

Datenschutz Management System (DSGVO Verfahrensverzeichnis)

<https://dsm.cloudcompany.at>

©2018 by Cloudcompany GmbH, A-2070 Retz, Kremserstraße 8
Tel. +43 2942 20670, Email: Info@Cloudcompany.at

Member of

 ARGE DATEN & privacyofficers

Übersicht

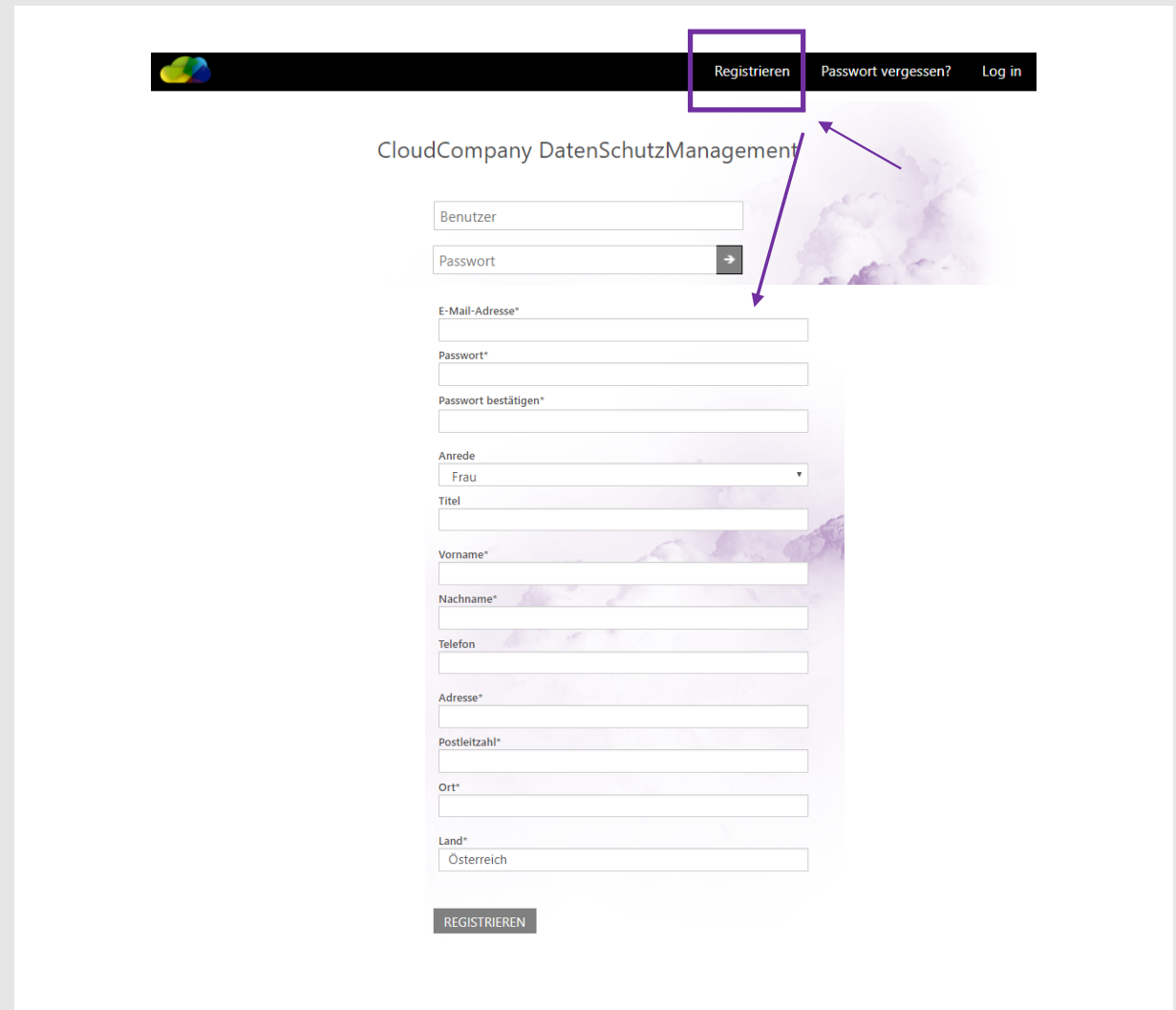
1. Einstieg in das VVZ
 1. Registrierung
 2. Log in
 3. Hilfreiche Funktionen
2. Mandant/Firma erstellen
 1. Allgemein
 2. TOMs
 3. DS-Maßnahmen & Sperr- und Löschmaßnahmen
 4. Dokumente
 5. Datenanwendung erstellen
 1. Allgemein: Art, Zweck,
 2. Datenkategorien
 3. Risikoanalyse/Folgenabschätzung

1. Einstieg in das VVZ

1. Registrierung
2. Log in
3. Hilfreiche Funktionen

1.1. Registrierung

- Um in das VVZ einzusteigen, muss man sich zuerst registrieren
- Das Registrierungstool erreicht man über den Button "Registrieren"
- Nach Ausfüllen der Daten kann sich in Folge einloggen



CloudCompany DatenSchutzManagement

Benutzer

Passwort

E-Mail-Adresse*

Passwort*

Passwort bestätigen*

Anrede
Frau

Titel

Vorname*

Nachname*

Telefon

Adresse*

Postleitzahl*

Ort*

Land*
Österreich

1.2. Log In

- Einloggen kann man sich in Folge über
 - Benutzername
 - Passwort
 - Authenticator

CloudCompany DatenSchutzManagement



1. 3. Hilfreiche Funktionen

- Es gibt mehrere Ebenen im VVZ. (z.B.: Für einen Mandanten können Applikationen und für die Applikationen Datenkategorien erstellt werden)
- **Zurück** = um auf die vorherige Ansicht zurück zu kommen
- **Speichern** = Dadurch kann man einen neuen Datensatz speichern oder wenn man etwas ändern will durch Eingabe neuer Datensätze die alten überschreiben.
- **Neu** = Dadurch kann man neue Firmen, Datenanwendungen, usw. neu anlegen
- **Letzte Änderung** = Man kann immer sehen wann wer das letzte Mal etwas geändert hat. Durch klicken auf "letzte Änderung" erscheint die History, also der Verlauf der bisherigen Änderungen

Mandanten> Testfirma> Testapplikation> Stammdaten bearbeiten

ZURÜCK ←

SPEICHERN 

NEU 

Letzte Änderung am 17.12.2017 um 16:30 von Katrin

1. 3. Hilfreiche Funktionen

- **Öffentliche Dokumente** = In den öffentlichen Dokumenten gibt es Informationen bzw. Gesetzestexte, die eine Rechtsgrundlage für viele Datenkategorien darstellen können

Öffentliche Dokumente

Name	Beschreibung	Datum
DSGVO-Aufbewahrungsfristen.pdf	Auswahl einiger wichtiger bundesgesetzli	22.Dez.2017
AuslBG.pdf	Bundesgesetz vom 20. März 1975, mit dem	02.Dez.2017
SchOG.pdf	Bundesgesetz vom 25. Juli 1962 über die	02.Dez.2017
BPG.pdf	Bundesgesetz vom 17. Mai 1990, mit dem b	02.Dez.2017
TPG.pdf	Bundesgesetz über das Zusammentreffen vo	02.Dez.2017
APG.pdf	Allgemeines Pensionsgesetz (APG)	02.Dez.2017
B-KJHG.pdf	Bundesgesetz über die Grundsätze für Hil	02.Dez.2017
KBBG.pdf	Kinderbetreuungsgeldgesetz (KBBG)	02.Dez.2017
HeimAufG.pdf	Bundesgesetz über den Schutz der persönl	02.Dez.2017
WKO-Cookie-Richtlinie.pdf	WKO Information Cookie-Richtlinie	02.Dez.2017

1 2 >

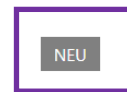
ÖFFNEN

2. Mandant / Firma

1. Allgemein
2. TOMs
3. DS-Maßnahmen & Sperr- und Löschmaßnahmen
4. Dokumente
5. Datenanwendung erstellen

2.1.Allgemein: Mandantenliste

- Nach dem Einloggen erscheint eine Liste aller angelegter Mandanten
- Um einen neuen Mandanten zu erstellen muss man auf “NEU” klicken



Suchen

Mandantenliste

Name	Firmenbuch	Telefon	E-Mail Adresse	Aktiv	Letzte Änderung
Testfirma	0123	0123	test@test.at	Ja	17.Dez.2017

2.1.Allgemein: Mandantenliste

- Um einen Mandanten anzulegen muss man folgende relevante Daten eingeben:
 - Firmendaten
 - Geschäftsführer
 - IT-Leiter
 - Datenschutzbeauftragter
 - Sonstige Ansprechpartner
- **“Aktiv”** = durch diesen Button kann man einen Mandanten aktiv oder inaktiv setzen

Mandanten > Neuer Mandant

Firma	<input type="text"/>	<input type="checkbox"/> Aktiv
Firmenbuchnummer	<input type="text"/>	UID Nummer <input type="text"/>
E-Mail-Adresse	<input type="text"/>	Telefon <input type="text"/> Fax <input type="text"/>
Geschäftsführer Name	<input type="text"/>	Geschäftsführer Telefon <input type="text"/> Geschäftsführer E-Mail <input type="text"/>
IT-Leiter Name	<input type="text"/>	IT-Leiter Telefon <input type="text"/> IT-Leiter E-Mail <input type="text"/>
DSB Name	<input type="text"/>	DSB Telefon <input type="text"/> DSB Email <input type="text"/>
Bemerkungen	<input type="text"/>	

Ansprechpartner	Adresszeile 1	Adresszeile 2
<input type="text"/>	<input type="text"/>	<input type="text"/>
Postleitzahl	Stadt	Land
<input type="text"/>	<input type="text"/>	<input type="text"/>
Ansprechpartner E-Mail	Telefon	Fax
<input type="text"/>	<input type="text"/>	<input type="text"/>

2. 2. TOMs: Allgemein

- Die TOMs gibt es auf mehreren Ebenen
 - 1.Mandant
 - 2.Datenanwendung
 - 3.Datenkategorie
- Wenn die TOMS auf einer höheren Ebene (z.B. dem Mandaten) eingestellt werde, werden diese in Folge automatisch für jede niedrigere Ebene (Datenanwendung & Datenkategorie) übernommen. Man kann sie aber auch auf der niegrigeren Ebene manuell wieder ändern

Technische & Organisatorische Maßnahmen (TOMs)

- Zutrittskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Ausgabekontrolle
- Trennungsgebot
- Verfügbarkeitskontrolle
- Verschlüsselung
- Anonymisierung
- Pseudonymisierung
- Folgenabschätzung erforderlich

2. 2. TOMs

- **Zutrittskontrolle** = Verhinderung eines unbefugten Zutritt zu p.b. Daten
- **Zugriffskontrolle** = Ausschließlich berechnigte Nutzer können auf Inhalte zugreifen, für welche sie berechnigt sind & Daten können nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden

Technische & Organisatorische Maßnahmen (TOMs)

- Zutrittskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Ausgabekontrolle
- Trennungsgebot
- Verfügbarkeitskontrolle
- Verschlüsselung
- Anonymisierung
- Pseudonymisierung
- Folgenabschätzung erforderlich

2. 2. TOMs

- **Weitergabekontrolle** = Verhinderung, dass p.b. Daten bei Weitergabe oder Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können + Dokumentation welche Daten an welche Stellen weitergegeben werden (VVZ)
- **Eingabekontrolle** = Nachträgliche Möglichkeit zu überprüfen, von wem p.b. Daten eingegeben, verändert oder gelöscht worden sind
- **Ausgabekontrolle** = z.B. Prozess zur Verifizierung daß nur an Berechtigte Daten übermittelt werden, z.B. verschlüsselte Datenleitungen, Freigabeprozess etc.,

Technische & Organisatorische Maßnahmen (TOMs)

- Zutrittskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Ausgabekontrolle
- Trennungsgebot
- Verfügbarkeitskontrolle
- Verschlüsselung
- Anonymisierung
- Pseudonymisierung
- Folgenabschätzung erforderlich

2. 2. TOMs

- **Trennungsgebot** = Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden
- **Verfügbarkeitskontrolle** = Schutz der Daten gegen zufällige Zerstörung oder Verlust
- **Verschlüsselung** = z.B. bei elektronischer Übermittlung

Technische & Organisatorische Maßnahmen (TOMs)

- Zutrittskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Ausgabekontrolle
- Trennungsgebot
- Verfügbarkeitskontrolle
- Verschlüsselung
- Anonymisierung
- Pseudonymisierung
- Folgenabschätzung erforderlich

2. 2. TOMs

- **Anonymisierung** = Veränderung der p.b. Daten, sodass diese nicht mehr einer Person zugeordnet werden können
- **Pseudonymisierung** = Veränderung eines Identifikationsmerkmals (z.B. Name) durch ein Pseudonym (Code), um die Feststellung der Identität der Person auszuschließen oder wesentlich zu erschweren. Ein Zusammenführen von Person und Daten ist noch möglich, allerdings nur mit einem Zuordnungscode
- **Folgenabschätzung erforderlich** = Abschätzung der Folgen der Datenverarbeitung für die Betroffenen + Ergreifen von Maßnahmen – Detailinformationen unter Risikoanalyse

Technische & Organisatorische Maßnahmen (TOMs)

- Zutrittskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Ausgabekontrolle
- Trennungsgebot
- Verfügbarkeitskontrolle
- Verschlüsselung
- Anonymisierung
- Pseudonymisierung
- Folgenabschätzung erforderlich

2. 3. DS-Maßnahmen & Sperr- und Löschmaßnahmen

- **DS – Maßnahmen** = Definieren von Maßnahmen bei Verlust von Daten (z.B. interne Melderichtlinien) oder bei Zugriffen (z.B. Vorgehensweise bei unbefugtem Zugriff, Berechtigungsstufen, ...)
- **Sperr- und Löschmaßnahmen** = Analyse ob und wenn ja, wann Daten gelöscht oder gesperrt werden.
Treffen von Maßnahmen für das Löschen und Sperren von Daten

Datenschutzmaßnahmen bei Verlust

Datenschutzmaßnahmen bei Zugriff

Beschreibung der technischen Umsetzung

Sperr- und Löschfristen

Löschen nach Monaten

0

Umsetzung der Sperr- und Löschmaßnahmen

2. 4. Dokumente

- Dokumente, die für die Firma, Datenanwendung, Datenkategorie oder Sonstiges relevant sind, kann man auf allen Ebenen raupladen.
- Die Dokumente werden allerdings NICHT für die niedrigeren Ebenen mitübernommen (Im Gegensatz zu den TOMs)

Dokumente

Name	Beschreibung	Datum
<input type="text"/>	<input type="text"/>	
		<input type="button" value="ÖFFNEN"/>
<input type="text"/>		<input type="button" value="↑"/>
	<input type="text" value="Beschreibung"/>	
		<input type="button" value="SENDEN"/>



2. 5. Datenanwendung

1. Allgemein
2. Datenkategorien
3. Risikoanalyse / Folgenabschätzung

2. 5. 1. Allgemein: Datenanwendungen Liste

- Innerhalb des Mandanten erschreint eine Liste mit den einzelnen Datenanwendungen, die verwendet werden
- Um eine neue Datenanwendung zu erstellen muss man auf “NEU” klicken

NEU Datenanwendungen

Name	Version	Zweck der Anwendung	Abgeschlossen	Aktiv	Letzte Änderung
Testapplikation	1.0		Nein	Ja	17.Dez.2017

2.5.1 Allgemein: Stammdateneingabe

- Um eine Datenanwendung anzulegen muss man folgende relevanten Daten eingeben:
 - Bezeichnung, Version, Kontaktperson
 - Letzes Audit
 - DA Nummer
 - Kategorisierung um welche Art von Datenanwendung es sich handelt:
 - IT- Applikation (z.B. Buchhaltungsprogramm, ...)
 - **Hosting ??**
 - Digitales Dokument (z.B. Excel, PDF, ...)
 - **Cloud**
 - **Analoge Daten**
 - E-Mail
 - **Zweck** = Welchen Zweck soll die Datenanwendung erfüllen
 - Info externer DL
- “Aktiv”

Mandanten> Testfirma> Neue DatenAnwendung

Bezeichnung der Datenanwendung	Version	<input checked="" type="checkbox"/> Aktiv
<input type="text"/>	<input type="text"/>	
Letztes Audit	Abschlussinfo	<input type="checkbox"/> Abgeschlossen
<input type="text" value="2.02.2018"/>	<input type="text"/>	
DA Nummer	Fachabteilung	
<input type="text"/>	<input type="text"/>	
Kontaktperson	Kontaktperson Telefon	Kontaktperson E-Mail Adresse
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> IT Applikation	<input type="checkbox"/> Digitales Dokument	<input type="checkbox"/> Analoge Daten
<input type="checkbox"/> Hosting	<input type="checkbox"/> Cloud	<input type="checkbox"/> E-Mail
Zweck der Anwendung	Info externer Dienstleister	
<input type="text"/>	<input type="text"/>	

2. 5. 2. Datenkategorie: Liste

- Innerhalb der Datenanwendung erscheint eine Liste mit den einzelnen Datenkategorien für eine Datenanwendung
- Um einen neue Kategorie zu erstellen muss man auf “NEU” klicken



Name	Herkunft der Daten	Aktiv	Letzte Änderung
Sensible Daten		Ja	06.Dez.2017
Stammdaten		Ja	06.Dez.2017

2. 5. 2. Datenkategorie: Stammdateneingabe

- Um eine Datenkategorie anzulegen muss man folgende relevante Daten eingeben:
 - Bezeichnung
 - **Besondere Kategorie** = Wenn es sich um sensible Daten handelt
 - **Mitarbeiter / Endkunden / Ansprechpartner / sonstige:** Kategorisierung auf welche Personengruppe die p.b. sich beziehen
 - **Herkunft:** Von wo die Daten stammen und wie sie eingegeben werden (manuell, automatisch über Applikation, ...)
 - **Übermittlung:** Wie und an wen Daten übermittelt werden
- “Aktiv”

Mandanten> Testfirma> Testapplikation> Neue Datenkategorie

Bezeichnung	<input type="text"/>	<input checked="" type="checkbox"/> Aktiv
<input type="checkbox"/> Besondere Kategorie	<input type="checkbox"/> Mitarbeiter	<input type="checkbox"/> Endkunden/Klienten
<input type="checkbox"/> Ansprechpartner bei Geschäftspartnern	<input type="checkbox"/> Ansprechpartner bei Lieferanten	
Sonstige	Herkunft der Daten	Übermittlung der Daten an
<input type="text"/>	<input type="text"/>	<input type="text"/>

2. 5. 2. Datenkategorie: Rechtsgrundlage

- Jede Datenkategorie verlangt eine Rechtsgrundlage
- **Vertrag** = Wenn es mit der betroffenen Person einen Vertrag gibt (z.B. Anstellungsvertrag, Beherbergungsvertrag, ...)
- **Erfüllung rechtlicher Verpflichtungen** = Wenn es eine gesetzliche Grundlage gibt, die eine Datenerhebung/verarbeitung vorsieht
- **Einwilligung mit Nachweis** = Wenn die betroffene Person die Datenerhebung/verarbeitung einwilligt
- **Lebenswichtige Interessen** = Wenn die Datenerhebung/verarbeitung notwendig ist um lebenswichtige Interessen des Betroffenen zu wahren
- **Interessenabwägung** = Es werden die Interessen des Betroffenen und des Datenverarbeiters abgewogen, die eine Datenerhebung/verarbeitung rechtfertigen

Rechtsgrundlagen

- Vertrag
- Erfüllung rechtlicher Verpflichtungen
- Einwilligung mit Nachweis
- Lebenswichtige Interessen
- Interessensabwegung

Sonstige

2. 5. 3. Risikoanalyse / Folgenabschätzung für Datenanwendung: Liste

- Innerhalb der Datenanwendung erscheint eine Liste mit den einzelnen Risikoanalysen / Folgenabschätzungen für eine Datenanwendung
- Um einen neue Kategorie zu erstellen muss man auf “NEU” klicken

NEU Risikoanalyse / Folgenabschätzung			
Schadensszenario	Eintrittsplausibilität	Aktiv	Letzte Änderung
Diebstahl	groß	Ja	05.Feb.2018

2. 5. 3. Risikoanalyse / Folgenabschätzung für Datenanwendung: Stammdateneingabe

- Um eine Datenkategorie anzulegen muss man folgende relevante Daten eingeben:
 - **Schadensszenario** = Beschreibung eines möglichen Schaden (z.B. Diebstahl)
 - Eintrittsplausibilität, Schadenspotential, Schutzmaßnahmen
 - **Schadenspotential & Eintrittsplausibilität Neu** = Wie sich das Risiko nach Implementierung der Maßnahme verändert hat
- “Aktiv”

Mandanten> Testfirma> Testapplikation> Neue Risikoanalyse

Schadensszenario

Eintrittsplausibilität

Aktiv

Schadenspotential

Schutzmaßnahmen

Nach Schutzmaßnahme

Schadenspotential Neu

Eintrittsplausibilität Neu