ROADMAP DSGVO

Dokumentation: Verarbeitungsverzeichnis	Das Verarbeitungsverzeichnis hat eine Aufstellung zu enthalten, welche Datenkategorien und Datenarten auf welcher Rechtsgrundlage verarbeitet werden, wie lange sie gespeichert werden und welche technischen und organisatorischen Maßnahmen zu ihrem Schutz angewendet werden. Dies kann zB in Form einer Excel Tabelle geschehen. Ein Beispiel dafür finden Sie unter: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html. Werden nur die Kontaktdaten der Kunden/Klienten im Adressbuch (auch am Telefon) oder in den E-Mails gespeichert, ist das Führen eines Verarbeitungsverzeichnisses nicht notwendig.	Art 30 DSGVO
DEFINITIONEN		
Personenbezogene Daten	Unter „**personenbezogene Daten**“ versteht man alle Daten, die eine Person identifizieren oder identifizierbar machen. Dazu gehören alle Daten, durch die direkt oder indirekt ein Zusammenhang mit der Person hergestellt werden kann. Das sind Daten wie der Name, die Anschrift, das Geburtsdatum, eine Kennnummer oder auch Merkmale, die Auskunft über die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität geben. Personen, deren Daten verarbeitet werden, werden als „**betroffene Personen**" bezeichnet. Die Daten von juristischen Personen (Unternehmen) sind von der DSGVO nicht geschützt (teilweise jedoch vom Datenschutzgesetz). Wenn ein Vertrag zwischen zwei Unternehmen geschlossen wird (B2B-Verhältnis), sind die Vorschriften der DSGVO auf die Daten des Unternehmens nicht anwendbar, auf die der Mitarbeiter allerdings schon.	Art 4 DSGVO
Besondere Kategorien personenbezogener Daten	Unter „**Daten besonderer Kategorien**", auch „**sensible**" **Daten** genannt, werden Daten verstanden, die den höchstpersönlichen Lebensbereich einer betroffenen Person betreffen. Das sind Daten, aus denen zB die rassische und ethnische Herkunft, die politische Meinung oder eine Gewerkschaftszugehörigkeit hervorgehen. Ebenso ist die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten oder Daten zum Sexualleben, der sexuellen Orientierung oder der Religionszugehörigkeit umfasst. Eine Verarbeitung dieser Daten ist prinzipiell verboten, außer die betroffene Person hat in die Datenverarbeitung eingewilligt oder es liegt ein anderer, in der DSGVO oder in einem Gesetz explizit genannter, Grund für die Verarbeitung vor.	Art 9 DSGVO
Verarbeitung	Unter „**Verarbeitung**" versteht man jeden mit oder ohne automatisierten Verfahren ausgeführten Vorgang oder eine Vorgangsreihe, bei dem personenbezogene Daten verwendet werden. Dazu gehören unter anderem das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Ab 25.05.2018 sind keine DVR - Meldungen mehr notwendig.	Art 6 DSGVO
Verantwortlicher	Unter „**Verantwortlicher**" versteht man die (natürliche oder juristische) Person, die die personenbezogenen Daten verarbeitet (zB erhebt, verwaltet, speichert, übermittelt) und den Zweck und/oder die Mittel der Verarbeitung festsetzt. Verantwortlicher sind daher die selbständigen HumanenergetikerInnen, sonstige Beauftragte, BeraterInnen, BereitstellerInnen und InformantInnen, AstrologInnen, Farb- und TypberaterInnen, TierbetreuerInnen, -pensionen, -trainerInnen (und sonstige persönliche Dienstleister). Achtung: Werden die Daten nicht zu eigenen Zwecken verarbeitet, sondern zu einem von einem Verantwortlichen vorgegebenen Zweck (zB eine Druckerei adressiert eine Aussendung mit Adressdaten), ist man nicht	Art 4 DSGVO; Art 28 DSGVO

	Verantwortlicher, sondern Auftragsverarbeiter. Verantwortlicher und Auftragsverarbeiter haben künftig zwingend einen schriftlichen Vertrag über die Auftragsverarbeitung abzuschließen.	
Betroffenenrechte	„**Betroffenenrechte**" beschreiben die Rechte, die die betroffene Person (Kunden/Klienten) hinsichtlich ihrer personenbezogenen Daten hat. Die Rechte umfassen i) das Recht auf Auskunft, welche Daten wie und wofür verarbeitet werden; ii) das Recht auf Einschränkung der Verarbeitung; iii) das Recht auf Berichtigung der Daten; iv) das Recht auf Löschung; v) das Recht auf Datenportabilität, das heißt auf Übertragung aller Daten auf eine von der betroffenen Person bestimmte Person und vi) das Recht auf Widerspruch gegen die Verarbeitung ihrer Daten. Als persönlicher Dienstleister hat man diesen Pflichten zur Auskunft, Löschung von Daten etc nachzukommen, anderenfalls hohe Strafen drohen.	Art 15 - 21 DSGVO
THEMEN	**MAßNAHMEN**	**RECHTSGRUNDLAGEN**
DATENERHEBUNG		
Erhebung der personenbezogenen Daten *Wie erhalte ich personenbezogene Daten?*	▪ Erhalt von personenbezogenen Daten wie zB Name (Vor- und Nachname), Anschrift, E-Mail-Adresse, Geburtsdatum, weitere Geburtsdaten (Geburtsort, Geburtsstunde), Fotos, persönliche Widmungen, Konfektions- und Schuhgröße, Zahlungsdaten ▪ Übermitteln von Daten per E-Mail/Kontaktformular auf der Website ▪ Ausfüllen einer Einverständniserklärung und/oder eines Aufklärungsbogens ▪ Ausfüllen eines Kundenblattes/Formulars oder persönliches Gespräch mit den Klienten/Kunden/Interessenten und dadurch Erhalt der Daten	Art 5 DSGVO ; Art 6 DSGVO
Wie habe ich mit Daten umzugehen, die ich per E-Mail/Kontaktformular erhalte?	▪ Ablagesystem für die Daten entwickeln (Ordnersystem etablieren) ▪ Speicherung der Daten auf einem sicheren System - gesicherter Computer (Firewall, Virenschutz, Passwörter, etc) ▪ Nur die Personen, die für die Beratung/Behandlung/Betreuung Zugriff benötigen, dürfen Zugriff auf die Daten haben ▪ Bereits vor Abschluss eines Vertrages über die Beratung/Behandlung/Betreuung ist die Verarbeitung durch die Anfrage (Interesse des Kunden/Klienten an einer Beratung/Behandlung/Betreuung) gerechtfertigt, um zB ein Angebot zu erstellen ▪ Sichere Übermittlung des fertigen Ergebnisses an den Kunden (Achtung: Aufpassen bei Übermittlung per E-Mail, Verschlüsselung mitunter empfohlen – kommt auf die Daten an)	Art 5 DSGVO ; Art 6 DSGVO

Wie habe ich mit Daten auf Papier (zB Aufklärungsbogen/Kartei/Kundenblatt) umzugehen?	▪ Ablagesystem entwickeln - Aufbewahrung in einem versperrbaren Schrank (Aktenschrank) ▪ Nur die Personen, die für die Beratung/Behandlung/Betreuung Zugriff benötigen, dürfen Zugriff auf die Daten haben ▪ Bereits vor Abschluss eines Vertrages über die Beratung/Behandlung/Betreuung ist die Verarbeitung durch die Anfrage (Interesse des Kunden/Klienten an einer Beratung/Behandlung/Betreuung) gerechtfertigt, um zB ein Angebot zu erstellen	Art 5 DSGVO ; Art 6 DSGVO
Erhebung sensibler Daten	▪ Unterlagen über die Gesundheit (von Menschen): Befunde von Ärzten oder sonstigen Unterlagen, aus denen Informationen über den Gesundheitszustand der Klienten hervorgehen ▪ Unterlagen, aus denen die ethnische oder rassische Herkunft oder die Gewerkschaftszugehörigkeit hervorgehen ▪ Unterlagen, aus denen die Religionszugehörigkeit hervorgeht ▪ Achtung bei der Verarbeitung von sensiblen Daten – Einwilligungserklärung des Kunden einholen	Art 9 DSGVO
DATENVERWALTUNG		
Digitale Daten *Wie gehe ich mit personenbezogenen Daten um, die ich digital verwalte?*	▪ Entwicklung eines Ablagesystems - eigene Ordner am Computer erstellen ▪ Kontrolle, wer Zugriff auf die Daten hat (Zugriffskontrolle) ▪ Kontrolle, wer Zugriff auf den Computer / das Tablet / das Handy hat durch Codes und Passwörter ▪ Wird der Computer von mehreren Personen verwendet ist pro Person ein eigener Account zu erstellen, auf den nur diese Person zugreifen kann (Passwortschutz erforderlich)	Art 5 DSGVO ; Art 6 DSGVO ; Art 24 DSGVO ; Art 32 DSGVO
Papierakt / Karteien *Wie gehe ich mit Daten um, die ich in Papierform verwalte?*	▪ Entwicklung eines Ablagesystems für Papierakt / Kartei / Aufzeichnungen ▪ Aufbewahrung in einem versperrbaren Schrank (Aktenschrank) ▪ Schutz vor dem Zugriff durch andere Personen auf die Papierakten, Aufzeichnungen oder sonstige übermittelte Unterlagen ▪ Beaufsichtigung externer Personen (zu Hause) ▪ Sichere Verwahrung in einer uneinsichtigen Hülle, wenn man die Akten/Aufzeichnungen mit zum Kunden / Klienten mitnimmt ▪ Kunde/Klient darf die Daten der anderen Klienten/Kunden nicht sehen (Verwendung von Trennblättern, eigenen Ordnern, eigene Aktenmappe etc)	Art 5 DSGVO ; Art 6 DSGVO ; Art 24 DSGVO ; Art 32 DSGVO

Mobiltelefon *Worauf habe ich zu achten, wenn ich mein privates Mobiltelefon auch beruflich nutze?*	▪ Messenger Dienste (WhatsApp, Facebook Messenger, etc) und Applikationen die auf die Kontaktdaten zugreifen erfüllen oftmals nicht die datenschutzrechtlichen Anforderungen der DSGVO und sind stets im Einzelfall auf ihre Zulässigkeit zu prüfen ▪ Im Zweifel: zwei Mobiltelefone, eines für private Kontakte und eines für berufliche Kontakte ▪ Entwicklung insbesondere im Hinblick auf WhatsApp beobachten	Art 24 DSGVO ; Art 32 DSGVO
Home Office / Arbeiten in der Öffentlichkeit *Worauf habe ich zu achten, wenn ich von zu Hause arbeite oder in der Öffentlichkeit (zB in einem Park, Kaffeehaus)?*	▪ Gesicherte Laptops / Tablets / Handys (Firewall, Virenschutz, Updates, Passwort / Codegeschützt) ▪ Daten sollen nicht auf dem Desktop gespeichert werden ▪ Nicht auf fremden Computer / Tablet / Handy arbeiten und schon gar nicht Daten auf fremden Computer / Tablet / Handy speichern ▪ Keine fremden USB-Sticks/externe Festplatten verwenden, eigene USB-Sticks/externe Festplatten nicht verborgen ▪ Wird der Computer von mehreren Personen verwendet (zB zu Hause) ist pro Person unbedingt ein eigener Account zu erstellen, auf den nur diese Person zugreifen kann (Passwortschutz erforderlich) ▪ Nicht in öffentlichem WLAN arbeiten ▪ Daten nicht offen liegen lassen (zB Akten, Texte, Dokumente, Aufzeichnungen, etc) ▪ Bildschirm darf von Dritten nicht eingesehen werden können	Art 24 DSGVO ; Art 32 DSGVO
DATENVERARBEITUNG		
Wann darf ich Daten verarbeiten? *Worauf habe ich zu achten? Brauche ich eine Einwilligung?*	▪ Daten dürfen nur aufgrund eines Vertrages (und im Zuge der Vertragsanbahnung bei einem Interessenten), mit Einwilligung der betroffenen Person, bei einem berechtigten Interesse oder aufgrund einer gesetzlichen Verpflichtung (Gesetz, Standesregeln [7 Jahre Aufbewahrungspflicht für die Unterlagen der Klienten]) verarbeitet werden ▪ Ob ein berechtigtes Interesse vorliegt oder eine Einwilligung notwendig ist, ist im Einzelfall zu klären - berechtigtes Interesse liegt immer dann vor, wenn das Recht an der Geheimhaltung/Nichtverarbeitung der Daten der betroffenen Person das Interesse des Unternehmers an der Datenverarbeitung nicht überwiegt (Interessenabwägung im Einzelfall!) ▪ Wenn es einen Vertrag über die Beratung/ energetische Behandlung mit dem Kunden/Klienten gibt, erfolgt eine Verarbeitung im Rahmen des Vertrages mit dem Kunden/Klienten ▪ Soll die Verarbeitung der personenbezogenen Daten für einen Zweck, der über die Erfüllung des Vertrages hinausgeht (zB Versenden von Newsletter und Werbung), erfolgen, muss eine Einwilligung eingeholt werden, solange keine gesetzliche Verpflichtung oder ein berechtigtes Interesse vorliegt	Art 6 DSGVO; ErwGr 47 DSGVO

	▪ Verarbeitung immer nur für einen bestimmten Zweck – der Zweck muss der betroffenen Person gegenüber klar sein oder offengelegt werden ▪ Eine Verarbeitung der personenbezogenen Daten eines Interessenten (der eine Anfrage geschickt hat), ist gerechtfertigt (Anbahnung eines Vertragsverhältnisses durch den Interessenten). Kommt die Beratung/energetische Behandlung/ Betreuung nicht zustande, sind die Daten zu löschen oder es muss eine Einwilligungserklärung eingeholt werden ▪ Anfragen dürfen jedoch noch eine gewisse Zeit gespeichert werden (Empfehlung: bis zu 3 Monaten)	
Wann hat eine Information der betroffenen Person zu erfolgen?	▪ Betroffene Personen müssen bei Erhebung ihrer Daten, über eine Erhebung der Daten und über die anschließende Verarbeitung informiert werden (zB im Aufklärungsbogen der Humanenergetiker). Hat man eine Website, erfolgt diese Information auch durch die Datenschutzerklärung (siehe unten: Website). ▪ Die Information muss der betroffenen Person verständlich sein, das heißt auch in einer Sprache, die die betroffene Person versteht ▪ Die Information enthält Angaben über: den Verantwortlichen (Firma des persönlichen Dienstleisters), Zwecke der Verarbeitung (Beratung/Behandlung/Betreuung), Dauer der Datenspeicherung, Hinweis auf die Rechte der betroffenen Person (Kunden hat Recht auf Auskunft, Löschung, Widerruf einer Einwilligung etc), Recht auf Beschwerde bei der Datenschutzbehörde, Grund der Verarbeitung (zB Beratung/Behandlung/Betreuung)	Art 12 DSGVO ; Art 13 DSGVO; Art 14 DSGVO
Muss ich alle Daten nach einer gewissen Zeit löschen?	▪ Die Löschung ist nur notwendig, wenn kein Grund (gesetzliche Aufbewahrungsfrist, Vertragsverhältnis über die Beratung/Behandlung/Betreuung etc) mehr besteht, die Daten zu behalten ▪ Hat das Vertragsverhältnis bereits vor langer Zeit geendet und sind keine weiteren Anfragen mehr erfolgt, sind die Daten zu löschen oder es ist eine Einwilligung einzuholen, um die Daten weiterhin zu speichern	Art 17 DSGVO
Wie muss eine Einwilligungserklärung aussehen?	▪ Hinweis, von wem die Daten verarbeitet werden (Verantwortlicher – Name/Firma des persönlichen Dienstleisters) ▪ Hinweis, welche Datenarten verarbeitet werden (zB Gesundheitsdaten, Name, Anschrift usw.) ▪ Hinweis, für welchen Zweck (Beratung/Behandlung/Betreuung) die Daten verarbeitet werden ▪ Hinweis, dass und wie die Einwilligung jederzeit widerrufen werden kann	Art 6 DSGVO ; Art 7 DSGVO ; Art 13 DSGVO
Rechte der betroffenen Personen *Worauf habe ich zu achten? Wie habe ich die Rechte der betroffenen Personen intern umzusetzen?*	▪ Internes System entwickeln, wie die Betroffenenrechte (zB Recht auf Auskunft, Löschung, etc) gewahrt werden können. Die Daten müssen gefunden werden können! (Suchfunktion, Volltextsuche, etc) ▪ Internes System entwickeln, wie den betroffenen Personen das Recht auf Auskunft gewährt wird ▪ Internes System entwickeln, um Daten zu berichtigen ▪ Internes System entwickeln, um Daten zu löschen	Art 15 bis 20 DSGVO

	▪ Internes System entwickeln, wie die Daten auf eine andere Person übertragen werden können ▪ Mitteilung an alle externen Dienstleister, denen die Daten offengelegt wurden, dass eine Löschung oder eine Änderung der Daten erfolgt ist	
Akten vor der DSGVO *Wie gehe ich mit Akten um, die vor Anwendbarkeit der DSGVO angelegt wurden?*	▪ Wenn gesetzliche Aufbewahrungsfrist vorliegt ist die Aufbewahrung in Ordnung ▪ Darüber hinaus: grundsätzlich Einholung einer Einwilligungserklärung ▪ Minimierung der gespeicherten Daten auf die von der Aufbewahrungspflicht umfassten ▪ Rest: Löschen ▪ Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dürfen Daten jedoch aufgehoben und müssen nicht gelöscht werden	Art 5 DSGVO ; Art 6 DSGVO ; Art 17 DSGVO
SONSTIGES		
Newsletter *Worauf habe ich beim Versand von Newslettern zu achten?*	▪ Einwilligung der betroffenen Person einholen ▪ Möglichkeit des Widerrufs der Einwilligung im Newsletter ▪ Versand an Stammkunden kann unter das berechtigte Interesse des Unternehmens fallen (langjährige Kundenbeziehung) ▪ Wenn der Kunde seine E-Mailadresse freiwillig angibt und er darauf hingewiesen wird, dass unter anderem auch Newsletter verschickt werden, kann dies als Einwilligung gesehen werden - Nachweispflicht!	Art 6 DSGVO
Website *Worauf ist bei der Erhebung von Daten auf einer Website zu achten (Social Media PlugIns, Cookies, Tracking)?*	▪ Erstellen einer Datenschutzerklärung ▪ Aufklärung der Nutzer über die verwendeten Cookies und welche Daten durch diese erhoben werden und Einholung einer Einwilligung ▪ Aufklärung der Nutzer über verwendete Social Media PlugIns ▪ Aufklärung der Nutzer, welche Daten wie und ab wann erhoben und gespeichert werden	§ 96 TKG 2003
Brief an Kunden (Direct Mailing per Post)	▪ Direct Mailing (per Post) kann bei Kunden zu Marketingzwecken durch das berechtigte Interesse an der Datenverarbeitung gerechtfertigt sein ▪ Hinweis auf Abmeldung von der Mailing Liste bzw. auf die Möglichkeit des Widerrufs der Einwilligung	§ 6 DSGVO ; ErwGr 47 DSGVO

ROADMAP DSGVO

STRAFEN		
Verstoß gegen allgemeine Pflichten der DSGVO	▪ Strafen bis zu EUR 10.000.000 oder ▪ 2 % des weltweiten (Konzern-) Jahresumsatzes des vorangegangen Jahres	Art 83 DSGVO
Verstoß gegen die Grundsätze der Datenverarbeitung, die Einwilligung und die Betroffenenrechte	▪ Strafen bis zu EUR 20.000.000 oder ▪ 4 % des weltweiten (Konzern-) Jahresumsatzes des vorangegangenen Jahres	Art 83 DSGVO
Wer haftet bei einem Verstoß gegen die DSGVO? *Hafte ich für einen Verstoß gegen die DSGVO, den ein Dienstnehmer von mir begeht oder der durch einen von mir bestellten Auftragsverarbeiter geschieht?*	▪ Der Geschädigte kann sich aussuchen, ob er Ersatz von dem Verantwortlichen oder von dem Auftragsverarbeiter verlangt (sie haften gemeinsam im Außenverhältnis) ▪ Sollte der Geschädigte den Verantwortlichen in Anspruch nehmen, obwohl ihn keine Schuld trifft und er alle Vorgaben der DSGVO und von anderen nationalen Datenschutzgesetzen eingehalten hat, kann der Verantwortliche wiederum Ersatz von dem Auftragsverarbeiter verlangen	Art 82 DSGVO
ALLGEMEIN		
Auftragsverarbeitung *Worauf habe ich bei einer Auftragsverarbeitung zu achten?*	▪ Abschluss eines Auftragsverarbeitungsvertrags ▪ Sorgfältige Auswahl des Dritten – Solidarhaftung!	Art 28 DSGVO
Datenschutzerklärung *Welchen Mindestinhalt hat eine Datenschutzerklärung zu enthalten?*	▪ Aufklärung der Nutzer über die verwendeten Cookies und welche Daten durch diese erhoben werden ▪ Aufklärung der Nutzer über verwendete Social Media PlugIns ▪ Information über Retargeting Maßnahmen ▪ Information über verwendete Tools wie Google AdWords oder Google Analytics ▪ Aufklärung der Nutzer, welche Daten wie und ab wann erhoben werden ▪ Informationen über die Rechte der Betroffenen ▪ Information über Beschwerderecht bei der Datenschutzbehörde	Art 13 DSGVO

MUSTER EINWILLIGUNGSERKLÄRUNGEN		
Muster Einwilligungserklärung *Einwilligung für zB Aufklärungsbogen zur Weiterverarbeitung der Kundendaten zu Marketingzwecken*	"Ich, [Name], willige ein, dass meine personenbezogenen Daten, welche im Rahmen der Beratung/Behandlung/Betreuung erhoben wurden, [Einfügen der Datenarten, z.B.: Name, Adresse, Geburtsdatum] zum Zweck [Zweck einfügen, z.B. Versand von Newslettern, Geburtstagsglückwünsche, Eventeinladungen, usw. Achtung: "Marketingzwecke" oder "Werbung" ist zu ungenau und darf deshalb nicht verwendet werden] von [persönlicher Dienstleister] verarbeitet werden. Ich kann meine Einwilligung jederzeit per Mail an [E-Mail-Adresse] oder schriftlich an [Adresse] widerrufen."	Art 6 DSGVO