Anleitung zum Erarbeiten eines Datenschutzkonzeptes nach DSGVO Für einen Kleinbetrieb bzw EPU

Dies ist die Anleitung!
Die Vorlage zum Ausfüllen finden Sie hier: https://temt-datenschutz.eu/wp-content/uploads/Datenschutz-Vorlage-Konzept.odt

Vorab

Die Anleitung und die Vorlage sind praktische Unterlagen, um als EPU/Kleinbetrieb einen **ersten Entwurf** für eine DSGVO-konforme Dokumentation erstellen zu können. Dieser sollte dann noch mit einem DSGVO-Berater bzw IT-Experten und möglicherweise Rechtsanwalt überarbeitet werden. Vergessen Sie nicht, Sie sind der/die Verantwortliche, sie haften!

Förderungen

Momentan gibt es leider keine direkte Förderungen betreffs DSGVO, da die WKO wegen zu großer Nachfrage kein Budget mehr dafür hat.

Beratung

- Gerne stehe ich Ihnen für DSGVO-Beratung zur Verfügung https://temt-datenschutz.eu/
- Für technische Umsetzung wie Verschlüsselung, BackUp, … wäre Michael Werzowa Ihr Ansprechpartner, siehe auch: https://temt-datenschutz.eu/
- Weitere kostenlose Anleitungen und Vorlagen für Psychotherapeuten finden Sie unter https://www.dataprivacydoctors.at/vorlagen/

Einleitung

Diese Anleitung und das Konzept haben wir für **EPUs** erstellt und können diese Anleitung und das Konzept verwenden

- und bei den TOMs haben wir dazu geschrieben, was nur für Sie gilt

und mit Anhang für **Kleinbetrieb im allgemeinen** (Personalwesen, Ausbildung Mitarbeiter) erstellt,

- bei denen mehr als eine Person Zugriff auf die personenbezogenen (=pb) Daten haben
- die mindestens eine Person, sei es auch nur halbtags, im Angestelltenverhältnis haben
- und die nicht umfangreich und/oder als Kerntätigkeit Art 9 Daten (zB Gesundheitsdaten, Sexualität, Religion, ethische Herkunft Gewerkschaft, Politik, …) verarbeiten (siehe **Datenschutzbeauftragter)**

Fotos bei Veranstaltungen

Wie man mit dem Fotografieren bei Veranstaltungen umgehen sollte, finden Sie hier: https://www.dataprotect.at/2018/05/15/verwendung-von-fotos-von-veranstaltungen-nach-dem-25-05-2018/ , wobei wir ergänzend hinzufügen wollen, dass Sie das Fotografieren auch zeitlich und/oder örtlich eingrenzen sollten, denn es sollten auch Leute auf Ihre Veranstaltungen kommen können, die nicht unbedingt fotografiert werden wollen!
Zeitlich: Nur von 19 bis 20 Uhr oder nur bei der Siegerehrung/Preisverleihung oder bei der Ansprache oder Eröffnung oder ….
Örtlich: Bei Ausstellungen zb nur in den markierten Räumen oder bei Vorträgen, ..nur bis in die ersten 10 Reihen oder nur Tribüne A oder ……..

Anleitung

Im weiteren die notwendigen Schritte, um als EPU/Kleinbetrieb einen **ersten Entwurf** für eine DSGVO-konform Dokumentation erstellen zu können. Lesen Sie bitte unbedingt den Disclaimer auf der letzten Seite!

Alles in Gelb ist entsprechend dem konkreten Fall zu ändern

Grün bedeutet, dass hier Ihr IT-Berater oder Software-Anbieter helfen sollte

Blau bedeutet, dass hier Ihre Steuerberater/Bilanzbuchhalterin helfen sollte, insbesondere beim Verarbeitungsverzeichnis Personalwesen

Insbesondere bei Verträgen sollte eine Rechtsanwaltskanzlei kontaktiert werden.

Deckblatt und allgemeiner Teil

- Bitte die gelb markierten Felder mit Ihren Daten ersetzen
- Disclaimer löschen
- Wenn fertig, Inhaltsverzeichnis erstellen,
- Regelmäßige Weiterbildung auch im Bereich des Datenschutzes ist anzuraten
  Hinweis: Auch hier bietet die **Initiative KMU DIGITAL** sinnvolle Förderungen, womit 50% der Kosten von einschlägigen Weiterbildungsmaßnahmen rückvergütet werden.

Verarbeitungsverzeichnisse

Rechnungswesen und Geschäftsabwicklung:

- Bei Unternehmen mit mehreren Personen ist der Verantwortliche der Geschäftsführer.

- Bitte vermeiden sie den Begriff Datenschutzbeauftragter, außer Sie braucht einen, denn Datenschutzbeauftragte sind (arbeits-) rechtlich besonders geschützt.

- **Kategorien der verarbeiten Daten**

  - Die Felder für Datenkategorien bitte mit den Feldern aus Ihrer Software, aus Ihrer Praxis ersetzen oder wenn nicht benötigt, streichen. Sollten mehrere Ihrer Daten unter eine Datenkategorie fallen, so nehmen Sie die allgemeinere hier.

  - Wir haben nicht die Daten, die an Ihren, Homepage-Hoster, IT-Dienstleister (mit Fernwartung) bzw. Software-Anbieter mit Fernwartung* in die Spalte eingetragen. Da Sie aber sowieso einen Datenverarbeitungs-Vereinbarung nach Art 28 mit den Genannten abschließen müssen, werden in dieser Vereinbarung alle pb Daten erfasst (siehe dort) und sie brauchen dann nur die Nummer des Empfängers in das jeweilige Feld der Spalte dazu schreiben.
    Aber dies können Sie später machen, wenn wir in dieser Anleitung zum Anhang und zu den Art 28 Datenverarbeitungs-Vereinbarungen kommen.
    * Mögliche weitere Datenverarbeiter siehe **Anhang „Mustervereinbarung für Auftragsverarbeitung“ in Empfänger neue Zeile** machen.

- **Kategorien der Empfänger**

  - Falls Sie Fernwartung Ihres Computer zulassen, so müssen Sie es hier dokumentieren
  - Wenn Sie z. B. hier Zeile Inkassobüro streicht, so dies bitte auch oben als Spalte streichen

Kundenbetreuung und Marketing

- **Kategorien der verarbeiten Daten**

  - Die Felder für Datenkategorien bitte mit den Feldern aus Ihrer Software, aus Ihrer Praxis ersetzen oder wenn nicht benötigt, streichen. Sollten mehrere Ihrer Daten unter eine Datenkategorie fallen, so nehmen Sie die allgemeinere hier.

  - **Newsletter:**
    Bitte in der letzten Spalte schreibt entweder intern, wenn Sie Newsletter selber versendet oder extern, wenn Sie einen Newsletter-Tool-Anbieter aus der EU bzw. DACH– eher nicht USA – verwendet, denn Sie müssen auch eine (deutschsprachige) Datenverarbeitungs-Vereinbarung nach Art 28 abschließen (siehe Anhang).

- **Sichere und verschlüsselte Datendiensten für Ihre Kommunikation**
  Statt WhatsApp, das wir kritisch sehen, gibt es mehrere sehr gute und vertrauenswürdige Anbieter von verschlüsselten und sicheren Kommunikations-Apps mit den gleichen Funktionen wie zB telegram, wire oder signal.

  Wir verwenden schon seit Jahren www.signal.org sowohl auf unseren Handys als auch auf unseren Desktops und sind zufrieden damit, aber die anderen Anbieter sind sicher

genauso gut – **Ihre Wahl** und dann in die Zeile Empfänger eintragen

Mehr zu signal.org: https://support.signal.org/hc/en-us/articles/212477768-Is-it-private-Can-I-trust-it- Da signal.org keinen Zugang zu den gesendeten Daten, SMS und Gesprächen hat und ebenso nicht zu den Telefonnummern, werden keine pb Daten an signal.org übertragen und Sie brauchen daher nichts in die Spalte eintragen und es bedarf daher auch keiner Vereinbarung gemäß Art 28 DSGVO. Sollte die Datenschutzbehörde zu einer anderen Meinung gelangen,

Personalwesen nur für KMUs

Sie Anhang.

- Um das Risiko für die Mitarbeiter und die Betroffenen gering zu halten, sollen die Verträge von einem Rechtsanwalt erstellt/gegengelesen werden und die TOMs soweit als möglich und vertretbar durchgeführt worden sein, um auch die Mitarbeiter zu schützen!

- Geheimhaltungsvereinbarung mit Mitarbeitern und Dritten siehe Anhang

- DSGVO-Schulung der Mitarbeitern ist ausdrücklich angeraten, auch aus Haftungsgründen.

Weitere Verarbeitungsverzeichnisse

Es kann leicht sein, dass Sie pB Daten auch anderswo verarbeiten, erfassen, einsetzen usw. Sollte daher die obigen Verzeichnisse nicht alle Ihre Verarbeitungen abdecken, so findet Sie hier **weitere Verarbeitungsverzeichnisse** und da ist höchstwahrscheinlich auch die von Ihnen gesuchte dabei

1. **Sehr gute Zusatz- Muster und Vorlagen für** Kleinbetriebe (zB: Online-Shop, Aushang, …..)
https://www.wko.at/branchen/handel/datenschutzgrundverordnung-in-handelsunternehmen.html

2. Eine sehr gute Liste mit diversen **weiteren Verarbeitungsverzeichnissen,** wie zB Internetseite, Freelancer-Datenbank, Verkauf / Vertrieb, CRM, Projektverwaltung
Zeiterfassung, Kontaktverwaltung; Terminverwaltung, E-Mail, Videoüberwachung. Controlling, , Revision / Compliance, Einkauf, IT, Verwaltung, Fuhrparkmanagement, Facility Management, Marketing, Produktion, Finanzbuchhaltung, Lohnbuchhaltung, Personal / HR, Bewerbermanagement
https://www.datenschutz-guru.de/verzeichnis-von-verarbeitungstaetigkeiten/

3. Verarbeitungsverzeichnisse für diverse Berufe und Gewerbe
https://www.lda.bayern.de/de/kleine-unternehmen.html

TIPP

Bei mehr als 3-4 Verzeichnissen, raten wir Ihnen eine Excel-Datei zu benutzen, da es so einfacher und übersichtlicher wird:

>	Zwecke der Datenverarbeitung	Rechtsgrundlage	Beschreibung der Verarbeitung	Verarbeitung besonderer Arten personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO	Betroffene / betroffene Personengruppen	Personenbezogene Daten / Datenkategorien	Empfänger / Empfängerkategorien	Drittstaatentransfer	Zugriffsberechtigte	Regelfristen für die Löschung	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

Checkliste – IT Safe (WKO)

Bitte unbedingt machen: Wir, alle Management und Mitarbeiter sind die wirklich hilfreiche IT-Checkliste für EPUs unter https://itsafe.wkoratgeber.at/ durch gegangen und konnte feststellen, ob und wo es in meinem Kleinunternehmen Probleme im IT-Bereich geben könnte. Die daraus folgenden Maßnahmen im weiteren.

Selbstschutz

Wir versuche unser Such- und Surfverhalten soweit wie möglich „sicher“ zu gestalten und verwenden daher zB den europäischen Open Source Browser https://cliqz.com/ inklusive Ghostery (verhindert und zeigt mir die Trackingversuche) und zB die europäische Suchmaschine: https://www.startpage.com statt Google .

Handy

Die privaten und beruflichen Daten, wenn möglich, voneinander trennen (eigene Folder/ Gruppen/.. Apple bietet diese Funktion bei einigen Handys jetzt an. Vielleicht doch eigene Firmenhandys beschaffen?!

Unser Firmen-Handies sind durch mind. 6-stelliges Passwort bzw. Biometrie geschützt. Es gibt die Möglichkeit die Daten „fern zu löschen“ bei Apple, bei anderen Handys bitte Security-App downloaden. Bluetooth-Funktion ist nur beim Autofahren eingeschaltet. WLAN ist abgeschaltet. In öffentliche WLAN-Netze wähle ich/wir mich nicht ein und es gibt auch keine automatische Verbindung mit mir/uns bekannten WLANs. Wenn ich/wir ein neues Handy/Laptop/Computer kaufe, so lasse ich/wir mein altes Handy Laptop/Computer von meinem IT-Fachmann immer vollständig löschen (Datenverarbeitungs-Vereinbarung nach Art 28) Falls ich/wir USB-Sticks verwende, so sind die Daten darauf verschlüsselt und ein Passwort ist notwendig, um auf die Daten zu zugreifen.

Impressum und Datenschutzerklärung (WKO)

Impressum

- Das Impressum für vereine: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Das-korrekte-Website-Impressum-Verein.pdf

- Mit dem ECG-Service können Sie mit ein paar Klicks ein rechtlich gültiges Impressum erstellen.

- Wir raten Ihnen ausdrücklich von http://www…… zu **httpS://……** zu wechseln.

- Wenn Ihre Homepage mit WordPress erstellt wurde, so findet Sie oder der Ersteller/Betreiber hier wichtige Tipps: https://www.blogmojo.de/wordpress-plugins-dsgvo

AGBs

- Vorlagen gibt es bei der WKO oder bei Ihrer Standes/Berufsvertretung

Datenschutzerklärung

Sehr gute Seite auf der man Datenschutz Erklärungen für Web Seiten erzeugen kann, möglicherweise kostenpflichtig.
Wir haben den Generator auch für unsere Homepage verwendet.
!!!!!!!!! https://datenschutz-generator.de !!!!!!!!!

- **Gemäß Informationspflicht**
  müssen Sie in Ihrer Datenschutzerklärung auch allgemein beschreiben welche Daten Sie wie verarbeiten und an wen weiterleiten (siehe Ihr Verzeichnisse bei Zweck und Datenkategorien)
- **Dauer**
  und wie lange:
  zb Bei einem bestehenden oder abgeschlossenem Vertrag aufgrund der gesetzlichen Aufbewahrungsfristen wie z. B. § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen.
- **Einwilligungserklärung**
  Die Datenschutz-Grundverordnung (DSGVO) verpflichtet jeden Verantwortlichen, die betroffene Person in präziser, transparenter, verständlicher und leicht zugänglicher Form über die wichtigsten Aspekte einer Datenverarbeitung zu informieren. Dies hat schriftlich (einschließlich elektronisch) zu erfolgen. Werden die Daten direkt bei der betroffenen Person erhoben, **wie bei der Einwilligungserklärung**, so hat diese Information sogleich zu erfolgen.

  https://dsgvo-informationsverpflichtungen.wkoratgeber.at

  Am Ende des Ratgebers erhalten Sie ein **Merkblatt mit Textbausteinen** für Ihre Informationspflicht, die Sie für Ihre Einwillungserklärung sowie Datenschutzerklärung verwenden können.

TOMs als Fließtext

In der Vorlage finden sie eine Excel-ToDo-Liste, eine Liste der Maßnahmen, die Sie umsetzten

sollten. Wenn sie eine Maßnahme umsetzen sollten Sie aus der TOM-Beschreibung einen Fließtext, ganze Sätze machen, ähnlich wie Ärzte es in ihrer Dokumentation machen http://www.aekwien.at/documents/4771581/22586874/DSGVO+Verzeichnis+Muster+EP/c8ddf437-3f23-4020-9b74-278915cc608f)

Als Beispiel für ein EPU:

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

X	Zuordnung von Benutzerrechten **Einzelpraxis, daher Verantwortliche**	X	Erstellen von Benutzerprofilen **Einzelpraxis, daher Verantwortliche**
X	Passwortvergabe **Einzelpraxis, daher Verantwortliche**		Authentifikation mit biometrischen Verfahren

Es müssen keine Benutzerrechte vergeben und keine Benutzerprofile erstellt werden, da der Verantwortliche als EPU der einzige ist, der Zugriff auf die pb Daten hat.

Meine Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Der Vorteil: *Sie sehen mit einem Blick, was Sie schon umgesetzt haben (Fließtext) und was noch zu tun ist (Excel-Liste).*

TOMs - Einzelne Maßnahmen

- Bitte – auch in Absprache mit IT-Berater bzw. Software-Anbieter – umgesetzten TOMs ankreuzen und anderen entfernen

- Bei den Feldern sind Maßnahmen, die wir als Mindeststandart bis zum 24. Mai 2018 empfehlen **X** Rot angekreuzt. Alle weiteren Maßnahmen bitte so schnell wie möglich umsetzen.

- Organisatorische Maßnahmen und z. B. abschließbarer Aktenschrank usw. können Sie selber machen, bei IT-Maßnahmen wie Zuordnung von Benutzerrechten, usw sollten Sie unbedingt Ihren IT-Berater bzw. Softwareanbieter einbinden.

- Vor allem bei der Absicherung Ihrer Datenbank vor unbefugtem Zugriff brauchen Sie Hilfe von Experten.

- Zuordnung von Benutzerrechten (EPU: nur Verantwortliche)
- Erstellen von Benutzerprofilen (EPU, daher nur Verantwortliche)

Wo zB (EPU: nur Verantwortliche) steht, müssen Sie als KMU, wo mehrere Personen tätig sind und zugriff auf die pb Daten haben, unbedingt die Software entsprechend anpassen, wenn sie es noch nicht ist!

- Verschlüsselung aller (Firmen-) Computer, Laptops, Handys, USB und regelmäßiges Backups

- Bei Verschlüsselungen ist der Prozess wie folgt:
  1. Schritt: Backup
  2. Schritt: kontrollieren ob Backup funktioniert
  3. Schritt:Verschlüsseln

- **Ein Kontroll- und Verbesserungsprozess sollte mindestens 1x jährlich durchgeführt werden, so auch die DSGVO.** **Datenschutz ist ein Prozess!**

Prozesse betreffs Betroffenenrechte

Quelle: http://www.aekwien.at/documents/4771581/22586874/DSGVO+Verzeichnis+Muster+EP/c8ddf437-3f23-4020-9b74-278915cc608f)

Feststellung der Identität:

- „Sehr geehrte Frau/Herr …!
  Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen, wie zB pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zukommen zu lassen. Dieser wird von mir nach der Überprüfung sogleich wieder gelöscht.
  Ich danke Ihnen für Ihr Verständnis

  oder

- Das sicherst wäre den Betroffenen zu bitten, seinen Ausweis/Führerschein vor die Handykamera zu halten. Dies mag bei sensiblen Daten nach Art 9 und vor allem bei Erziehungsberechtigten wohl der einzige gangbare Weg sein, die Identität sicher fest zu stellen.

Wir raten Ihnen daher hier **Ihre eigene Risikoanalyse** (siehe dort) zu machen und dann entsprechend Ihrer Einschätzung vorzugehen und dies in der Vorlage zu dokumentieren.

- **Screenshot**
  Sollte Ihnen Ihr Programm bessere Möglichkeiten bieten, als die (Stamm) Daten des Betroffenen per Screenshot zu erfassen, so verwenden sie natürlich diesen Weg. Leider können aber die meisten Programme dies (noch) nicht.

- Leider kann man bei vielen Programmen zB die Rechnung usw **nicht** nach 7 Jahren löschen oder bei Antrag auf Löschung **nicht** sofort löschen, da hilft – solange der Anbieter der Software es nicht geändert hat – nur die Funktion „Auftragssperre", die es bei den meisten Programmen gibt!

E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO)

- Eine sehr gute Listung der DSGVO-konformen Newsletter-Tool-Anbier findet Sie hier: https://www.blogmojo.de/adv-vertraege/

- Am besten schreibt Sie alle Ihre Newsletter-Empfänger an und bittet Sie sie Ihnen eine neue Einwilligung zu geben. Die Rücklaufquote hängt von der freundlichen, vielleicht sogar witzigen Formulierung ab. Und machen Sie es bald, bevor es alle anderen machen!

- Eigenes Email als **datenschutz@**…HP…….at/com wäre auch anzuraten

Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

Wir haben Ihnen hier eine Teil-Risikoanalyse gemacht. ABER Sie müssen sie trotzdem für sich noch einmal machen bzw. vervollständigen, da es immer vom konkreten Fall, den individuellen Umständen UND den gesetzten TOMs abhängig ist!

Schutzbedarfsanalyse

Unsere Vorabanalyse ergab, dass es sich bei folgende pb Daten der Klienten, Auszubildenden, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit vernachlässigbaren bis geringem Schutzbedarf handelt, da sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht und auch allgemeine TOMs gemäß DSGVO gesetzt wurden:

Öffentlich zugängliche Daten, Ordnungsnummer, Name, Firma oder sonstige Geschäftsbezeichnung, Anrede/Geschlecht, Anschrift, Homepage, Kontaktdaten (Tel., Mail, Fax,), Berufs-, Branchen- und Geschäftsbezeichnung,

Firmenbuchdaten, Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Nummer und Intrastat-Kenn-Nummer, Korrespondenzsprache, Namen der Kontaktpersonen/Erziehungsberechtigte, Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.), Funktion/Rolle der Kontaktperson usw.)

Des weiteren ergab unsere Vorabanalyse, dass es sich bei folgende pb Daten der Klienten, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit einen **hohen** und **sehr hohen** Schutzbedarf handelt und daher eine erweiterte Risiko-Analyse durchgeführt werden muss.

Alle Daten gemäß iSd Art 9 der Mitarbeiter Fotos .. Interessen (auf Grund eigener Angaben des Kunden, Lieferanten, Interessierten, ...), Kaufverhalten (Frequenz und Volumen), Personenstand, usw. …….. Personenstand, Geburtsdatum, Bankverbindungen, Kreditkartennummern und -unternehmen, (Behandlungs-) Vertragstext und Korrespondenzen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch und Mitschriften und Fotos usw ……..

Risikoanalyse ohne Maßnahmen

- Analysieren Sie bitte Ihre Daten und tragen Sie sie in die entsprechenden **Risikokategorien** in die Vorlage ein.

- Wir haben schon Kategorie 1 + 4 in die **Risiko-Matrix** eingetragen, die anderen machen Sie bitte gemäß Ihrer Einschätzung (siehe unten Schwere und Eintrittswahrscheinlichkeit) selber!

Bewertungsmaßstäbe

- Hier die Bewertungsmaßstäbe um die Daten in das entsprechende Feld der **Risiko-Matrix** eintragen zu können:

Schwere:

Schwere	Auswirkung auf Betroffene	Folgen überwinden	Beispiele
Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, …
Begrenzt	Wesentliche Unannehmlichkeiten	Unannehmlichkeiten sollten sich – trotz Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, …
Wesentlich	Wesentliche Folgen	Unannehmlichkeiten sollten sich – trotz großer Schwierigkeiten – überwinden lassen	Kategorien und Klassifizierungen werden bekannt, Missbrauch von Geldern, Vorladungen, Verschlechterung eines Verhältnisses, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte, Gerüchte, …
Existenz-gefährdend	Irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	**Bekanntwerden zB der Diagnose führen zu finanzielle Not, Kündigung, Familientragödien, Selbstmord, …** und/oder vertrauliche Mitschriften werden Konkurrenz bzw. Öffentlichkeit bekannt und gefährden Betrieb;Beruf, Identitätsdiebstahl; … langfristige Beschwerden, Tod, …

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Eintrittswahrscheinlichkeit:

EWK	Wahrscheinlichkeit	Beispiele
Vernachlässigbar	0-24% Wahrscheinlichkeit	zB Diebstahl von Unterlagen aus einem Safe
Möglich	25-69% Wahrscheinlichkeit	Zb gezielter und koordinierter Angriff durch einen Hacker, Verlust des Hardware bzw. pb Daten durch Diebstahl oder durch fahrlässiges Handeln
Sehr wahrscheinlich	70-99% Wahrscheinlichkeit	zB Eindringung eines Schädigungs-Mails,
Garantiert	100% Wahrscheinlichkeit garantiert	zB Ausfall durch einen Festplattenausfall, Festplatten halten ca 3 – 5 Jahre! Datenverluste durch technische Fehler

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Maßnahmen

Siehe TOMs, insbesondere Verschlüsselung!
Sie müsst schauen, dass Sie die Kategorien in der Risiko-Matrix
von rechts oben in Rot => nach links unten in Grün mit Hilfe Ihre Maßnahmen bekommen!

Risiko-Matrix mit Maßnahmen

Bitte hier die Kategorien 1 - 4 gemäß Ihrer Maßnahmen eintragen!

Ein angemessenes Datenschutzniveau

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
	• Mit Datenschutzbehörde **kommunizieren**	
• Betroffene sind nicht zu informieren		

- Für mich, den der Ausgangspunkt war mein Datenschutzkonzept, war dann dieses Datenschutz-niveau absolut angemessen und deshalb in **Ich-Form,** aber dies ist mein Zugang:

  ✔ Die pb Daten der Kategorie 1 haben wir trotz TOMs „Risiko“ zugeordnet, da bei einer **mög-lichen** Datenschutzverletzung die Folgen **begrenzt** sind und so der betroffene Klient höchstwahrscheinlich nicht informiert werden muss, nichts desto trotz wird die Behörde über diesen Fällen informiert.

  ✔ Als Verantwortliche/r ist mir so auch bewusster, dass einmal gesetzte TOMs nicht für alle Zeiten alle möglichen und vor allem neuartige (kriminelle) Datenschutzverletzungen auf-fangen können und ich bleibe so acht und wachsam. **=> Datenschutz ist ein Prozess!**

  ✔ **Achtung: Sollte es doch zu einer Datenschutzverletzung kommen, so müssen Sie dafür trotzdem noch einmal eine Risikoanalyse aus Sicht der Betroffenen machen, da es voral-lem bei Unerwartetem doch zu einem hohen Risiko für Betroffene kommen kann!**

Liebe Nutzer dieser Anleitung!

Wir wollen ausdrücklich festhalten, dass niemand zum jetzigen Zeitpunkt ein perfektes und juristisch wasserdichtes Konzept abliefern kann, zu viele Punkte sind offen, strittig und es fehlen die letztinstanzlichen Gerichtsentscheidungen, aber dass Sie, wenn Sie diese Vorlage sorgfältig ausfüllen, eine Risikoanalyse durchführen, die vorgeschlagenen TOMs auch wirklich als Mindeststandart umsetzen und sich per Newsletter updaten, sicherheitshalber einen Rechtsanwalt, Steuerberater und IT-Spezialisten beiziehen, die Behörde höchstwahrscheinlich von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen wird und Sie vor allem gegenüber Ihren Kunden mit gutem Gewissen sagen können:

> *„Liebe Kunden und Klientinnen!*
> *Vertrauen zwischen mir als Verantwortliche und Ihnen ist die Grundlage und Voraussetzung für meine Beratung, daher sind auch alle Ihre persönlichen und beruflichen Daten bei mir in guten Händen.*
>
> *Ich sichere Ihnen zu, dass ich sorgsam und streng vertraulich damit umgehe und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen bin.“*

Hochachtungsvoll
Christopher Temt und Michael Werzowa

Anhang

Muster Datenschutzverletzung (WKO)

Sollte Ihnen eine Datenschutzverletzung passiert sein oder Ihnen bekannt geworden sein, die ein Risiko für die Betroffenen bedeutet (neue von ihnen erstellte Risiko-Matrix gelb) so müssen Sie innerhalb von 72 Stunden die zuständige Datenschutzbehörde informieren.

Sollte ein **hohes Risiko** für die Betroffenen bestehen (neu erstellte Risiko-Matrix – doch ROT - und Ihre TOMs), so müssen Sie auch innerhalb von 72 Stunden **alle** Betroffene informieren.

- Bitte die gelb markierten Felder mit Ihren Daten ersetzen

Fernwartung

Bei allen IT-Dienstleistern die mit Hilfe von Fernwartung Zugriff auf ihren Computer bekommen ohne aber pb Daen zu verarbeiten: https://www.datenschutz-guru.de/wartungsvertrag/

Mustervertrag Auftragsverarbeitung (WKO)

- Typische Auftragsverarbeitungen **für Betriebe** nach Art 28 und daher eine **Datenverarbeitungs-Vereinbarung Art 28 DSGVO mit Ihnen notwendig,** sind Dienstleistungen wie:

    - Hosting der Webseiten
    - IT-Anbieter/Datendiensten
    - Software-Anbieter
    - Newsletter-Tool-Anbieter
    - Graphiker und Drucker, wenn sie Visitenkarten von mehreren Personen oder ein Adressbuch oder ein Mitgliederverzeichnis machen (so die Landesdatenschutzbehörde Bayern)
    - Letterdruck (Personalisierter externer Versand)
    - reine Lohnverrechnung

- Wir haben Ihnen in der Datenverarbeitungs-Vereinbarung mit Fernwartung dazugeschrieben
    - Hier muss auch der IT-Anbieter bzw. Software-Anbieter mit Fernwartung angeben, welche Daten er von Ihnen übertragen bekommt, Diese dann bitte unter **X** in das Verarbeitungsverzeichnis vorne dann eintragen!

- weitere mögliche sind:
    - die rein dv-technischen Arbeiten für die Lohn-und Gehaltsabrechnungen oder die Finanzbuchhaltung,
    - Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud Computing (fremder Server)
    - die Werbeadressenverarbeitung in einem Lettershop
    - die Kontaktdatenerhebung durch ein Callcenter,
    - die Auslagerung eines Teils des eigenen Telekommunikationsanlagenbetriebs (soweit nicht TKG),
    - die Datenerfassung, die Datenkonvertierung oder das Einscannen von Dokumenten,
    - die Backup-Sicherheitsspeicherung und andere Archivierungen,
    - die Datenträgerentsorgung
    - Software für das „Customer Relationship Management“ (CRM Systeme)
    - Online Shops,
    - Online Marketing Software
    - Online-Bewerbermanagement Tools
    - Online ~~HR~~ Software,
    - Online Software für das Projektmanagement oder die Zeiterfassung,
    - web - basierte ERP-Systeme.
    - …..
- Sonstige IT-Dienstleister, zu deren Leistungen der Umgang mit personenbezogenen Kunden-/Klienten/Mitgliederdaten gehört

Keine Auftragsverarbeitung und damit Verantwortliche und somit **keine Datenverarbeitungs-Vereinbarung gemäß Art 28 DSGVO notwendig sind** die Auslagerung von Aufgaben/Funktonen oder die externe Inanspruchnahme von Fachleistungen an/von einem Dritten mit dort

eigenverantwortlicher Wahrnehmung wie:

- Personalverwaltung, Mitarbeiterrekrutierung, Vertragskundenbetreuung, Finanzberatung, **Steuerberatung**, Unternehmens/DSGVO-Beratung, Wirtschafsprüfung, Rechtsanwälte, Notar, Kunden, Apotheken, Anbieter von Telefonleitungen, bzw. Internetleitungen, Post, Transport, Ärzte, Krankenhäuser, Sozialversicherung, Inkassotätgkeit mit Forderungsübertragung, Sachveständigen- bzw. Gutachterbeauftragung, usw.

- Bei diesen, da Verantwortliche, müssen Sie nichts tun!

  Es wäre aber anzuraten, das Sie sich vergewissern, dass diese Verantwortlichen auch eine Dokumentation gemäß DSGVO betreffs des Datenschutz haben.

Aber siehe Disclaimer und wenn Sie unsicher sind, so bei zwei Rechtsanwälten nachfragen. Wenn Sie widersprüchliche Antworten bekommt, dann schicken Sie sicherheitshalber ein Datenverarbeitungs-Vereinbarung (siehe Anhang) Sollte der Empfänger ablehnen, so dokumentiert Sie dies!

Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO)

- **Alle Mitarbeiter** müssen dies unterschreiben – am Besten nach deren Schulung!
- In allen Fällen, wo Dritte in Ausübung ihrer beruflichen/ehrenamtlichen Tätigkeit bzw in Ausbildung voraussichtlich **Kenntnis** über teilweise sehr sensible personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse **erhalten könnten**

Mit der Bitte um Ihre Empfehlungen:

Wenn Ihnen die Anleitung und die Vorlage gefällt, sie Ihnen hilft Ihre Datenschutz-Dokumentation zügig und profund fertigzustellen, so würde ich mich über eine Empfehlung von Ihnen freuen:

- auf Google: https://www.google.com/maps?cid=3865384573598671919&hl=en
- auf Herold: https://www.herold.at/gelbe-seiten/wien/H4ZLJ/temt-notfallcoach-im-19-bezirk/
- auf Facebook: https://www.facebook.com/datenschutzberater/

Gerne würde ich Sie auch als neuen Kontakt begrüßen

- auf LinkedIn: https://www.linkedin.com/in/teamberater/
  auch dort gibt es die Möglichkeit zu empfehlen bzw Fähigkeiten anzuklicken
- auf Xing: https://www.xing.com/profile/Christopher_Temt/portfolio

Danke
Christopher Temt

DISCLAIMER

Sämtliche zur Verfügung gestellten Inhalte wurden mit der größtmöglichen Sorgfalt erstellt. Die Autoren, Christopher Temt und Michael Werzowa, übernehmen jedoch keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der bereitgestellten Informationen (einschließlich des Verweises auf externe Quellen WKO, Ärztekammer, ...). Die korrekte Datenschutzdokumentation und die TOMs erfordert stets eine **konkrete Prüfung im Einzelfall**, und meist auch Änderungen in den eigenen Prozessen, weshalb die Beiziehung eines Datenschutzberaters, Besuch eines DSGVO-Workshops, sowie eines Rechtsanwaltes, insbesondere bei der Erstellung oder Überprüfung von Verträgen, dringend empfohlen wird. Die zur Verfügung gestellten Inhalte stellen keine Beratungsleistung welcher Art auch immer dar und können eine Beratung auch nicht ersetzen.

Haftungsansprüche gegen den Christopher Temt, und/oder Michael Werzowa welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden, beziehen, die durch die Nutzung oder Nichtnutzung der zur Verfügung gestellten Informationen verursacht wurden, sind ausgeschlossen. Die Autoren behalten es sich ausdrücklich vor, Teile der zur Verfügung gestellten Information oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.