UGP
Das Unternehmensgründungs-programm des AMS

bit management
member of bit group

ösb Consulting

Im Auftrag des AMS
Arbeitsmarktservice Wien

Handout

Gruppenberatung

Datenschutz und Datensicherheit in meinem Unternehmen

Erstellt: Christian Toller

Am: 01.06.2022

Datenschutz Grundverordnung DSGVO

Das Wichtigste für Gründer/innen knapp zusammengefasst

Aktualisiert am 6.7.2022
Zusammengestellt von: Christian Toller, tethis IT e.U., Wien
Auch online verfügbar: www.tethis-it.at/dsgvo-zusammenfassung
Die Vollständigkeit und Korrektheit dieses Dokumentes wird nicht garantiert.

Die Gesetze

Bisher: Datenschutzgesetz (DSG) 2000
Ab 25.5.2018:

- EU Datenschutzgrundverordnung (DSGVO)
- Österreichische Anpassungen: DSG 2018

Außerdem: E-Commerce Gesetz, Telekommunikationsgesetz, Gewerbeordnung 1994, TKG

Die DSGVO ist in Kraft seit 24.5.2016, verpflichtend umzusetzen ab 25.5.2018

Strafen

Maximal 2% des weltweiten Jahresumsatzes oder 10 Mio. €, je nachdem was höher ist.
In schweren Fällen 4% / 20 Mio. €
Datenschutzbehörde verhängt Strafen, gegen den Bescheid kann Widerspruch eingelegt werden.

Österreichische Anpassung

Am 14. April wurde die „Datenschutz Deregulierung 2018“ beschlossen:

1. Angemessene Bestrafungen (Verhältnismäßigkeit)
2. Beim ersten Verstoß wird nur verwarnt
3. Günstigere Regelung (alt / neu) wird angewendet
4. Behörden bleiben praktisch straffrei, keine Doppelbestrafung
5. Keine Strafen für Spione
6. Schadenersatzforderung durch Organisationen nicht möglich
7. DSGVO gilt nicht für Journalisten
8. Videoüberwachung zulässig

Siehe: https://www.wko.at/branchen/k/handel/versicherungsagenten/erleichterungen-bei-der-dsgvo.html

Wichtig: Die Datenschutzbehörde fühlt sich an die Punkte 1, 2 und 3 NICHT gebunden, weil sie in direktem Widerspruch zur DSGVO stehen, und EU Gesetze Vorrang vor nationalem Recht haben.

Gültigkeitsbereich

Gilt für alle Firmen, die am EU Markt teilnehmen (also auch für ausländische Firmen)

Schützt personenbezogene Daten lebender, natürlicher Personen
Gilt NICHT für

- Daten aus der eigenen Familie und dem Freundeskreis
- Daten Verstorbener
- Anonymisierte Daten

Personenbezogene Daten sind alle Informationen, die irgendwie einer Person zugeordnet werden können (Name, Schuhgröße einer Person, aber nicht ein Landschaftsfoto oder ein Straßenname)

Verarbeitung personenbezogener Daten = alles was man mit einer solchen Information macht (aufschreiben, speichern, kopieren, weitergeben, sichern, ….)

Keine relevanten Ausnahmen für kleine Firmen!

Rollen in der DSGVO

Betroffene(r):	Derjenige, dessen Daten verarbeitet werden. In der Regel ein Kunde, Lieferant, Mitarbeiter
Verantwortliche(r):	Derjenige, der die Daten verarbeitet. In der Regel Ihr!
Empfänger:	Jemand, an den der Verantwortliche Daten weitergibt und der Sie dann eigenverantwortlich verarbeitet
Auftragsverarbeiter:	Jemand, der die Daten im Auftrag des Verantwortlichen verarbeitet, aber keine Verantwortung übernimmt.

Auftragsverarbeiter

Verantwortliche(r): Entscheidet über Zwecke und Mittel der Datenverarbeitung.

Auftragsverarbeiter: Verarbeitet Daten im Auftrag / im Interesse / zugunsten eines Auftraggebers.

Vor allem wer über den Zweck entscheidet, ist verantwortlich.
Das können auch beide sein! Besser für Euch ist geteilte Verantwortung.

Beispiele für Auftragsverarbeiter: Mailchimp, Microsoft Office 365, Webhoster, DropBox, Cloud Datensicherung
Beispiele für selbst Verantwortlicher Banken, Steuerberater, Versanddienstleister

Der Verantwortliche muss sich von Auftragsverarbeiter schriftlich zusichern lassen, dass dieser die DSGVO einhält. Diese Vereinbarung nennt man Auftragsverarbeiter-Vereinbarung. Darin muss dokumentiert werden, welche Daten zu welchem Zweck an den Auftragsverarbeiter übermittelt werden.

Verhältnismäßigkeit

Gefordert sind nur Maßnahmen, die in Hinsicht auf Kosten und Aufwand der Unternehmensgröße und dem Risiko angemessen sind.

Besonders schützenswerte Daten / sensible Daten

„Daten besonderer Kategorien“ machen eine Datenschutzfolgeabschätzung notwendig und erfordern konsequente Schutzmaßnahmen:

- Daten von Kindern (bis 14 Jahre)
- Rassische oder ethnische Herkunft
- Politische Meinungen
- Religiöse o. weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische oder biometrische Daten
- Gesundheitsdaten
- Sexualleben oder sexuelle Orientierung

Die Grundsätze des DSGVO

Die Verarbeitung (also Speicherung, Analyse, Verwendung) von personenbezogenen Daten ist prinzipiell verboten. Die Gesetze regeln nur die Ausnahmen.

1. Rechtmäßig und Transparent

Verarbeitung von personenbezogenen Daten nur mit Rechtsgrundlage erlaubt, z.B.
- aus vertraglichen oder rechtlichen
- lebenswichtigen Interessen
- mit Erlaubnis des Betroffenen

Komplette Liste der Rechtsgrundlagen siehe unten!
Daten müssen rechtmäßig beschafft werden.
Betroffene Personen können Auskunft über die gespeicherten Daten verlangen.

2. Nur mit Zweckbindung

Bei der Zustimmung muss der Zweck der Datenspeicherung benannt werden.
Verarbeitung zu anderen Zwecken erfordert separate Zustimmung

3. So wenig wie möglich

Es dürfen nur so viele Daten erhoben und gespeichert werden, wie für den genannten Zweck notwendig sind.

4. Nur so lange wie nötig

Daten dürfen nur für eine bestimmte Dauer gespeichert werden.
Im Zweifel haben die gesetzlichen Aufbewahrungsfristen Vorrang.
Nach Ablauf dieser Frist müssen die Daten gelöscht werden.

5. Korrekt und sicher

Integrität und Vertraulichkeit
Die Daten müssen gegen versehentlichen Verlust oder Beschädigung geschützt werden
=> Datensicherung ist jetzt Pflicht
Die Daten müssen vertraulich bleiben
=> Zugangsschutz (Passwörter, Berechtigungen)
=> Verschlüsselung
=> Pseudonymisierung

Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung nicht-sensibler Daten:

Laut DSGVO	Grundlage
Art 6 Abs 1 lit a	Mit Einwilligung des Betroffenen
Art 6 Abs 1 lit b	Zur Erfüllung eines Vertrages
Art 6 Abs 1 lit c	Aufgrund rechtlicher Vorschriften
Art 6 Abs 1 lit d	Aus lebenswichtigen Interessen
Art 6 Abs 1 lit e	Bei öffentlichem Interesse
Art 6 Abs 1 lit f	Bei berechtigten Interessen des Verantwortlichen, sofern Rechte des Betroffenen nicht überwiegen (nicht bei Kindern)
Art 9 Abs 2 lit e	Daten wurden vom Betroffenen veröffentlicht

Rechtsgrundlagen für die Verarbeitung sensibler Daten:

Laut DSGVO	Grundlage
Art 9 Abs 2 lit a	Mit Einwilligung des Betroffenen
Art 9 Abs 2 lit b	Aufgrund Arbeits-/Sozialrecht, Kollektivvertrag, Betriebsvereinbarung
Art 9 Abs 2 lit c	Aus lebenswichtigen Interessen
Art 9 Abs 2 lit e	Daten wurden vom Betroffenen veröffentlicht
Art 9 Abs 2 lit f	Zur Geltendmachung von Rechtsansprüchen
Art 9 Abs 2 lit h	Für Zwecke der Gesundheitsvorsorge / medizinischen Behandl.
Art 9 Abs 2 lit g,l,j	Bei erheblichem öffentlichem Interesse (gesundheitlich, wissenschaftlich, historisch)

Rechte der betroffenen Personen

Recht auf Information (Datenschutzerklärung)

Der Betroffene muss, z.B. in einer Datenschutzerklärung, über folgende Punkte informiert werden:
- Name und Kontaktdaten des Verantwortlichen
- Zweck der Verarbeitung
- Gesetzliche Grundlagen oder berechtigte Interessen
- Bei Weitergabe der Daten: Empfänger
- Werden Daten ins nicht-EU-Ausland transferiert? Wie wird die Anwendung der DSGVO sichergestellt?
- Dauer der Speicherung, Kriterien für Löschung

- Die Betroffenenrechte (diese Liste)
- Das Beschwerderecht
- Ob die Bereitstellung der Daten gesetzlich vorgeschrieben oder vertraglich notwendig ist und Folgen falls sie nicht bereitgestellt werden.
- Quelle der Daten (falls nicht direkt vom Betroffenen, z.B. Telefonbuch)

Recht auf Auskunft

Betroffene Personen haben das Recht auf Auskunft in klarer einfacher Sprache
Ergebnisse eigener Arbeit und geistiges Eigentum müssen nicht herausgegeben werden.
Alle Kontaktdaten, E-Mails, CRM Daten sind herauszugeben
Die Auskunft muss kostenlos sein, zumindest solange die Auskunftspflicht nicht missbraucht wird.

Recht auf Berichtigung, Löschung und Einschränkung

Der Betroffene hat das Recht die gespeicherten Daten zu korrigieren.
Er kann fordern, dass die Daten gelöscht werden. Ausnahme: Die Daten müssen aus gesetzlichen oder vertraglichen Gründen gespeichert werden.
Die Verwendung der Daten kann auf bestimmte Zwecke eingeschränkt werden.

Recht auf Datenübertragung

Der Betroffene kann die Übergabe von gespeicherten Daten an ein anderes Unternehmen fordern, z.B. an einen anderen Webhoster oder Mailprovider.

Recht auf Widerspruch

Ein einmal gegebenes Einverständnis zur Datenverarbeitung kann jederzeit widerrufen werden.

Umsetzungsfristen

Für die Umsetzung dieser Rechte: 1 Monat, kann um 2 Monate verlängert werden.

Pflichten des Verantwortlichen

Der Verantwortliche, also derjenige der die Daten verarbeitet, hat folgende Pflichten

Informationspflicht & Umsetzung der Betroffenenrechte

Die Rechte der Betroffenen müssen umgesetzt werden.
Die Informationspflichten sind zu erfüllen (Datenschutzerklärung)

Umsetzung von Maßnahmen zum Datenschutz

Es sind, **in Hinsicht auf Risiko, Aufwand und Größe des Unternehmens angemessene,** technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen.

Privacy by Design

Eingesetzte Technologien sollten bereits mit Blick auf den Datenschutz entwickelt worden sein. Voreinstellungen sollte so gesetzt werden, dass sie dem Datenschutz gerecht werden.

Risikoanalyse

Das Risiko einer Datenschutzverletzung muss analysiert und gewichtet werden. Sollte sich ein hohes Risiko ergeben, muss eine Datenschutzfolgeabschätzung durchgeführt werden. Anm.: Für „normale“ Anwendungen eher nicht nötig.

Meldung von Datenschutzverletzungen

Sollte eine Datenschutzverletzung auftreten, ist dies innerhalb von 72 Stunden der Aufsichtsbehörde zu melden, sofern ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
Sollte ein hohes Risiko bestehen, ist auch die betroffene Person zu informieren.
Eine Datenschutzverletzung wäre z.B. ein Hackerangriff, der Verlust eines Datenträgers, der Diebstahl eines Handys oder Laptops.

Zusammenarbeit mit der Datenschutzbehörde

Ernennung eines Datenschutzbeauftragten

Nur für Firmen, die sich primär mit der Verarbeitung von sensiblen Daten, der systematischen Überwachung beschäftigen oder Datenverarbeitung in großem

Umfang betreiben.
Für kleinere Firmen eher nicht relevant.

Dokumentationspflicht

Die Datenverarbeitungsprozesse müssen in einem Verfahrensverzeichnis (siehe unten) dokumentiert werden.
Unternehmen unter 250 Mitarbeitern müssen das nur, wenn Daten nicht nur gelegentlich verarbeitet werden, sensible Daten verarbeitet werden oder ein Risiko für Rechte und Freiheiten besteht. In der Praxis: Jeder ist verpflichtet.

Außerdem muss nachgewiesen werden:

- Verpflichtung der Mitarbeiter auf Einhaltung des Datenschutzes
- Schriftliche Vereinbarungen mit Auftragsverarbeitern (siehe unten)
- Regelmäßige Überprüfungen der Maßnahmen & Dokumentation

Übersicht über die zu erstellenden Dokumente

Intern (Datenschutzbehörde kann Einsicht verlangen. Für Außenstehenden aber nicht sichtbar, d.h. keine Gefahr von Abmahnungen)

- Verfahrensverzeichnis (welche Daten werden wie verarbeitet?)
- Liste der technischen und organisatorischen Maßnahmen (TOMs)
- Auftragsverarbeiter-Verträge
- Risikoanalyse & Datenschutzfolgeabschätzung
- Entscheidung, dass (kein) Datenschutzbeauftragter ernannt wird
- Mitarbeitervereinbarungen
- Regelmäßige Überprüfung

Extern (Dokumente müssen veröffentlicht oder Kunden zur Verfügung gestellt werden. Gefahr von Abmahnungen, wenn Dokumente fehlen oder falsch sind)

- Datenschutzerklärung
- Einwilligungserklärungen

Datenverarbeitung im Ausland

Datenverarbeitung innerhalb der EU unproblematisch

Außerhalb der EU nur…

- Wenn ein „Angemessenheits-Beschluss“ der EU Kommission vorliegt:
  Norway, Liechtenstein, Iceland, Andorra, Argentina, Canada, Faroer Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, Großbritannien
- Wenn geeignete Garantien vorliegen (ISO Zertifizierung)
- Wenn ein Grund für eine Ausnahme vorliegt:
  - Ausdrückliche Einwilligung
  - Erfüllung eines Vertrages
  - Geltendmachung von Rechtsansprüchen
  - Lebenswichtige Interessen des Betroffenen
  - Öffentliches Interesse
- Wenn in der Auftragsverarbeiter-Vereinbarung die sog. EU Standard-Vertragsklauseln vereinbart sind

Achtung: Das „Privacy Shield“ für US Unternehmen gilt NICHT mehr, da US Behörden immer auf Daten europäischer Bürger zugreifen können, ohne das man sich dagegen wehren könnte. Mehr dazu: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html

Vorgehensweise bei der Umsetzung

1. Verfahrensverzeichnis mit folgenden Informationen erstellen

Die DSGVO macht keine Vorschriften in Hinsicht auf den nötigen Detail-Level, also grob bleiben. D.h. „Buchhaltung“, „Marketing“, „Verkauf über Webshop“ wäre je ein Verfahren.

- Name des Verantwortlichen
- Name der Verarbeitung
- Zweck der Verarbeitung
- Kategorien der verarbeiteten Daten
- Kategorien der betroffenen Personen
- Kategorien der Empfänger
- Übermittlung an Drittländer?
- Fristen für Löschung (wenn möglich)
- Allg. Beschreibung der TOMs (wenn möglich)
- Rechtsgrundlage (ratsam, aber nicht von der DSGVO gefordert)
- Auftragsverarbeiter (ratsam, aber nicht von der DSGVO gefordert)

Bei den Vorlagen gibt es eine Excel-Tabelle („Gedächtnisstütze“), die als Checkliste benutzt werden kann, aber nicht ausgefüllt werden muss.
Die folgende Tabelle ist das eigentliche Verfahrensverzeichnis (als XLS bei den Vorlagen)

Zwecke der Verarbeitung	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (1)	Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (2)	Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO	Rechtsgrundlage der Datenverarbeitung	Auftragsverarbeiter
Finanzbuchhaltung und Rechnungswesen	- Namen, Anschrift, Bankverbindungen, Umsatzsteuer-Identifikationsnummer von Debitoren und Kreditoren - Umsätze inkl. Rechnungsnummer, Verwendungszwecke und sonstige Angaben, die im Zusammenhang mit Finanztransaktionen anfallen - Betroffene Personengruppen: Kunden, Lieferanten,	- Mitarbeiterin zwecks Bearbeitung von Bestellungen. - soweit gesetzlich erforderlich an die Finanzverwaltung, Steuerberater und Wirtschaftsprüfer - ansonsten erfolgt eine Weitergabe der Daten wenn und soweit eine Rechtsgrundlage für die Datenübermittlung vorliegt.	Keine	Buchhaltungsdaten werden für eine Dauer von 7 Jahren aufbewahrt. Nach Ablauf dieser gesetzlichen Aufbewahrungspflicht werden die Daten grundsätzlich gelöscht. Ausgenommen hiervon sind die Fälle, in denen Verwaltungsverfahren oder Gerichtsverfahren anhängig sind, für die betreffenden Daten benötigt werden.	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 6 Abs 1 lit b (Vertragserfüllung) DSGVO Art 6 Abs 1 lit c (rechtliche Vorschriften)	- Microsoft Office 365 - Dropbox
Personalverwaltung	- Name, Anschrift, Geburtsdatum, Personenstand, Staatsbürgerschaft, Kinder, Bankverbindung, Kontaktdaten, Sozialversicherungsdaten, Gehaltsdaten, Krankenstandsdaten, Arbeitsbescheinigungen und weitere Daten laut Liste der Standard- und Musteranwendungen nach DSG 2000 (3) - Betroffene Personen: MitarbeiterInnen	- soweit gesetzlich erforderlich an die Finanzverwaltung, Sozialversicherungsträger, Gemeinden, Arbeitsmarktservice - Steuerberater (soweit für die Buchhaltung erforderlich) - Banken (soweit für Gehaltszahlungen erforderlich) Ansonsten erfolgteine Weitergabe der Daten wenn und soweit eine Rechtsgrundlage für die Datenübertragung vorliegt	Keine	Bis zur Beendigung der Beziehung mit dem Betroffenen und darüber hinaus solange gesetzliche Aufbewahrungsfristen bestehen oder Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können.	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 9 Abs 1 lit a (Einwilligung) DSGVO Art 6 Abs 1 lit b (Arbeitsrecht)	- Microsoft Office 365 - Dropbox
Einkauf	- Kontaktdaten (Name, Firma, Tel. Nr., E-Mail-Adresse) - Betroffene Personen: Händler, Verkäufer, Lieferanten	- Mitarbeiterin	Keine	Bei Beendigung der geschäftlichen Zusammenarbeit, frühestens nach 7 Jahren (Aufbewahrungspflicht)	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 6 Abs 1 lit b (Vertragserfüllung)	- Microsoft Office 365 - Dropbox
Kundenbetreuung	- Name, Firma, E-Mail-Adresse, Tel. und Fax. Nr. - Informationen zu früheren Aufträgen und Anfragen - Kommunkation (E-Mails, SMS, Telefonnotizen) - Betroffene Personen: Kunden	- Newsletterversender - Online CRM System - Microsoft Office 365 (Kontaktdatenbank, E-Mail-Versand)	Keine	Kundendaten werden für eine Dauer von 7 Jahren aufbewahrt. Nach Ablauf dieser gesetzlichen Aufbewahrungspflicht werden die Daten grundsätzlich gelöscht. Ausgenommen hiervon sind die Fälle, in denen Verwaltungsverfahren oder Gerichtsverfahren anhängig sind, für die betreffenden Daten benötigt werden.	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	Art 6 Abs 1 lit a DSGVO (Einwilligung) Art 6 Abs 1 lit b DSGVO (Vertragserfüllung)	- Gsuite (Gmail for Business)
Versand eines Newsletters zu Marketingzwecken	Name, E-Mail-Adresse eines Newsletter-Abonnenten IP-Adresse und Zeitpunkt der Anmeldung zum Newsletter - Betroffene Personene: Newsletterabonnenten	- Mitarbeiterin - Dienstleister für Newsletterversand	Newsletterversender Mailchimp in den USA (Mitglied des Privacy Shield)	- Daten werden mit der Abmeldung vom Newsletter oder bei Unzustellbarkeit der E-Mails gelöscht	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	Art 6 Abs 1 lit a DSGVO (Einwilligung)	Mailchimp

Betrieb einer Webseite zum Marketingzwecken und statistische Analyse der Nutzung	- IP Adressen (Google Analytics: nur anonymisierte IP Adressen) - Bei Nutzung des Kontaktformulars: Name, E-Mail-Adresse, Tel.Nr., IP Adresse - Cookies - Betroffene Personen: Besucher der Webseite	- Webhoster - Dienstleister für Nutzungsanalyse (Google Analytics) - Facebook (Facebook Pixel ohne erweiterten Abgleich)	Dienstleister für Nutzungsanalyse in den USA (Google Analytics und Facebook, beide Mitglied des Privacy Shield)	- IP Adressen beim Webhoster werden nach 3 Monaten gelöscht - Google Analytics Daten werden nach einem Jahr gelöscht	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	Art 6 Abs 1 lit f DSGVO (berechtigte Interessen)	tethis IT (Webhosting) Mailchimp Facebook
Betrieb eines Webshops	- Name, Anschrift, Tel. Nr., E-Mail-Adresse - bestellte Waren - gespeicherte Waren (Wunschliste) - Zahlungsstatus - Betroffene Personen: Nutzer der Webshops	- Mitarbeiterin - Zahlungsdienstleister	Keine	Daten werden für eine Dauer von 7 Jahren aufbewahrt. Nach Ablauf dieser gesetzlichen Aufbewahrungspflicht werden die Daten grundsätzlich gelöscht. Ausgenommen hiervon sind die Fälle, in denen Verwaltungsverfahren oder Gerichtsverfahren anhängig sind, für die betreffenden Daten benötigt werden.	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 6 Abs 1 lit b (Vertragserfüllung) DSGVO Art 6 Abs 1 lit c (rechtliche Vorschriften)	tethis IT (Webhosting)
Logistik und Versand	- Name, Anschrift, Telefonnummer, bestellte Waren - Betroffene Personen: Kunden (Sendungsempfänger)	- Mitarbeiterin - Logistikpartner	Nur bei Versand ins nicht-EU Ausland: Logistikpartner im Empfängerland	Versanddaten werden für eine Dauer von 7 Jahren aufbewahrt. Nach Ablauf dieser gesetzlichen Aufbewahrungspflicht werden die Daten grundsätzlich gelöscht. Ausgenommen hiervon sind die Fälle, in denen Verwaltungsverfahren oder Gerichtsverfahren anhängig sind, für die betreffenden Daten benötigt werden.	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 6 Abs 1 lit b (Vertragserfüllung) DSGVO Art 6 Abs 1 lit c (rechtliche Vorschriften)	keine (Versanddienstleister sind Verantwortliche im Sinne der DSGVO und keine Auftragsverarbeiter)
Datensicherung	- Alle vorher genannten Daten, sofern auf den Geräten der Firma und deren Mitarbeitern, der Webseite oder bei Microsoft im Rahmen des Office 365 Abos gespeichert werden - Betroffene Personen: Mitarbeiter, Kunden, Lieferanten	- Dienstleister für Online Datensicherung	Keine	Datensicherungen werden nach einem Jahr gelöscht	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 6 Abs 1 lit c (rechtliche Vorschriften)	tethis IT (Cloud Datensicherung)
Durchführung von Musikunterricht	- Name, Anschrift, Tel. Nr., E-Mail-Adresse von Eltern (Auftraggeber) und Kind (Schüler) - Geburtsdatum und Unterrichtshistorie des Kindes - Betroffene Personen: Kunden (Eltern und deren Kinder)	- Mitarbeiter	Mail-Provider in den USA (Google Mail, Mitglied des Privacy Shield) Cloud-Speicher DropBox in den USA (Mitglied des Privacy Shield) Beides zwecks Verteilung von Informationen an die Schüler / Kunden	Daten werden für eine Dauer von 7 Jahren aufbewahrt. Nach Ablauf dieser gesetzlichen Aufbewahrungspflicht werden die Daten grundsätzlich gelöscht. Ausgenommen hiervon sind die Fälle, in denen Verwaltungsverfahren oder Gerichtsverfahren anhängig sind, für die betreffenden Daten benötigt werden.	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 6 Abs 1 lit b (Vertragserfüllung) DSGVO Art 6 Abs 1 lit a (Einwilligung) DSGVO Art 9 Abs 1 lit 1 (Einwilligung)	- Julitec - Google Mail - DropBox - WhatsApp
Bereitstellung von Videos der Unterrichtseinheiten	- Videoaufzeichnungen von Unterrichtseinheiten - Betroffene Personen: Schüler	- Schüler - Mitarbeiter	Mail-Provider in den USA (Google Mail, Mitglied des Privacy Shield) Cloud-Speicher DropBox in den USA (Mitglied des Privacy Shield) Beides zwecks Verteilung von Informationen an die Schüler / Kunden	Videos werden binnen eines Monats nach Ende der Kundenbeziehung gelöscht	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)	DSGVO Art 9 Abs 1 lit 1 (Einwilligung)	- Google Mail - DropBox

2. Technische & organisatorische Maßnahmen (TOMs) auflisten.

Beispiele für technische Maßnahmen

- Passwortschutz
- Zugangsbeschränkung (Berechtigungen)
- Verschlüsselung von Laptop und Handy
- Webseite mit HTTPS sichern und selbst HTTPS verwenden
- Datensicherung / Backups:
- Regelmäßige Updates, Updates, Updates
- Virenschutz installieren (der eingebaute reicht)
- Firewall (normalerweise aktiv, UPNP am Router abschalten)
- Schutz der Webseite

Beispiele für organisatorische Maßnahmen:

- Räume verschließen
- Akten, Datenträger und Geräte verschlossen aufbewahren
- Alte Akten Schreddern
- Brandschutz (Feuerlöscher, Rauchmelder)
- Alarmanlage
- WLAN-Router und LAN-Switch wegschließen
- Kommunikationsmittel bewusst wählen
- Unverschlüsselte E-Mails sind nicht sicher
- Need-to-know: Zugang zu Informationen beschränken
- Nach der Arbeit vom PC abmelden / sperren
- Clean Desk Policy, keine Aufrufe mit Namen
- Keine fremden Datenträger / USB Sticks
- Regelmäßig alte Daten löschen
  (z.B. im Rahmen der jährlichen Prüfung der DSGVO Dokumentation)
- Mitarbeiter-Vereinbarungen abschließen:
  1. Verpflichtung zur Geheimhaltung
  2. Regelungen für eigene Geräte
  3. Einwilligung in Datenverarbeitung
- Bei Kündigungen:
  1. Daten löschen (lassen)
  2. Rechte entziehen

3. Dringenden Verbesserungsbedarf identifizieren und umsetzen, z.B.

- Virenscanner installieren
- Datensicherung einrichten
- Newsletter-Anmeldung mit Double-Opt-In einrichten

4. Risikoabschätzung, Datenschutzbeauftragter

Normalerweise stellt die Verarbeiten personenbezogener Daten kleiner Firmen kein sonderliches Risiko dar, Ziel ist also, dass zu dokumentieren.
Dazu muss für jede Verarbeitung (= Zeile im Verfahrensverzeichnis) geprüft werden, ob ein hohes Risiko besteht. Dazu gibt es zwei Hilfsmittel:

1. Liste der Datenschutzbehörde mit Verarbeitungen, die nicht riskant sind: https://www.dsb.gv.at/verordnungen-in-osterreich (siehe auch unten und bei den Vorlagen)
   Lässt sich die Verarbeitung einer der Ausnahmen zuordnen, ist sie nicht riskant => ok

2. Falls das nicht möglich ist, für die restlichen Verarbeitungen den Fragenkatalog der WKO (Checkliste der WKO) beantworten (siehe unten und bei den Vorlagen)
   2 x „Ja“ => Verarbeitung ist wahrscheinlich nicht riskant (argumentieren!)
   > 2 x „Ja“ => Verarbeitung ist riskant, es muss eine Datenschutzfolgeabschätzung gemacht werden
   Ansonsten kein hohes Risiko

Sollte mindestens eine Verarbeitung ein hohes Risiko darstellen, muss eine Datenschutzfolgeabschätzung erstellt werden!

Außerdem: Entscheiden, ob ein Datenschutzbeauftragter nötig ist.
Nur für Firmen die sich primär mit der Verarbeitung von sensiblen Daten oder der regelmäßigen und systematischen Überwachung beschäftigen.

Entscheidungen dokumentieren

Verarbeitungen, für die laut Datenschutzbehörde kein hohes Risiko besteht und demnach auch keine Datenschutzfolgeabschätzung nötig ist:

- Bild- und Akustikdatenverarbeitung in Echtzeit
- Bild- und Akustikverarbeitungen zu Dokumentationszwecken
- Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken
- Rechts- und Beratungsberufe
- Archivierung, wissenschaftliche Forschung und Statistik
- Unterstützungsbekundungen
- Aktenverwaltung (Büroautomation) und Verfahrensführung
- Organisation von Veranstaltungen
- Preise und Ehrungen
- Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
- Personalverwaltung
- Mitgliederverwaltung
- Kundenbetreuung und Marketing für eigene Zwecke
- Sach- und Inventarverwaltung
- Register, Evidenzen, Bücher
- Zugriffsverwaltung für EDV-Systeme
- Zutrittskontrollsysteme
- Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)

	Verarbeitungsverfahren laut Verfahrensverzeichnis					
Risikokriterien	Finanzbuchhaltung und Rechnungswesen	Personalverwaltung	Kundenbetreuung	Versand eines Newsletters zu Marketingzwecken	Betrieb einer Webseite zum Marketingzwecken und statistische Analyse der Nutzung	Datensicherung
Bewirkt der Verarbeitungsvorgang ein (potentielles) Bewerten oder Einstufen betroffener Personen (etwa das Erstellen von Profilen und Prognosen), insbesondere auf Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen? Beispiel: Nutzer-Verhaltensprofile oder Marketingprofile durch Website-Analyse-Tools.	Nein	Nein	Nein	Nein	Nein	Nein
Beinhaltet der Verarbeitungsvorgang eine automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung?	Nein	Nein	Nein	Nein	Nein	Nein
Beinhaltet der Verarbeitungsvorgang möglicherweise eine systematische Überwachung, d.h. Vorgänge, die die Beobachtung, Überwachung oder Kontrolle betroffener Personen zum Ziel haben?	Nein	Nein	Nein	Nein	Nein	Nein
Werden vertrauliche Daten oder höchst persönliche Daten verarbeitet? Beispiele: „Sensible Daten“, personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten; aber auch personenbezogene Daten, die mit häuslichen oder privaten Aktivitäten verknüpft sind (z.B. private elektronische Kommunikation), sich auf die Ausübung der Grundrechte auswirken (z.B. das Erfassen der Standortdaten, wodurch eine Verfolgung des Bewegungsverhaltens ermöglicht wird und den Schutz der Privatsphäre berühren kann) oder deren Nutzung möglicherweise ernsthafte Konsequenzen im Alltag der betroffenen Personen haben kann (z.B. Bankdaten, die für den Zahlungsbetrug missbraucht werden könnten)	Nein	Ja	Nein	Nein	Nein	Nein
Erfolgt eine Datenverarbeitung in großem Umfang?	Nein	Nein	Nein	Nein	Nein	Nein
Zahl der betroffenen Personen (entweder konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe)	~500	1	~200	~200	~2000/Monat	~500
verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente	geringe Datenmenge	geringe Datenmenge	geringe Datenmenge	geringe Datenmenge	geringe Datenmenge	geringe Datenmenge
Dauer oder Dauerhaftigkeit der Datenverarbeitung	Löschung nach gesetzlicher Frist	Löschung nach gesetzlicher Frist	Löschung nach gesetzlicher Frist	Löschung bei Abmeldung	3 Monate	1 Jahr
geografisches Ausmaß der Datenverarbeitung	AT, D, CH	AT	AT, D, CH	AT, D, CH	AT, D, CH	AT, D, CH
Beinhaltet die Datenverarbeitung ein (potentielles) Abgleichen oder Zusammenführen von Datensätzen? Beispiel: Zusammenführen von Datensätzen aus unterschiedlichen Anwendungszwecken und dieser Vorgang von den betroffenen Personen vernünftigerweise auch nicht erwartet werden konnte.	Nein	Nein	Nein	Nein	Nein	Nein
Werden möglicherweise Daten schutzbedürftiger betroffener Personen verarbeitet? Beispiele: Kinder, Personen mit besonderem Schutzbedarf (Patienten, psychisch Kranke, Senioren, Asylbewerber), Arbeitnehmer.	Nein	Ja	Nein	Nein	Nein	Nein
Beinhaltet der Verarbeitungsvorgang eine innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen? Beispiel: Kombination aus Fingerabdruck- und Gesichtserkennung zum Zweck einer verbesserten Zugangskontrolle.	Nein	Nein	Nein	Nein	Nein	Nein
Kann die Datenverarbeitung die betroffenen Personen (potentiell) an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern? Beispiel: Durchsuchen von Bonitätsdatenbanken zum Zweck der Entscheidung, ob ein Kredit vergeben wird.	Nein	Nein	Nein	Nein	Nein	Nein
	kein hohes Risiko	**potentiell hohes Risiko**	**kein hohes Risiko**	**kein hohes Risiko**	**kein hohes Risiko**	**kein hohes Risiko**

5. Datenschutzerklärung(en) mit folgenden Punkten erstellen

- Verantwortlicher
- Welche Daten & Zweck der Verarbeitung
- Quelle, falls nicht selbst eingegeben
- Rechtsgrundlage
- Werden berechtigte Interessen verfolgt? Welche?
- Weitergabe an Drittstaaten? Ist der Empfänger "sicher"?
- Dauer der Speicherung, Kriterien für Löschung
- Werden automatisch Entscheidungen getroffen? Welche?
- Rechte des Betroffenen (Auskunft, Widerspruch, Beschwerde, etc.)
- Datenschutzbeauftragter, Kontaktdaten

Beispiele für Datenschutzerklärungen werden zum Download bereitgestellt.
Für die Datenverarbeitung durch die Webseite kann auch ein Generator verwendet werden. Dabei aber bitte beachten, dass keine deutschen Gesetze erwähnt werden sollten. Außerdem decken die Generatoren die Datenverarbeitung im Rahmen der eigentlichen Tätigkeit nicht ab.

Es spricht nichts gegen zwei Datenschutzerklärungen, eine für die Webseite und eine, die z.B. bei Vertragsabschluss übergeben wird.

6. Auftragsverarbeiter-Verträge einsammeln

- Beim Newsletter-Provider, Webhoster, Anbieter von Clouddiensten anmelden und nachsehen, ob es irgendwo eine Auftragsverarbeiter-Vereinbarung, Data Processing Agreement, Data Processing Addendum oder ähnliches gibt.
- Alternativ anschreiben und Auftragsverarbeiter-Vertrag anfordern
- Oder in folgender Liste von Clouddiensten und den dazugehörigen Auftragsverarbeiter-Vereinbarung nachsehen:
  https://www.blogmojo.de/av-vertraege/

7. Einwilligungserklärungen formulieren

Eine korrekte Einwilligungserklärung muss:

- keiner bestimmten Form folgen
- dokumentierbar sein (also eher schriftlich, elektronisch)
- Freiwillig erfolgen (keine Abhängigkeiten)
- Für einen bestimmten Fall erfolgen (Zweck nennen)
- In informierter Weise erfolgen (nicht verstecken, klare Sprache)

Vorausgefüllte Erklärungen (gesetzter Haken) sind nicht zulässig.
„Kopplungsverbot" beachten!

Beispiel-Formulierungen:

- ☐ Ich möchte regelmäßig per E-Mail Informationen rund um die Humanenergetik und zu neuen Workshops erhalten. Bitte senden Sie mir Ihren Newsletter an folgende E-Mail-Adresse: <Feld zum Eingeben der E-Mail-Adresse>
- ☐ Ich möchte Sitzungen per Skype durchführen und stimme der Übermittlung meines Namens und meiner E-Mail-Adresse an Skype sowie der Übertragung des Gespräches mittels Skype zu. Skype ist eine Dienstleistung der Microsoft Corp., USA. Die Daten werden in die USA übertragen.
- ☐ Ich möchte per E-Mail kommunizieren und stimme der Übermittlung von persönlichen und/oder vertraulichen Daten per unverschlüsselter E-Mail zu. Mir ist bewusst, dass die Inhalte dieser E-Mails auf dem Übertragungsweg möglicherweise in Drittstaaten übertragen und von Dritten eingesehen werden können.

Auch ein Cookie Popup ist eine Einwilligung. Dafür am besten ein Plugin oder eine Funktion des Webseiten-Baukastens wählen, das bei der Formulierung hilft.

8. Weisungen an Mitarbeiter dokumentieren

- Mitarbeiter müssen vertraglich zur Einhaltung des Datenschutzes verpflichtet werden

9. Regelmäßige Prüfung / Verbesserung

- Ist das Verarbeitungsverzeichnis vollständig?
- Haben sich die Risiken verändert?
- Wurden die TOMs umgesetzt?
- Sind die TOMs noch angemessen?
- Die jährliche Prüfung ist zu dokumentieren

Technische Maßnahmen zum Datenschutz

Sind Cloud-Dienste sicher

Cloud Dienste wie DropBox, OneDrive oder eine Online Buchhaltungslösung habe einige Vorteile:

- erhöhte Redundanz / Fehlertoleranz
- bessere Überwachung
- kein eigenes technisches Knowhow nötig
- räumliche Trennung der Daten
- evtl. Versionierung
- verbesserte Teamarbeit

Aber: Man vertraut einer fremden Firma eigene Daten (und die der Kunden) an. Bei der Auswahl ist Vertrauen entscheidend.
Der Anbieter muss in der EU oder einem „sicheren" Drittland sein
Der Anbieter muss eine Auftragsdatenvereinbarung zur Verfügung stellen

Das Thema WhatsApp

Das Problem: WhatsApp verschickt bei der Installation das komplette Telefonbuch des Handys. D.h. Nutzung auf einem Handy mit Kunden-Tel. Nummern ist nicht legal.
Dazu ist die Einwilligung aller Personen, die im Telefonbuch gespeichert sind, notwendig

Mögliche Auswege:

- Keine Tel. Nr. speichern, oder erst nach Einwilligung des Kunden
- Handy benutzen, das separate Telefonbücher erlaubt (z.B. Blackberry)
- Alternative Apps: Threema, Signal oder SMS
- Mit Hilfe einer Mobile-Device-Management Lösung den Zugriff von WhatsApp auf das geschäftliche Telefonbuch verhindern: https://www.miradore.com/de/ oder https://www.manageengine.com/mobile-device-management/

Passwörter

- Kein Gerät, keine Web-Anwendung ohne Passwort!
- Bildschirmschoner mit Passwort einrichten
- Länge ist wichtig! Lieber ein langes Passwort als ein komplexes
- Für jede Anwendung ein eigenes Passwort! Sonst hat der Verlust eines Passworts schwere Konsequenzen
- Tipp für das Bilden von Passwörtern: Immer das gleiche am Anfang, am Schluss variabel, dabei Sonderzeichen und Großbuchstaben einstreuen, z.B.: !mmerDasGle1chefacebook!
- Passwortmanager nutzen: lastpass.eu, 1password.com, keepass.info

Passwortdiebstahl erkennen und reagieren

Auf https://haveibeenpwned.com/ und https://sec.hpi.de/ilc/ prüfen, ob das eigene Passwort bekannt geworden ist
Falls ja, sind alle Dienste, bei denen man sich mit der betroffenen Kombination aus Benutzername & Passwort anmeldet, gefährdet.

- ⇒ Sofort Passwort ändern
- ⇒ Im Zweifel: Alle wichtigen Passwörter ändern!

Wenn möglich, 2-Faktor Authentisierung benutzen

Dabei wird zusätzlich zum Passwort auch noch ein Code auf das Handy geschickt, ein Code per E-Mail geschickt, eine Handy-App verwendet, das Gesicht oder ein Fingerabdruck erkannt.

Prinzipiell sichere als Anmeldung nur mit Passwort, ist aber etwas aufwendiger in der Nutzung.

Viele Anbieter von Cloud-Diensten bieten 2-Faktor-Authentisierung an (auch als MFA oder 2FA bezeichnet).
Für die eigene Webseite gibt es Plugins (z.B. Google Authenticator, Wordfence, Wordpress 2-step verification, Duo, Rublon, Two Factor Authentication)

Geräte und externe Speicher verschlüsseln

Verhindert, dass Geräte und Speicher unbefugt ausgelesen werden und sorgt bei Diebstahl dafür, dass wir die Datenschutzbehörde und unsere Kunden NICHT informieren müssen.

	Handy	Computer
Apple	standardmäßig eingeschaltet	Festplatten Dienstprogramm / Filevault aktivieren
Windows / Android	Einstellungen / Sicherheit / Verschlüsseln bei neueren Huawei Handys schon eingeschaltet	Win 10 Pro oder neuer Computer: Bitlocker aktivieren Alternativ Vera-Crypt installieren Win10 Home kann günstig auf Pro upgegradet werden

DSGVO und die eigene Webseite

https / verschlüsseltes Internet

Die Verwendung von https hat zwei Vorteile:

1. Beweist, dass die Webseite tatsächlich vom Eigentümer stammt.
   Aber Vorsicht! Die Domäne muss stimmen (also keine Fake-Domäne wie bonkoustria.at)
2. Die Daten werden zwischen Browser und Webserver verschlüsselt übertragen und können nicht „abgehört" werden.
3. Google „bestraft" Seiten, die kein https verwenden mit schlechterem Ranking
4. Die Browser warnen vor Seiten ohne https

Für die eigene Webseite ist https Pflicht, sobald ein Besucher Daten eingeben kann (Newsletter Anmeldung, Kontaktformular, Webshop).

Für https benötig man ein Zertifikat. Let's Encrypt Zertifikate sind kostenlos und sollten von jedem Webhoster zur Verfügung gestellt werden.

Neue Webseite unbedingt mit https einrichten.
Nachträgliche Umstellung kann kompliziert werden. Auf „Likes" achten!
Anleitungen: https://www.wpbeginner.com/wp-tutorials/how-to-add-ssl-and-https-in-wordpress/, https://www.miss-webdesign.at/wordpress-auf-https-umstellen/

Ist die Webseite DSGVO-konform?

Zu beachten ist jede Funktion, die Daten über Besucher sammelt und evtl. (z.B. zur Analyse) weitergibt:

- Server-Protokolle
- Social-Media (Like-Buttons, Share-Buttons)
- Anti-spam oder Sicherheits-Funktionen
- Statistiken, Performance Monitoring
- Ressourcen von anderen Seiten (Videos, Bilder, Fonts)
- Cookies

Wenn unklar ist, ob und welche Daten verarbeitet bzw. weitergegeben werden:

- googeln hilft!
- Plugin hier prüfen: https://www.blogmojo.de/wordpress-plugins-dsgvo/

Ist eine Einwilligung nötig?

Immer dann, wenn wir keine andere Rechtsgrundlage finden. In Frage kommen:
Vertrag => Information in der Datenschutzerklärung reicht
Berechtigtes Interesse => Information und eventuell Opt-Out
Wenn das Interesse des Besuchers überwiegt oder falls „nicht für den Betrieb der Webseite notwendig" => Einwilligung einholen

Beispiele:

Vertrag	Berechtigtes Interesse	Einwilligung
WooCommerce Angebotsformular Kursanmeldung	Server Logfiles Google Fonts Google Re-Captcha Kommentarformular	Google Analytics Facebook Pixel Akismet JetPack

Einwilligung so weit wie möglich vermeiden, weil es den Besucher mit einer Frage belästigt und oft nur schwer zu realisieren ist (Verarbeitung darf erst nach der Einwilligung passieren)

Cookies

Cookies speichern Besucher-spezifische Information in dessen Browser. Damit können Besucher auch auf anderen Webseiten wiedererkannt werden.

	Für den Betrieb der Webseite nötig	Nicht unbedingt nötig
Beispiele	Session Cookies Login Warenkorb Cookie-Entscheidung	Google Analytics Tracking Werbung Facebook etc.
Rechtsgrundlage	Berechtigtes Interesse	Einwilligung
Reicht Hinweis?	Ja. Datenschutzerklärung plus Cookie Hinweis	Nein. Cookie Hinweis mit Option mit Einwilligung nötig plus Datenschutzerklärung

Für den Cookie Hinweis ein Plugin verwenden, dass die Einwilligung abfragt und dafür sorgt, dass Google Analytics oder externe Medien nur geladen werden, wenn der Besucher zustimmt. Übersicht für WordPress hier: https://www.blogmojo.de/wordpress-cookie-plugins/, ich nehme meistens https://borlabs.io

Webseite sichern

Webseiten, Webserver, etc. werden ständig angegriffen
(Brute-Force-Attacks, Ausnutzung von Exploits)
Dagegen helfen:

- Updates!
- Sichere Passwörter UND Benutzernamen (nicht „admin“)
- 2-Faktor Authentisierung einrichten (z.B. Google Authenticator, Wordfence, Wordpress 2-step verification, Duo, Rublon, Two Factor Authentication)
- HTTPS für Admin-Bereich nutzen (sowieso nötig)
- Sicherheitsplugins können helfen, z.B. Wordfence, WPS Hide Login, Disable REST API (aber viel Unsinn am Markt)

Anleitung z.B. http://www.erfolgsrezepte-online.de/wordpress-absichern/

Datensicherung

Anforderungen an eine gute Datensicherung:

- Automatisch
- Räumlich getrennt
- Keine Arbeitskopie
- Speichert Versionen (hilft gegen Ransomware)

Was sollte gesichert werden
Natürlich alles, was für den Betrieb des Unternehmens relevant ist, lt. DSGVO insbesondere personenbezogene Daten.

- Daten auf dem Computer & NAS (wo sind relevante Daten?)
- Daten auf dem Handy
- E-Mails
- Webseite
- Daten aus Cloudlösungen (Buchhaltung, Online-Galerie, …)
- Daten aus Cloud-Speicher (Dropbox, OneDrive, etc.)

Wichtig: Wiederherstellung unbedingt testen! Ohne Test ist eine Datensicherung wertlos!

Mögliche Methoden für die Sicherung

- Kopie auf verschlüsselte externe Festplatte, USB Stick
  nicht automatisch, keine Versionen, E-Mails nicht enthalten, räumlich getrennt?
- Synchronisation mit Cloud-Speicher
  kurze Aufbewahrung, evtl. keine Versionen, Arbeitskopie, keine E-Mails, räumlich getrennt
- Cloud-Backup (tethis CDS, Veeam, Acronis und andere)
  automatisch, Versionen, E-Mails möglich, räumlich getrennt, abhängig vom Internet
  sichert auch Daten aus der Cloud und Office 365 oder Exchange Mailboxen, Datenbanken
- Backup auf NAS / Server / externe Platte mit Backup-Programm
  automatisch, Versionen, E-Mails möglich, räumlich getrennt?

Wichtige Erwägungen bzgl. Datensicherung

- Wo speichert das E-Mail-Programm die E-Mails?
  Diesen Ordner sichern
- Sichert der Webhoster evtl. die E-Mails?
- Cloud-Backup sichert z.T. auch E-Mails (Office 365)
- Wordpress: Plugins benutzen, sichern auf anderen Server
- Sichert der Webhoster? Mit Versionen?
- Regelmäßig komplett herunterladen (Dateien und Datenbank)
- Handy: eingebautes Backup, Backup Apps

Eingebaute Backuplösungen bei MacOS und Windows 10

Windows 10: Dateiversionsverlauf
Einrichtung:

- *Einstellungen* / *Update & Sicherheit* / Sicherung
- Externe Festplatte: *Laufwerk hinzufügen*
- Netzwerklaufwerk: *Weitere Optionen* / *Siehe erweiterte Einstel.* / *Netzwerkadresse auswählen* / *Netzwerkadresse hinzufügen*

Wiederherstellung:

- *Einstellungen* / *Update & Sicherheit* / Sicherung / *weitere Optio.*
- Ganz unten: *Daten von einer aktuellen Sicherung wiederherstellen*

MacOS: TimeMachine
Einrichtung:

- *Einstellungen* / *TimeMachine*/ *Backup-Volume auswählen*
- Externe Festplatte: *Laufwerk auswählen*
- Netzwerklaufwerk: Vorher im Finder *Gehe Zu / Mit Server verbinden /* NAS bzw. TimeMachine (Gerät) auswählen

Wiederherstellung:

- *Im Finder Programme / TimeMachine aufrufen*
- *Rechts Datum auswählen, Datei auswählen*

Updates, Updates, Updates

- Wichtigste Schutzmaßnahme (neben „Augen offen halten“)
- Ständiger Wettlauf zwischen Hackern und Herstellern
- Wann immer möglich: Automatisch installieren!
  Nachteil: kostet Zeit, kann Fehler verursachen
- Webseite: Wordpress (CMS) Updates installieren
  Vorher unbedingt Backup machen!
- Geräte: Modems, Router, Home-Automation nicht vergessen
- Handy: Updates nicht verhindern

Virenscanner

- Auch für Macs und Linux eine gute Idee
- Wichtig ist vor allem der „Echtzeitschutz“
- Regelmäßige Updates sind Pflicht
- Meine persönliche Meinung: Microsoft Defender reicht aus
- Auf Handys gelten Virenscanner als problematisch
- Wenn Virus / Trojaner gefunden wurde:
- Gefundenen Virus im Internet nachschlagen
- Von USB / CD starten und komplett prüfen

Die Augen offenhalten!

- Schadsoftware kommt meistens per E-Mail
- Mailprogramm komplette Adresse anzeigen lassen
- Vorsicht mit Anhängen bei unbekannten Absendern
- Warnungen NICHT einfach wegklicken
- Programme nur aus seriösen Quellen herunterladen
- Im Zweifel: Abbrechen
- Nach Infektion: Von sauberem Medium starten, testen, neu installieren

Firewall

Gibt es im Router und in jedem PC / Mac
Unterbindet eingehende Verbindungen aus dem Internet
Ausgehende Verbindungen (und Antworten) sind erlaubt
„UPNP“ abschalten, damit können sich Apps selbst „ein Loch“ in die Firewall bohren, was normalerweise nicht nötig ist

Organisatorische Maßnahmen

Kommunikationsmittel bewusst wählen!

Unverschlüsselte E-Mails sind nicht sicher
E-Mail-Verschlüsselung ist einfach, erfordert aber den Austausch von Zertifikaten oder Passwörtern
Anleitung für Outlook https://outlook-blog.de/9161/e-mails-in-outlook-verschluesseln/
Alternative 1: Einwilligung einholen
Alternative 2: Dropbox, OneDrive, SharePoint oder eigene Webseite benutzen

Weitere organisatorische Maßnahmen

- Need-to-know: Zugang zu Informationen beschränken
- Nach der Arbeit vom PC abmelden / sperren
- Clean Desk Policy, keine Aufrufe mit Namen

- Keine fremden Datenträger / USB Sticks
- Regelmäßig alte Daten löschen
  (z.B. im Rahmen der jährlichen Prüfung der DSGVO Dokumentation)
- Räume verschließen
- Akten, Datenträger und Geräte verschlossen aufbewahren
- Alte Akten Schreddern
- Brandschutz (Feuerlöscher, Rauchmelder)
- Alarmanlage
- WLAN-Router und LAN-Switch wegschließen

Mitarbeiter-Vereinbarung abschließen

- Verpflichtung zur Geheimhaltung
- Regelungen für eigene Geräte
- Einwilligung in Datenverarbeitung

Nach Kündigung eines Mitarbeiters aufräumen

- Daten löschen
- Zugangsrechte entziehen
- Schlüssel und Geräte zurücknehmen

Am Besten vorher einen Prozess für den Austritt von Mitarbeitern definieren und erteilte Rechte dokumentieren

Übrigens: Mails eines entlassenen Mitarbeiters dürfen nicht ohne weiteres gelesen werden. Selbst wenn dem Mitarbeiter die private Nutzung der Mailaccounts verboten war, muss man spätestens bei der ersten privaten Information aufhören zu lesen.
Ideal: Vorher mit dem Mitarbeiter vereinbaren, dass man nach Ende des Arbeitsverhältnisses die Mails lesen darf.

Wichtige Links, Beispiele, Vorlagen

Österreichische Datenschutzbehörde (Gesetzestexte, Formulare, Leitfaden zur Umsetzung)
https://www.dsb.gv.at

Datenschutz Deregulierungsgesetz 2018
https://www.parlament.gv.at/PAKT/VHG/XXVI/A/A_00189/index.shtml

WKO (Gesetze, Vorlagen, Checklisten):
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

WKO Checkliste zur Risikoabschätzung und Anleitung Datenschutzfolgeabschätzung:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

WKO Vorlage für eine Mitarbeitervereinbarung:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html

WKO IT-Safe: Tipps zu Datenschutzmaßnahmen, auch speziell für EPUs
https://www.wko.at/site/it-safe/start.html

WKO IT-Safe Fragebogen: Identifiziert Lücken im Datenschutz
https://itsafe.wkoratgeber.at/

WKO: Auswirkungen der DSGVO auf Webseiten und Webshops:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Auswirkungen-auf-Websites.html
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/datenverarbeitung-webshop-website.html

WKO: Bedingungen für erlaubten E-Mail-Versand:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html

RTR: Liste mit E-Mailadressen an die keine Werbung geschickt werden darf
https://www.rtr.at/de/tk/TKKS_ECGListe

WKO: Informationspflichten in einem Newsletter
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationspflichten_nach_dem_Mediengesetz_fuer_E-Mail-Ne.html

PrivacyOfficers.at, Verein österreichischer Datenschutzbeauftragter:

https://www.privacyofficers.at
z.B. Checkliste für die Umsetzung der DSGVO (eher für größere Unternehmen)
https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v1.0_24052017_FINAL.pdf

Stefan Hansen-Oest: Deutscher Anwalt mit pragmatischen Ansätzen zur DSGVO Umsetzung
http://www.datenschutz-guru.de

Stefan Hansen-Oest: Liste von möglichen TOMs zum Ankreuzen:
http://www.datenschutz-guru.de/files/Ausfuellhilfe_TOM_9_BDSG_V2.docx

Generator für Datenschutzerklärung
https://www.adsimple.at/datenschutz-generator/
https://www.ratgeberrecht.eu/leistungen/muster-datenschutzerklaerung.html

EU Standard-Vertragsklauseln für die Auftragsverarbeiter-Vereinbarung
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de

tethis IT: Beispiel einer Datenschutzerklärung inkl. Google Analytics, Mailchimp und Cloud-Diensten
https://tethis-it.at/dsgvo-informationspflichten/

Liste von Wordpress-Plugins und ob sie DSGVO-konform sind:
https://www.blogmojo.de/wordpress-plugins-dsgvo/

Liste von Cloud-Dienstleistern und wie man Auftragsverarbeiter-Verträge bekommt:
https://www.blogmojo.de/av-vertraege/

Wordpress-Plugins für Google Analytics und Facebook Pixel Opt-Out:
https://wordpress.org/plugins/opt-out-for-google-analytics/
https://wordpress.org/plugins/opt-out-facebook-pixel-dsgvo-gdpr/
(Hinweise zur Installation gibt es dort auch, nicht vergessen den Shortcode in die Datenschutzerklärung einzubauen.)