnis von Verarbeitungstätigkeiten, Datenschutzfolgeabschätzungen, Datenschutz bedeutet Organisation und klappt nur wenn es gelebt wird also Schulungsmaßnahmen / Sensibilisierungsmaßnamen mit Nachweis, Verpflichtung auf Vertraulichkeit der Mitarbeiter, definierte und dokumentierte Prozesse, Arbeitsanweisungen / Polices, Review Prozesse
- **Incident-Response-Management**;
  Definition von Zuständigkeiten für Vorfälle (Vorfallteam), Meldeprozess definieren, Maßnahmen für relevante und denkbare Vorfälle definieren, Eskalationswege festlegen, Melde- und Kontaktlisten pflegen, Prüfung des gemeldeten Vorfalls und Risikoklassifizerung wenn zutreffend durch das Vorfallteam, Reaktion auf den Vorfall (Kommunikation wie auch technische Maßnahmen), Reflexion und Nachbereitung um draus zu lernen

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DSGVO);
  Privacy by Design z.B. HTTPs, nur erforderliche Daten; Privacy by Default z..B. bewusstes Haken setzen
- **Auftragskontrolle**
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Technische und organisatorische Maßnahmen als Teil der Sicherheit der Verarbeitung gemäß Art. 32 EU DSGVO

Verantwortlicher:

<Firmenname> vertreten durch <die/die Geschäftsführer/Inhaber/Vorstand>: <Namen der vertretungsberechtigten Personen> <Geschäftsadresse>

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle *Kein unbefugter Zutritt zu Datenverarbeitungs-anlagen.*	☐ Sicherheitsschlösser ☐ Manuelles Schließsystem ☐ Chipkarten-/Transponder-Schließsystem ☐ Schließsystem mit Codesperre ☐ Biometrische Zutrittssperren ☐ Automatisches Zutrittskontrollsystem ☐ Schlüsselregelung (Schlüsselausgabe etc.) ☐ Alarmanlage ☐ Lichtschranken / Bewegungsmelder ☐ Videoüberwachung der Zugänge ☐ Personenkontrolle beim Pförtner / Empfang ☐ Protokollierung der Besucher ☐ Tragepflicht von Berechtigungsausweisen ☐ Sorgfältige Auswahl von Wachpersonal ☐ Sorgfältige Auswahl von Reinigungspersonal
Zugangskontrolle *Keine unbefugte Systembenutzung.*	☐ Zuordnung von Benutzerrechten ☐ Passwortvergabe sicherer Kennwörtern ☐ regelmäßige Passwortänderungen ☐ Authentifikation mit Benutzername / Passwort ☐ Authentifikation mit biometrischen Verfahren ☐ Zuordnung von Benutzerprofilen zu IT-Systemen ☐ Schlüsselregelung (Bereichsabhängig etc.) ☐ automatische Sperrmechanismen ☐ Sperren von externen Schnittstellen (USB etc.) ☐ Verschlüsselung von mobilen Datenträgern ☐ Verschlüsselung von Datenträgern in Notebooks ☐ Verschlüsselung von Smartphone-Inhalten / Tablets ☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) ☐ Einsatz einer Software-Firewall ☐ Einsatz einer Hardware-Firewall ☐ Einsatz von Intrusion-Detection-Systemen ☐ Einsatz von Virtual Private Networks (VPN) Technologie ☐ Einsatz von Anti-Viren-Software ☐ Patchmanagement für Betriebssystem und Anwendungen

Zugriffskontrolle *Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.*	☐ Rechtvergabe nach dem „need to know“ Prinzip ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel ☐ Verwaltung der Rechte durch Systemadministrator ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert ☐ automatische Sperrmechanismen ☐ Verschlüsselung von mobilen Datenträgern ☐ Verschlüsselung von Datenträgern in Notebooks ☐ Verschlüsselung von Smartphone-Inhalten/ Tablets ☐ physische Löschung von Datenträgern vor Wiederverwendung ☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern ☐ Protokollierung der Vernichtung ☐ Sichere Aufbewahrung von Datenträgern
Trennungskontrolle *Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.*	☐ logische Mandantentrennung (softwareseitig) ☐ Versehen der Datensätze mit Zweckattributen/ Datenfeldern ☐ Erstellung eines Berechtigungskonzepts ☐ Sandboxing ☐ Erstellung eines Berechtigungskonzepts ☐ Trennung von Produktiv- und Testsystem
Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) *Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.*	☐ Nutzung von Pseudonymisierung wo möglich (u.a. bei Weitergabe) ☐ geeignete Wahl der Pseudonymisierungsschlüssel ☐ Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle *Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.*	☐ E-Mail TLS Verschlüsslung ☐ E-Mail TLS Verschlüsslung mit pfs ☐ E-Mail End2End Verschlüsslung (u.a. pgp, S/MIME) ☐ elektronische Signatur ☐ Verschlüsselung von mobilen Datenträgern ☐ Verschlüsselung von Datenträgern in Notebooks ☐ Verschlüsselung von Smartphone-Inhalten / Tablets ☐ Weitergabe von Daten in anonymisierter oder mindestens pseudonymisierter Form ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen ☐ Erstellen einer Übersicht der Abruf- und Übermittlungsvorgänge ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen ☐ Beim physischen Transport: sichere Transportbehälter/ -verpackungen
Eingabekontrolle *Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*	☐ Dokumentenmanagement ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten ein-gegeben, geändert und gelöscht werden können. ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle *Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust,*	☐ gespiegelte Festplatten (RAID) ☐ gespiegelte Systeme / Cluster ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Schutzsteckdosenleisten in Serverräumen / Überspannungsschutz ☐ Einsatz einer Software-Firewall ☐ Einsatz einer Hardware-Firewall ☐ Einsatz von Intrusion-Detection-Systemen ☐ Einsatz von Anti-Viren-Software ☐ Erstellen eines Backup- & Recoverykonzepts (u.a. (online/offline; on-site/off-site) ☐ regelmäßige Datenwiederherstellungtests ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

	☐ Klimaanlage in Serverräumen ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen ☐ Feuer- und Rauchmeldeanlagen ☐ Feuerlöschgeräte in Serverräumen (CO2) ☐ Serverräume nicht unter sanitären Anlagen, wasserführenden Leitungen ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen ☐ Serverräume über der Wassergrenze (Hochwasser) ☐ Wartungsverträge mit geeigneter Reaktionszeit ☐ Patchmanagement für Betriebssystem und Anwendungen
rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);	☐ Erstellen eines Notfallplans ☐ Nutzung virtueller Maschinen mit Offsitesicherung ☐ passender Hardware-Service-Vertrag ☐ eigene Ersatzteilbevorratung ☐ Wartungsverträge mit geeigneter Reaktionszeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 DSGVO)

Datenschutz-Management	☐ Bestellung eines Datenschutzbeauftragter ☐ Einsatz vom Datenschutzkoordinatoren ☐ Verzeichnis von Verarbeitungstätigkeiten ☐ Datenschutzfolgeabschätzungen ☐ Schulungsmaßnahmen/ Sensibilisierungsmaßnamen mit Nachweis ☐ Verpflichtung auf Vertraulichkeit der Mitarbeiter ☐ definierte und dokumentierte Prozesse ☐ Arbeitsanweisungen/ Polices mit Datenschutzhintergrund ☐ Review Prozesse
Incident-Response-Management	☐ Definition von Zuständigkeiten und Verantwortlichkeiten für Vorfälle (z.B. Vorfallteam) ☐ definierter Meldeprozess ☐ definierte Maßnahmen für relevante und denkbare Vorfälle ☐ definierte Eskalationswege ☐ aktuelle Melde- und Kontaktlisten ☐ Prüfungsprozess für gemeldete Vorfälle und anschließender Risikoklassifizierung wenn zutreffend ☐ vorbereitete Reaktionen auf den Vorfall (Kommunikation wie auch technische Maßnahmen) ☐ Reflexion und Nachbereitungsprozess um aus Vorfällen zu lernen

datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	☐ Prozess zur Sicherstellung von Privacy by Design bei Änderungen ☐ Prozess zur Sicherstellung von Privacy by Default bei Änderungen
Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten ☐ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen ☐ Sicherstellung der Verpflichtung auf die Vertraulichkeit durch den Auftragnehmer ☐ Auftragnehmer hat Datenschutzbeauftragten bestellt ☐ vertraglich festgelegte Verpflichtungen und Zuständigkeiten ☐ Auftragsverarbeitungsverträge ☐ wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart ☐ Vertragsstrafen bei Verstößen / klare Haftungsregelungen ☐ schriftliche Weisungen an den Auftragnehmer ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Risiken bewerten

Die Risiken lassen sich ideal mittels einer Risikoanalyse bewerten, so kann man schnell auch sehen wo es noch welche Restrisken gibt.

Schritt 1: Schutzstufe definieren (Teil 1)

Wir bedienen uns hier dem Schutzstufenkonzept des LfD Niedersachsen und legen fest:

A+B = geringes Risiko

C, D und E = hohes bzw. sehr hohes Risiko

Bewerten Sie die Schutzstufen exponentiell um den starken Anstieg der Gefahren gerecht zu werden (also: A = 1, B = 2, C = 4, D = 8, sowie E = 16).

Für Datenkategorien mit einen hohen und sehr hohen Risiko (also C, D und E) haben führen Sie eine erweiterte Schutzbedarfsanalyse durch.

Risiken bewerten

Schritt 1: Schutzstufe definieren (Teil 2)

Schutzstufe	Personenbezogene Daten,	zum Beispiel
A = 1	die frei zugänglich sind. Der Einsichtnehmende muss dabei kein berechtigtes Interesse geltend machen.	Telefonbücher, Adressbücher, Wahlvorschlagsverzeichnisse
B = 2	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse der Einsichtnehmenden gebunden ist.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen
C = 4	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **beeinträchtigen könnte** („Ansehen").	Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten
D = 8	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **erheblich beeinträchtigen könnte** („Existenz").	Straffälligkeit, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen
E = 16	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen **beeinträchtigen könnte.**	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können

Risiken bewerten

Schritt 2: Ermittlung des jeweiligen Schutzbedarfs

Schutzziel	Normal	Hoch	Sehr hoch
Vertraulichkeit	1	2	3
Integrität	1	2	3
Verfügbarkeit	1	2	3

Risiken bewerten

Schritt 3: Risikowert 1 Ermittlung

Die einzelnen Datenkategorien werden in einer Tabelle erfasst, mit Werten verssehen und der Risikowert berechnet.

Datenkategorie	Schutzstufe	Vertraulichkeit 1	Integrität 1	Verfügbarkeit 1	Risikowert 1
Bankdaten	C (4)	2	2	1	16
Zahlungsverhalten	D (8)	2	1	2	32

Bankdaten haben die Schutzstufe C also 4 Punkte. Die Daten über das Zahlungsverhalten hingegen sind gemäß der Tabelle D also 8 Punkte.

Die Schutzstufe müssen nun mit den Schutzbedarfswerten 1 multipliziert werden um den Risikowert 1 zu erhalten bspw. 4 x 2 x 2 x 1 = 16.

Für kleinere Unternehmen, welche die Verarbeitung von personenbezogenen Daten nicht zum Gegenstand ihrer originären Tätigkeit haben, **hat sich die umfassende Risikoanalyse ab 16 Punkten Risikowert 1 als praktikabel herausgestellt.**

Risiken bewerten

Schritt 4: Risikowert 2 Ermittlung

Nun ergänzt man die Tabelle um die Risiko reduzierenden Maßnahmen und bewertet erneut.

Datenkategorie	… .	Risikowert 1	dokumentierte Maßnahmen	Vertrau-lichkeit 2	Integrität 2	Verfüg-barkeit 2	Risikowert 2
Bankdaten	… .	16	-verschlüsselte Speicherung -minimale Zugriffsrechte -tägliches offsite Backup verschlüsselt inkl. Prüfung	1	2	1	8
Zahlungsverhalten	… .	32	-verschlüsselte Speicherung -minimale Zugriffsrechte -tägliches offsite Backup verschlüsselt inkl. Prüfung -HA Cluster	1	1	1	8

Zusammenfassung?

- Erstellen Sie die technischen und organisatorischen Maßnahmen für Ihren Betrieb → diese sind auch Teil Ihres Verzeichnisses der Verarbeitungstätigkeiten
- Prüfen Sie die technischen und organisatorischen Maßnahmen Ihrer Auftragsverarbeiter initial, so dann regelmäßig → i.d.R. 1 x jährlich
- Definieren Sie einen Prozess zur regelmäßigen Überprüfung der technischen und organisatorischen Maßnahmen, so dass diese noch vorhanden und aktiv sind und dokumentieren Sie die Überprüfung → i.d.R. 1 x jährlich
- Definieren Sie einen Prozess zur regelmäßigen Bewertung der Maßnahmen → Bewertung der Maßnahmen nach Risikoschema und dokumentieren diese
- Definieren Sie einen Prozess zur regelmäßigen Überprüfung der Wirksamkeit → Wirksamkeitstests (bspw. Penetrationstest / Wiederherstellung von Datensicherungen etc.) und dokumentieren diese
- Denken Sie auch daran organisatorische Maßnahmen zu bewerten und prüfen → bspw. rechtliche Änderungen / Überprüfung der Einhaltung von Polices und Richtlinien

Fragen?

Hilfe und Unterstützung?

Webinare zu einzelnen Fachthemen:

https://immobilienprofi.edudip.com/academy/eric.drissler

alle Workshops / Seminare / Webinare:

https://www.edcud.de/EDdatenschutz-Schulungen

Beratung, Datenschutz-Audit, Mitarbeiter Schulungen, externer DSB:

ED Computer & Design GmbH & Co. KG

Lina-Bommer-Weg 4

51149 Köln

Telefon +49 (0) 221 28 88 77 66

Telefax +49 (0) 221 28 88 77 67

E-Mail datenschutz@edcud.de Internet www.edcud.de