basstrid
Webdesign & Coaching

WIRSIND

DSGVO mit Hausverstand

Praktische Beispiele und Tipps für EPU‘s

basstrid
Webdesign & Coaching

Was ist die DSGVO?

- „DatenSchutzGrundVerOrdnung“
- seit 2018 in der gesamten EU verpflichtend
- gilt für alle Unternehmen
- gilt für **Daten, die Menschen betreffen** („personenbezogen“)
- Daten, die auffindbar sind („strukturiert“)

Betrifft also auch die Papierablage!

basstrid
Webdesign & Coaching

Tipp vom Hausverstand:

Je höher das **Risiko**
(=Schaden im Verlustfall),
desto umfangreicher müssen die
Maßnahmen sein!

basstrid
Webdesign & Coaching

Was brauchst du?

1. Verarbeitungsverzeichnis
   = DSGVO Dokumentation

   → Selber machen mit Vorlage

2. Datenschutzerklärung
   für deine Webseite UND für dein Unternehmen

   → Vorlagen verwenden

3. Einwilligungserklärungen
   z.B. Newsletter-Versand

   → Newsletter: wird automatisch erfasst
   Sonstige: Abspeichern!

4. Verträge mit Auftragsverarbeitern
   das sind Dienstleister, die für dich Kundendaten verarbeiten
   z.B. Newslettersoftware, Webseite

   → Vorlage vom Partner verwenden

5. DSGVO-konforme Webseite
   weil die Webseite am leichtesten überprüfbar ist

   → Selber machen oder Webdesigner fragen

basstrid
Webdesign & Coaching

Wer darf Einsicht verlangen ?

- Ein **Kunde** darf nur Auskunft über die eigenen Daten verlangen.
- In Österreich darf NUR die **Datenschutzbehörde** Einsicht in deine DSGVO-Unterlagen verlangen!

basstrid
Webdesign & Coaching

Ablauf einer Anfrage der DSB

1. DS-Behörde verlangt Einsicht (Grund: Anzeige, o.ä.)
2. Verarbeitungsverzeichnis & Dokumentation schicken
3. Nachfrage / Nachbesserungsauftrag seitens der Behörde
4. (Geld-)Strafen werden erst danach ausgesprochen

basstrid
Webdesign & Coaching

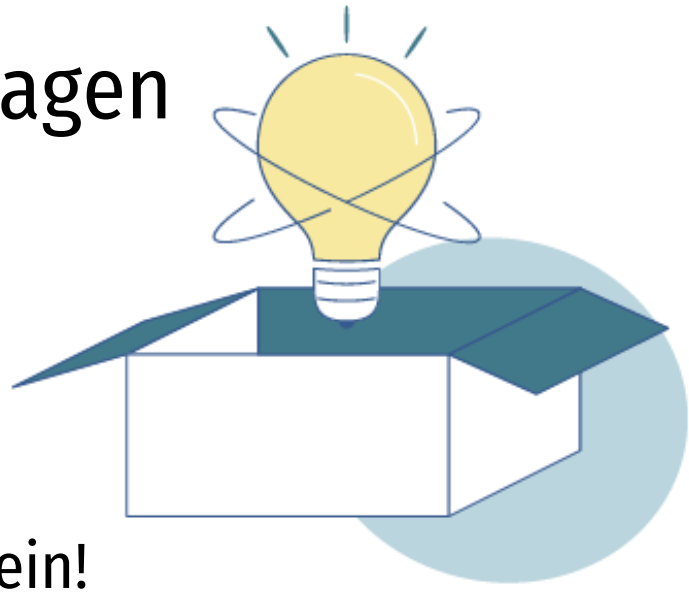
Tipp vom Hausverstand:

Bereite das **Verarbeitungsverzeichnis** zumindest rudimentär vor, damit du es bei einer Anfrage der DS-Behörde nur mehr **aktualisieren** musst!

basstrid
Webdesign & Coaching

Tipp vom Hausverstand:

Lege alle DSGVO-relevanten Unterlagen an **EINEM Ort** ab, um alles im Bedarfsfall griffbereit zu haben.



Das kann ein digitaler oder physischer Ordner sein!

basstrid
Webdesign & Coaching

Verarbeitungsverzeichnis

= Dokumentation deiner **personenbezogenen** Datenverarbeitungen

Muss Antworten auf folgende Fragen geben:

- **Welche Daten hast du?**
  z.B. Rechnungen, Kundendaten (Kontaktdaten, Projektbezogene Daten, etc.)

- **Was machst du mit den Daten?**
  Wo speicherst du sie?
  An wen gibst du sie weiter?
  Wie lange hebst du sie auf?
  Was tust du, um die Daten zu schützen?
  = Technisch-organisatorische Maßnahmen

basstrid
Webdesign & Coaching

Tipp vom Hausverstand:

Verwende dafür eine **Vorlage**.

Hier findest du eine kostenlose Vorlage für EPU‘s:

https://basstrid.at/wir-sind-1/

basstrid
Webdesign & Coaching

Technisch-organisatorische Maßnahmen

...müssen im Verarbeitungsverzeichnis enthalten sein und
Antworten auf folgende Frage geben:

Was tust du um deine Daten zu schützen?

Für den Datenschutz sind immer

MENSCH & MASCHINE

verantwortlich!

basstrid
Webdesign & Coaching

Ideen mit Hausverstand:

- Strikte **Trennung** von Privat und Beruf –
  am besten mit eigenen Geräten/eigenen Benutzern!
- **Versperrter Schrank**/Raum für Firmenunterlagen mit
  personenbezogenen Daten, z.B. Buchhaltung
- Mobile Geräte mit Code/biometrisch **sperren**
- Laptop verschlüsseln (ist im Windows möglich)
- **KEINE USB Sticks** mit personenbezogenen Daten herumtragen
- Technische Geräte regelmäßig **UPDATEN** um Sicherheitslücken zu schließen

basstrid
Webdesign & Coaching

Achtung auf die Weitergabe von Daten

- Rechnungslegungsdaten (Steuerberatungskanzlei)
- Verwendung von **Cloudspeichern** (Dropbox, OneDrive, etc.)
- Verwendung von **Software**, die Daten in der Cloud speichert
  - Buchhaltungssoftware, etc.
- Verwendung von **Online-Diensten**, z.B.
  - Newsletter-Software
  - Webseite
  - Webmail

Achtung: Datenweitergabe ins EU-Ausland nicht gestattet! (vereinfacht)

basstrid
Webdesign & Coaching

Tipp vom Hausverstand:

Verwende

- KEINE **kostenlosen** Services (Dropbox, etc.)
- Software die auf **Server in Europa läuft**

basstrid
Webdesign & Coaching

Deine Webseite...

...ist **öffentlich einsehbar** und macht dich angreifbar

Deine **Datenschutzerklärung** gibt den ersten Hinweis darauf, wie du mit dem Thema umgehst:

Hast du einfach **Textvorlagen** irgendwo rauskopiert, die gar nichts mit deiner Webseite zu tun haben?

z.B. Hinweise auf nicht eingebundene Social-Media-Plattformen, Newsletter, Shop, etc.

basstrid
Webdesign & Coaching

Cookies auf deiner Webseite

DSGVO-konforme Gestaltung

- Keine Datenübertragungen
- Keine Tracking-Cookies

= Kein Cookie-Banner nötig

mit Tracking & Datenübertragung

- Wenn Marketing- & Tracking-Cookies benötigt werden

= Cookie-Banner nötig, der NUR bei Zustimmung die Cookies lädt

basstrid
Webdesign & Coaching

DSGVO-konforme Webseite

Achte u.a. auf:

- **Google Fonts**

  sollen von deiner Webseite und nicht von Google geladen werden

- **Google Maps**

  Vermeide die Einbindung!

  ↪ **Besser**: Button mit Link zum Routenplaner!

- **Youtube Videos**

  Können in WordPress mit dem Plugin „Youtube Lyte“ DSGVO konform eingebunden werden

basstrid
Webdesign & Coaching

DSGVO-konforme Webseite

- Verwende **keine Tracking-Codes**

  z.B. von Facebook, Google, etc.

- **Vermeide Google Analytics**

  Vermeide die Einbindung

  Hoher Aufwand für DSGVO konforme Einbindung!

  ↪ Diese vielen Daten werden üblicherweise nicht benötigt/verwendet.

  Besser: Statistik-Plugins oder Matomo (vergleichbar mit GA) = kostenlos!

basstrid
Webdesign & Coaching

Tipps für die Datenschutzerklärung

Achte darauf, dass **alle verwendeten Plugins** & Erweiterungen deiner Webseite **in der Datenschutzerklärung** angeführt sind!

Für WordPress-Webseiten:

Übersicht über viele Plugins und deren Datenverarbeitung:

https://www.gradually.ai/wordpress-plugins-dsgvo/

basstrid
Webdesign & Coaching

Tipps für die Datenschutzerklärung

- Kostenlose Textvorlagen gibt es hier:

  https://opr.vc/

- Muster für DS-Erklärung:
  https://opr.vc/docs/allgemein/dse_einleitung/

basstrid
Webdesign & Coaching

basstrid
Webdesign & Coaching

Nicht vergessen:

- Du brauchst einen **Auftragsverarbeiter-Vertrag** mit deinem Web-Hosting-Unternehmen. Verwende deren Vorlage!
- Bei allen **Kontaktformularen** sollte ein Hinweis auf die Datenschutzerklärung zu finden sein:

  ☐ „Ich bin damit einverstanden, dass meine Daten elektronisch verarbeitet werden. Zur Datenschutzerklärung“

basstrid
Webdesign & Coaching

Newsletter / E-Mail-Marketing

Der Versand von E-Mails ist erlaubt an:

- aktive Kunden
- Interessenten, die eingewilligt haben

Auch die Eintragung in eine physische Liste ist eine Einwilligung!

- Reduziere die erfassten Daten auf das Minimum (Mailadresse, Name)
- **Füge in jedes Mail ein Impressum und die Möglichkeit sich abzumelden ein!**

basstrid
Webdesign & Coaching

Achtung: Heikle Themen

Es gibt ein paar Themen, bei denen du mehr dem **Gesetz** als dem Hausverstand folgen solltest:

- Bei **gesundheitsbezogenen** Daten oder sonstigen „**sensiblen**“ Daten wie Religion: Hier brauchst du eine Einwilligung ODER eine gesetzliche Grundlage
- **Videoüberwachung** am Gelände
- Angebote an **Kinder unter 14 Jahren**
- **Profiling**

basstrid
Webdesign & Coaching

Tipp vom Hausverstand:

- Keine Panik: Das Thema ist auch für DICH zu schaffen!
- Kein Perfektionismus: „Gut“ ist „gut genug“
- Prioritäten setzen:
  1. **Webseite** überprüfen und DSGVO konform machen
  2. **Verarbeitungsverzeichnis** (Vorlage) ausfüllen

Viel Erfolg!

Kontakt

Mag. Astrid Brückner

home@basstrid.at

Kostenlose Downloads:

https://basstrid.at/wir-sind-1/

basstrid
Webdesign & Coaching

Meine Services

- Webdesign mit WordPress
- WordPress-Coaching
- Datenschutzberatung
- SEO-Optimierung
- Newsletter-Marketing
- Update-Service für WordPress

basstrid
Webdesign & Coaching

basstrid
Webdesign & Coaching

DANKE

für eure Aufmerksamkeit!