Zu Beginn zwei gängige Mißverständnisse aufgeklärt:

1. Keine wko/WIFI-Stelle, Logo von der Zertifizierungsstelle vorgegeben;
2. Kein Datenschützer – Aufgabe vielmehr Kunden vor Betroffenen, der Behörde und Datenschützern zu schützen.

Warum ein externer Datenschutzbeauftragter?

Verpflichtete Bestellung nach Art 37 (1) a DSGVO für öffentliche Stellen;

Vermeidung Interessenskonflikt (Art 38 (6) DSGVO), d.h.

kein Angehöriger der Gemeindeleitung (Bgm, AL, etc)

insbesondere keine Leiter und/oder Mitarbeiter der IT

keine Angehörige des Betriebsrates / der Personalvertretung

Vorsicht auch bei allfälligen Nebentätigkeiten eines internen Datenschutzbeauftragten!

Nicht vergessen die Bestellung des Datenschutzbeauftragten an die Datenschutzbehörde zu melden! (Art 37 (7) DSGVO)

- Öffentlichkeitsarbeit: Gemeindezeitung
  Internetauftritt
- Rechtskonforme Kommunikation in der Gemeinde
- Gemeinderat / politische Parteien / Personalvertretung
- Potentielle Bedrohungsquellen / Haftungsfragen

Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
WIFI WKO
VALID: 07/2021

Die Themen des heutigen Workshop überschneiden sich.

Mein Fokus liegt auf der Wirtschaft, insbesondere Handelsunternehmen,
die Spezialisten der öffentlichen Verwaltung sitzen im Publikum!

Bitte jederzeit unterbrechen, Fragen, Ergänzungen und vor allem Widerspruch sind willkommen!

Erstes Beispiel – die Gemeindezeitung von Hart bei Graz / Steiermark, Oktober 2018;

Überzeichnet „hysterische" Auslegung der DSGVO;

Gut geregelt in Tirol:

§ 3(2) Tiroler Ehrungsgesetz > Informationspflicht

+

§ 3 (1) Tiroler Ehrungsgesetz > Widerspruchsrecht

=

Art 6 (1) a DSGVO > Einwilligung

Tipp: Schriftlich geben lassen und zumindests sechs Monate aufbewahren und Betroffene darauf hinweisen!

Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
WIFI WKO
VALID: 07/2021

Zweites Beispiel aus dem Burgenland: Bgm mit Stellungspflichtigen (voller Name und Tauglichkeitsstatus) in Lokalmedien und Internet.

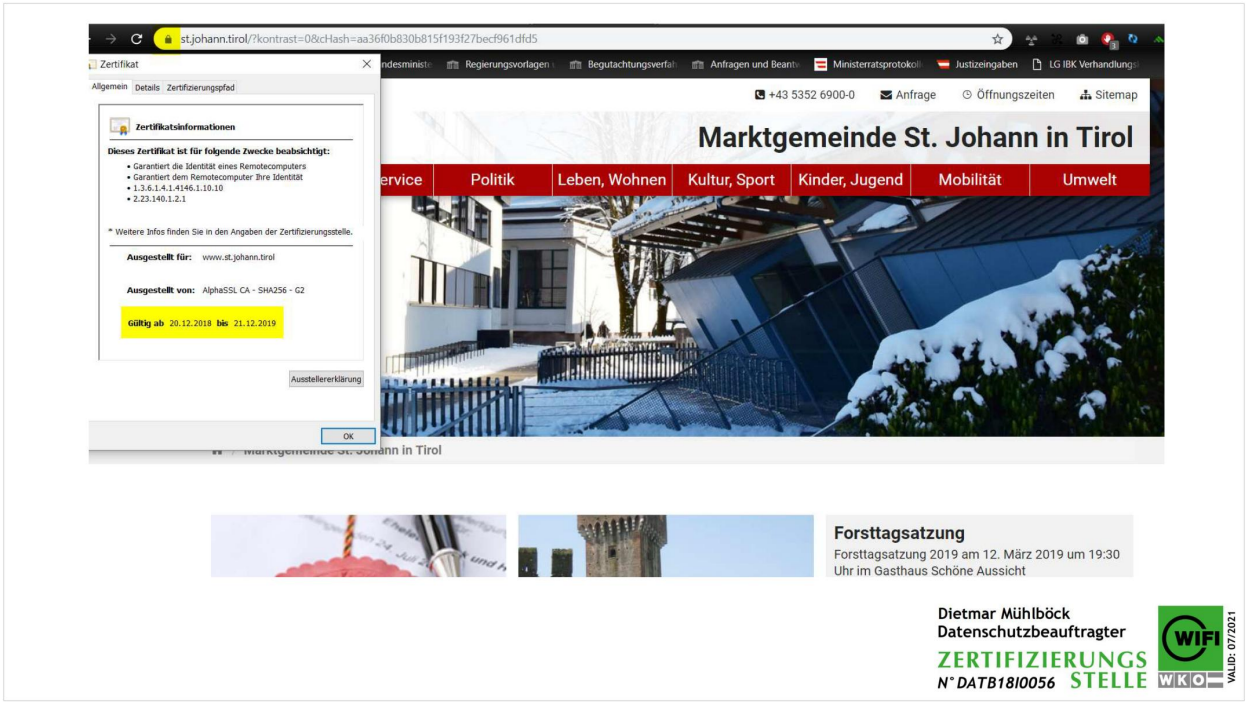
Probleme:

Woher kommen die Daten? (Laut Bgdl Gemeinden aus dem ZMR)

Liegen Einwilligungen nach 6 (1) a DSGVO vor?

Achtung: Tauglich bzw Untauglich = sensible Daten nach Art 4 Pkt 15 DSGVO!

Fraglich, ob die Stellung ein besonderer Anlass iSd Tiroler Ehrungsgesetzes ist!



Weiter zum Internetauftritt der Gemeinde.

Die Marktgemeinde St. Johann in Tirol hat sich „freiwillig“ gemeldet – vielen Dank ;-)

Darauf achten, dass die Seite verschlüsselt übertragen wird und das Sicherheitszertifikat gültig ist. - Ihr Webmaster hat das notwendige Fachwissen dazu!

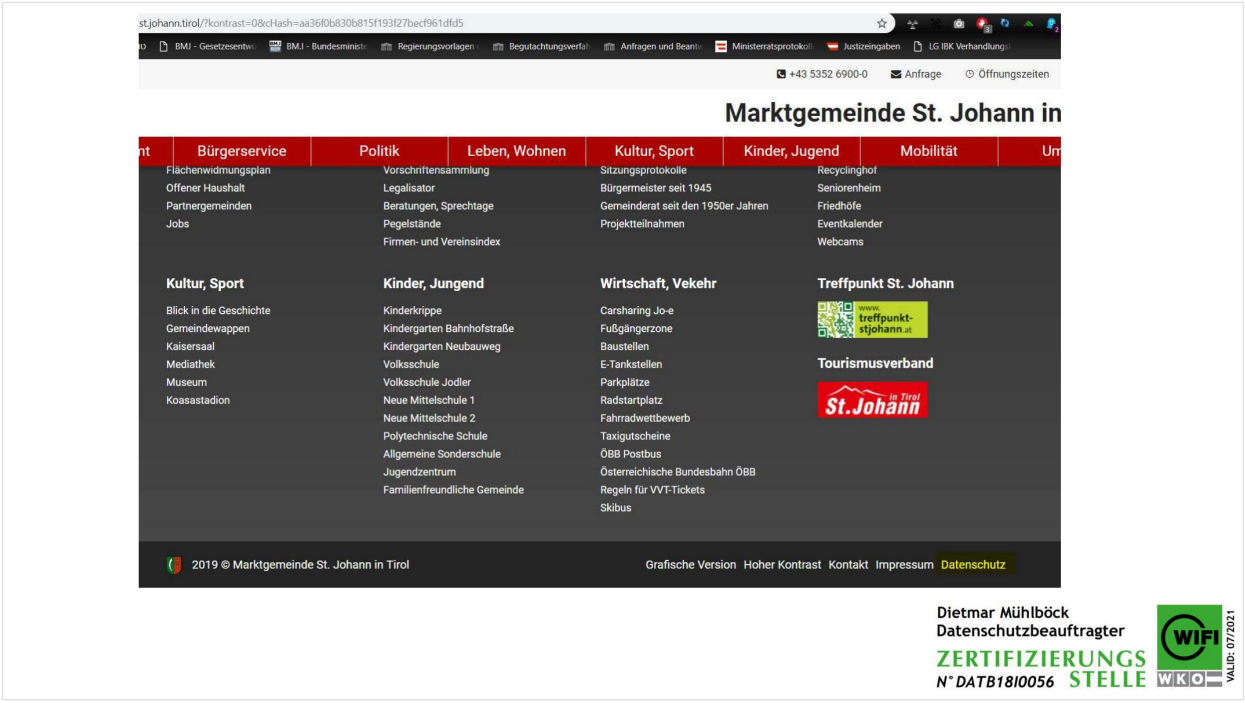
Haben Sie einen Auftragsdatenverarbeitungsvertrag mit Ihrem Webspace-Anbieter?

Wenn Sie die Möglichkeit haben, nutzen Sie das Angebot von *.tirol.gv.at!

Wenn Sie einen privaten Anbieter beauftragen, dann beauftragen Sie einen heimischen.

Der Zusammenschluß der österreichischen Anbieter – ISPA – hat für seine Mitglieder eine Datenschutzrichtlinie erstellt und veröffentlicht hier eine Liste der teilnehmenden Unternehmen: https://www.ispa.at/wissenspool/datenschutz.html

Bei ausländischen Anbietern sollten diese in der EU ihren Sitz haben; zur Sicherheit auf England jetzt schon verzichten (BREXIT)!



Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
WIFI WKO
VALID: 07/2021

Der Link zu Datenschutzerklärung muss leicht erreichbar sein, wie das Impressum.

Verwenden Sie einen „sprechenden Link“!

Gut: gemeinde.tirol.gv.at/datenschutz

Schlecht: gemeinde.tirol.gv.at/source=hp&ei=i9cDXJPWEaOVmgXtpL_Qbw&q=

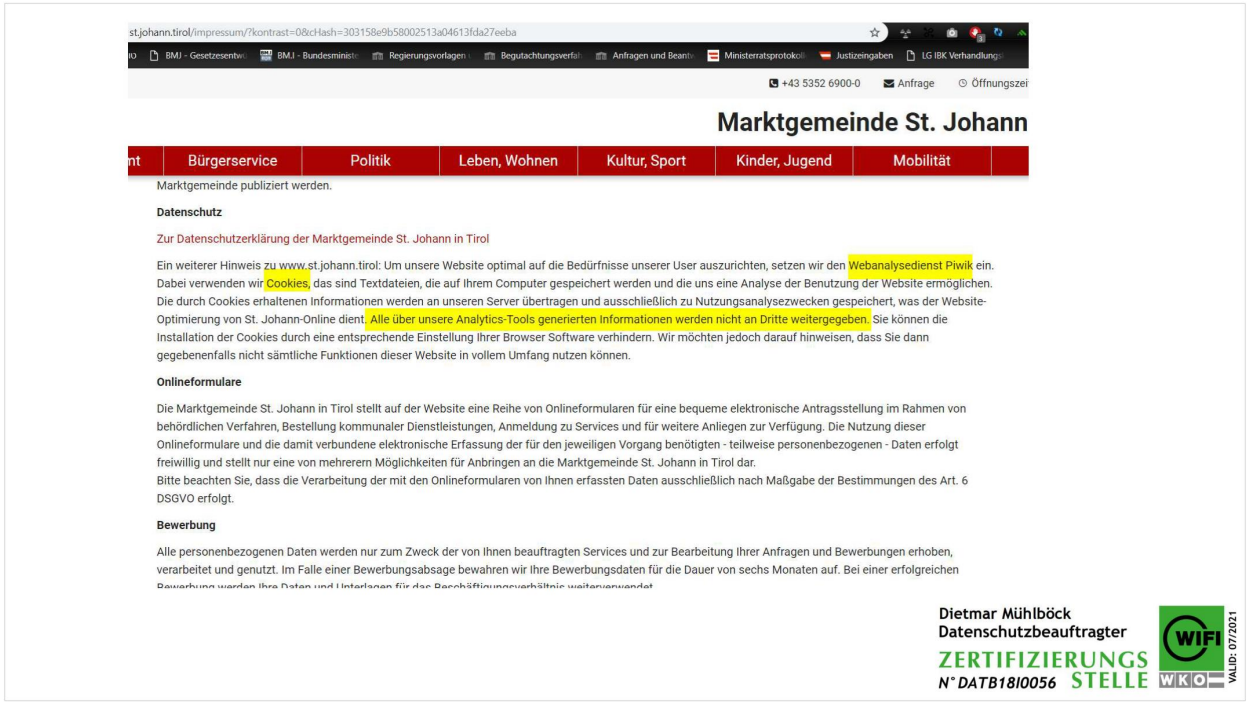
Achten Sie darauf, dass mit dem Link auch wirklich die Datenschutzerklärung zum Internetauftritt erreichbar ist!

Im Beispiel war die allgemeine Datenschutzerklärung verlinkt, darin ist kein Bezug zum Internetauftritt, diese war im Impressum „versteckt“.

Grundsätzlich zur Datenschutzerklärung (und alles, was sich an Betroffene richtet):

Einfach und klar verständlich formulieren, keine juristische Schachtelsätze!

Wenn Ihre Webseite mehrsprachig angeboten wird, Bsp Fremden-verkehrsort DE/EN/NL…, dann muss auch die Datenschutzerklärung in den verwendeten Sprachen angeboten werden!



st.johann.tirol/impressum/?kontrast=0&cHash=303158e9b58002513a04613fda27eeba

BMJ - Gesetzesentw... BMJ - Bundesministe... Regierungsvorlagen ... Begutachtungsverfah... Anfragen und Beant... Ministerratsprotokoll... Justizeingaben LG IBK Verhandlungs...

+43 5352 6900-0 Anfrage Öffnungszei

Marktgemeinde St. Johann

nt | Bürgerservice | Politik | Leben, Wohnen | Kultur, Sport | Kinder, Jugend | Mobilität

Marktgemeinde publiziert werden.

Datenschutz

Zur Datenschutzerklärung der Marktgemeinde St. Johann in Tirol

Ein weiterer Hinweis zu www.st.johann.tirol: Um unsere Website optimal auf die Bedürfnisse unserer User auszurichten, setzen wir den Webanalysedienst Piwik ein. Dabei verwenden wir Cookies, das sind Textdateien, die auf Ihrem Computer gespeichert werden und die uns eine Analyse der Benutzung der Website ermöglichen. Die durch Cookies erhaltenen Informationen werden an unseren Server übertragen und ausschließlich zu Nutzungsanalysezwecken gespeichert, was der Website-Optimierung von St. Johann-Online dient. Alle über unsere Analytics-Tools generierten Informationen werden nicht an Dritte weitergegeben. Sie können die Installation der Cookies durch eine entsprechende Einstellung Ihrer Browser Software verhindern. Wir möchten jedoch darauf hinweisen, dass Sie dann gegebenenfalls nicht sämtliche Funktionen dieser Website in vollem Umfang nutzen können.

Onlineformulare

Die Marktgemeinde St. Johann in Tirol stellt auf der Website eine Reihe von Onlineformularen für eine bequeme elektronische Antragsstellung im Rahmen von behördlichen Verfahren, Bestellung kommunaler Dienstleistungen, Anmeldung zu Services und für weitere Anliegen zur Verfügung. Die Nutzung dieser Onlineformulare und die damit verbundene elektronische Erfassung der für den jeweiligen Vorgang benötigten - teilweise personenbezogenen - Daten erfolgt freiwillig und stellt nur eine von mehrerern Möglichkeiten für Anbringen an die Marktgemeinde St. Johann in Tirol dar.
Bitte beachten Sie, dass die Verarbeitung der mit den Onlineformularen von Ihnen erfassten Daten ausschließlich nach Maßgabe der Bestimmungen des Art. 6 DSGVO erfolgt.

Bewerbung

Alle personenbezogenen Daten werden nur zum Zweck der von Ihnen beauftragten Services und zur Bearbeitung Ihrer Anfragen und Bewerbungen erhoben, verarbeitet und genutzt. Im Falle einer Bewerbungsabsage bewahren wir Ihre Bewerbungsdaten für die Dauer von sechs Monaten auf. Bei einer erfolgreichen Bewerbung werden Ihre Daten und Unterlagen für das Beschäftigungsverhältnis weiterverwendet

Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
WIFI WKO
VALID: 07/2021

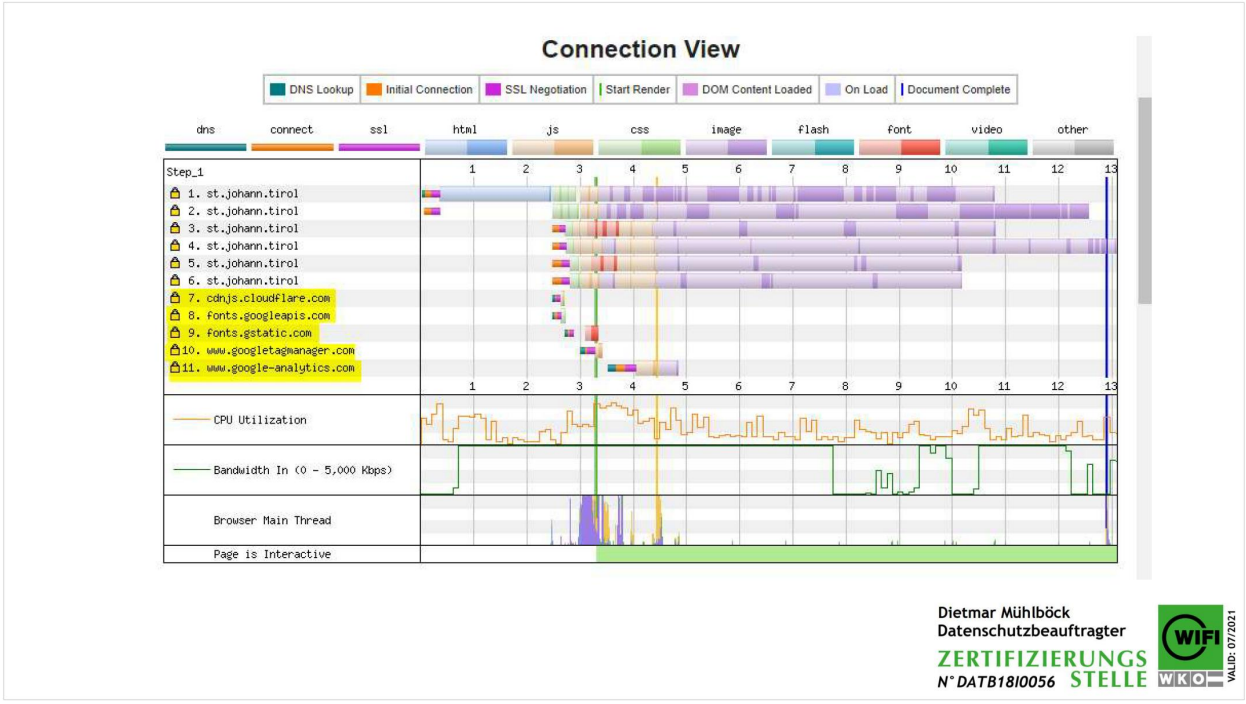
Hier nun die Datenschutzerklärung zum Internetauftritt.

Die Angaben müssen korrekt sein!

Im Beispiel: PIWIK gibt es seit Jänner 2018 nicht mehr.

Cookies beschreiben! Name, wo wird es verarbeitet, was tut es, Ablauf.
Beispiel:

Name	Anbieter	Zweck	Ablauf	Typ
Notwendige Cookies Notwendige Cookies helfen dabei, eine Webseite nutzbar zu machen, indem sie Grundfunktionen wie Seitennavigation und Zugriff auf sichere Bereiche der Webseite ermöglichen. Die Webseite kann ohne diese Cookies nicht richtig funktionieren.				
BIGipServer# (2x)	204-bha-091.mktoresp.com app-lon06.marketo.com	Verwendet, um Verkehr auf der Website auf mehreren Servern zu verteilen, um die Antwortzeiten zu optimieren.	Session	HTTP
PHPSESSID	seeburger.jobbase.io	Prescreen Cookie zur Erfassung von Benutzern von Bewerbungsformularen.	Session	HTTPS



Auf der vorherigen Folie ist angemerkt, dass keine Daten der Benutzer (= Betroffene iSd DSGVO) an Dritte weitergegeben werden.

Eine technische Analyse der Seite zeigt, dass das nicht zutrifft – und da wird die Datenschutzbehörde grantig. Richtig grantig… ;-)

Der Internetauftritt im Beispiel übertragt Daten an Cloudflare und Google.

Das muss in der Datenschutzerklärung angeführt sein!

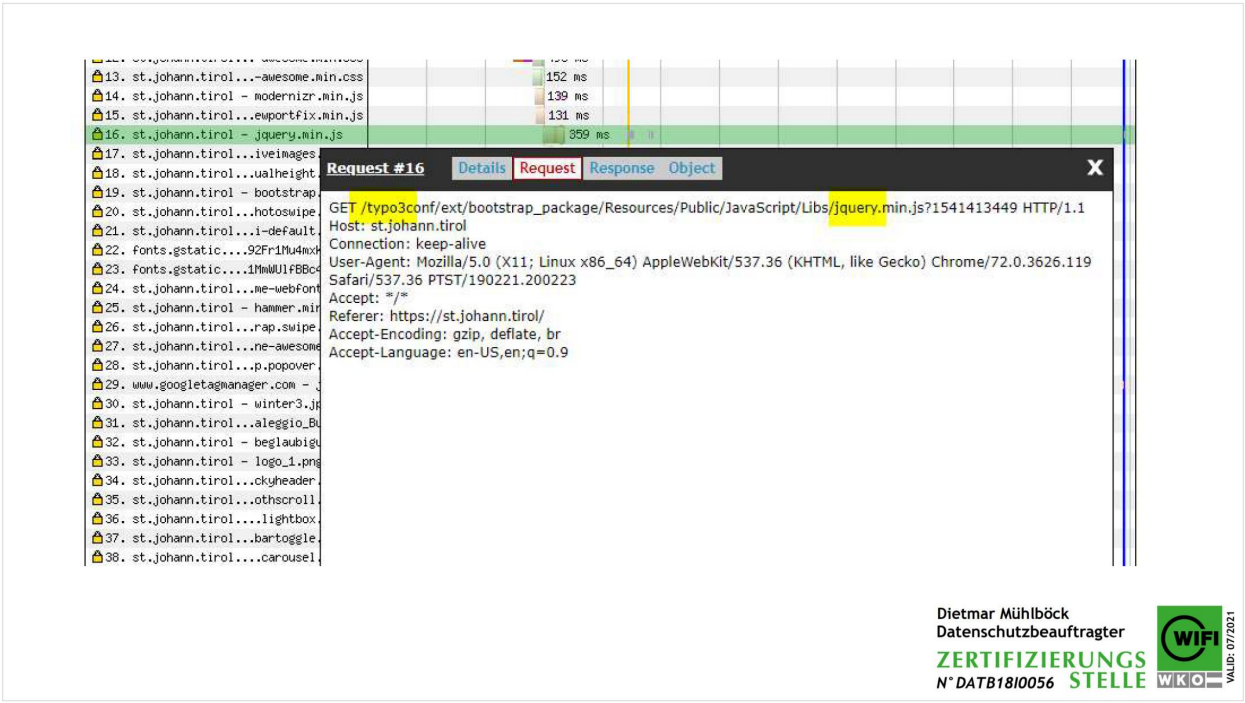
Schließen Sie einen Auftragsdatenverarbeitungsvertrag mit den jeweiligen Verarbeitern!

Wenn Sie Statistiken führen, dann anonymisieren Sie die IP-Adressen der Benutzer – Ihr Webmaster hat das notwendige Fachwissen dazu.

Wenn Sie dese Statistiken archivieren, dann müssen Sie auch bei Anfragen beauskunftet werden, insbesondere bei fixer IP des Benutzers!

Sidekick: § 7 Tiroler Datenverarbeitungsgesetz hinterfragenswert, ebenso wie das gesamte Gesetz! Stichwort Verfassungsnovelle zum Jänner 2020!

Testen Sie Ihren Internetauftritt unter: webpagetest.org



Wenn Sie ein CMS (Content Management System – Inhaltsverwaltungssystem) – im Beispiel typo3 - verwenden, dann achten Sie darauf, dass es am neuesten Stand ist und alle Updates, insbesondere Sicherheitsupdates, regelmäßig eingespielt sind! - Das ist in den Prüfkatalogen der Datenschutzbehörde enthalten.

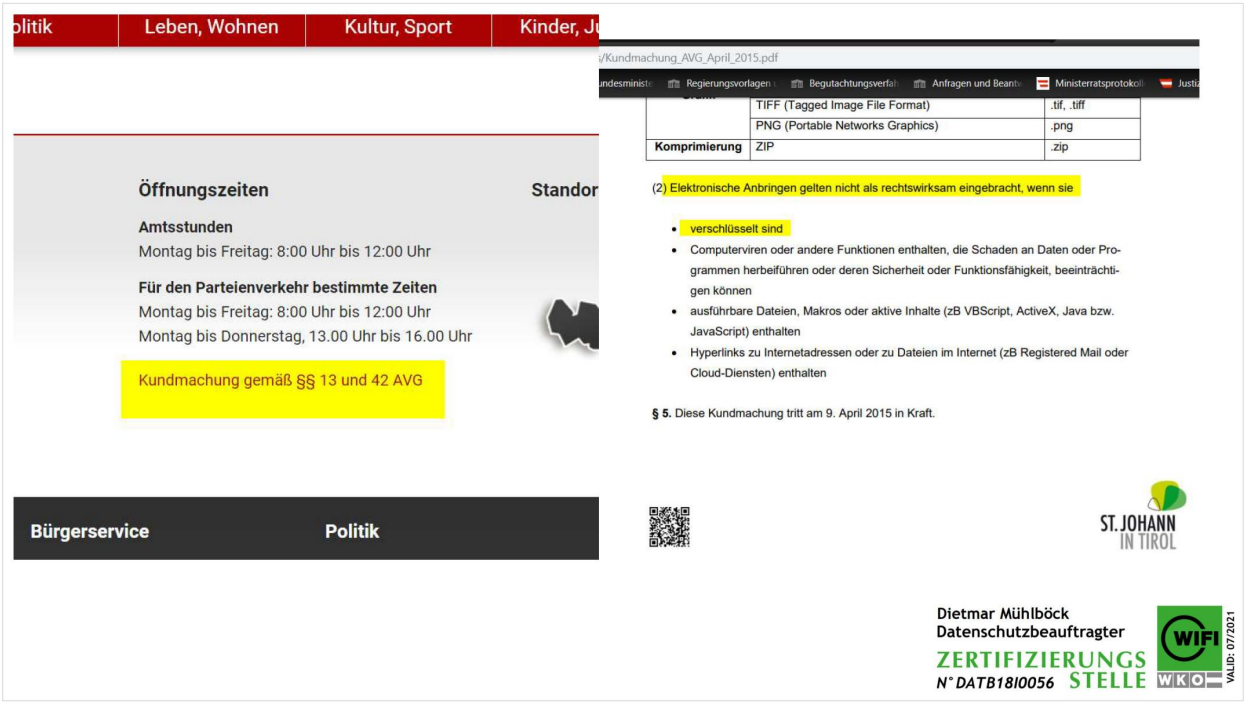
Wenn Sie ein CMS verwenden, dass nicht lokal bei Ihnen installiert ist, dann schließen Sie einen Auftragsdatenverarbeitungsvertrag mit dem Anbieter.

Achtung: Beim weit verbreiteten WordPress ist das nur in der Bezahlversion möglich!

Wenn Sie, wie im Beispiel jquery, externe Programmbibliotheken verwenden, dann achten Sie darauf welche Daten übertragen werden.

Jquery ist problematisch, da es nicht im Privacy Shield angeführt ist und Daten in ein Drittland übertragen werden.

Beauftragen Sie Ihren Webmaster damit!



Anmerkungen zur Kommunikation:

Email-Verschlüsselung forcieren, nicht behindern!

Veröffentlichen Sie einen öffentlichen PGP-Schlüssel für zumindest eine Email-Adresse Ihrer Gemeinde.

PGP steht für „Pretty Good Privacy“ und ist ein Programm zur Datenverschlüsselung.

Messenger-Dienste sind immer problematisch!

Das weit verbreitete WhatsApp ist nicht datenschutzkonform.

Bedenkenlos verwendet werden können:

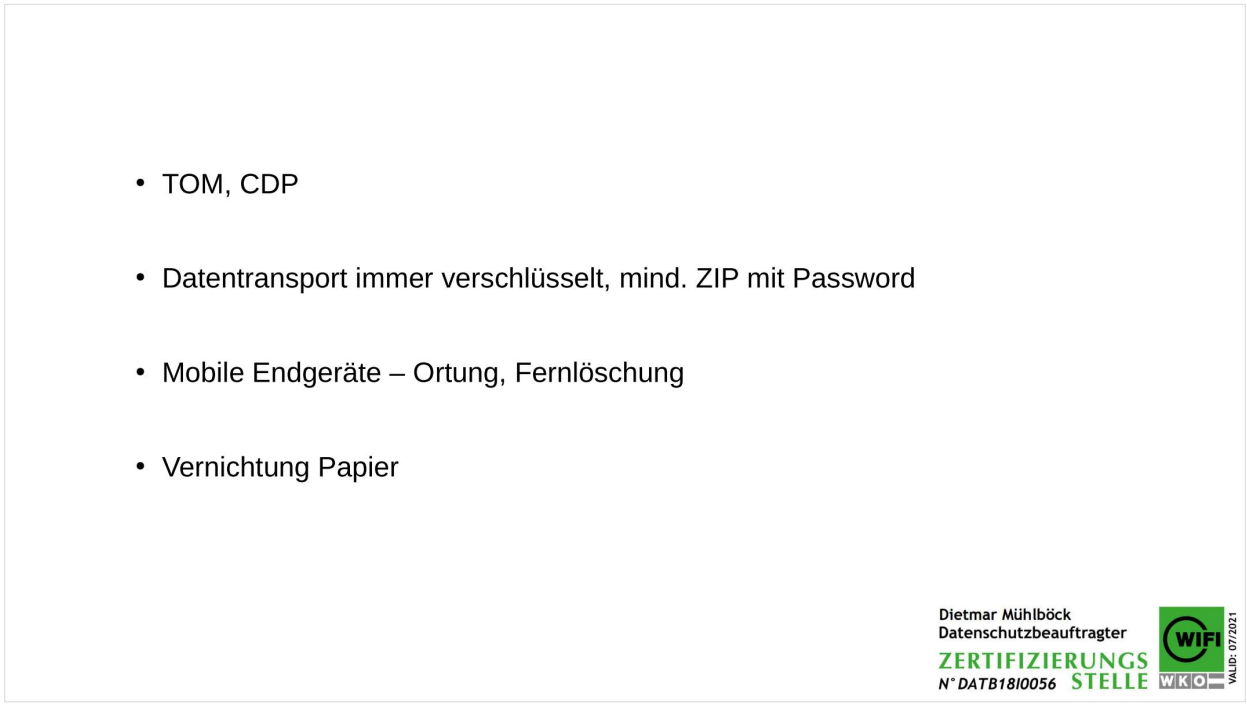
- kostenpflichtig Threema

- kostenlos Signal

Fax:

Geräte nicht öffentlich zugänglich aufstellen!

Online-Fax-Dienste: Auftragsverarbeitungsvertrag schließen!



TOM = Technisch-Organisatorische Maßnahmen

CDP = Clean Desk Policy

Physische Datensicherheit ist wesentlicher Bestandteil eines effizienten Datenschutzes!

1:1 Umsetzung ist nicht notwendig, aber versuchen sich an die Norm ISO 27001anzunähern!

Gute Hinweise dazu finden sich beim Deutschen Bundesamt für Sicherheit in der IT:

http://ux9.de/CN6V8fDm

Physische Datensicherheit:

Feuerfeste und verschließbare Aktenschränke

Einbrüche, Feuer oder Vandalismus können einen Meldefall nach Art 33 DSGVO auslösen!

Datentransport auf USB-Stick / DVD immer verschlüsselt!

Teure Sticks mit Hardware-Verschlüsselung sind nicht notwendig, ein ZIP-Archiv ist ausreichend. > http://ux9.de/xyp2ZUTM

Akten/Papiervernichtung: Sicherheitsstufe 4! > http://ux9.de/vRlTH8vJ
Externe Aktenvernichter: Auftragsdatenverarbeitungsvertrag abschließen!

Folgepunkte zusammengefaßt:

Datenweitergabe an Fraktionen (Wählerverzeichnis) oder Personalvertretung (für Wahlen) erfolgen auf einer gesetzlichen Grundlage, müssen aber im Datenverarbeitungsverzeichnis Angeführt sein.

Nach Art 30 (5) DSG keine Geldstrafen/bußen gegen öffentliche Stellen, aber andere Sanktionen sind möglich:

- Ermahnungen und Verwarnungen – schlechtes Bild in der Öffentlichkeit!

- Einzug und Vernichtung der Verarbeitungsgeräte (Bsp Videoüberwachung)

Es besteht dennoch eine zivilrechtliche Haftung nach § 29 DSG!

> "Alleine das vorliegen einer unzulässigen Verarbeitung genügt nicht um einen materiellen Schaden zu begründen, es muss zu einer greifbaren negativen Auswirkung auf den Betroffenen kommen." > Schweiger in Knyrim, DatKomm Art 82, Rz 17

> Immaterielle Schäden sind nicht abschließend geregelt, Urteile gibt es hauptsächlich im Zusammenhang mit dem MedienG.

Essentiell ist die Zusammenarbeit mit der Datenschutzbehörde, das wird in diversen Straferkenntnissen immer wieder betont!

Die Klassiker:

Fehlende verpflichtete Meldung der Bestellung eines Datenschutzbeauftragten an die Datenschutzbehörde!

Spamfilter auf der Email-Adresse des Datenschutzbeauftragten sind legitim, der Spam/Junk-Ordner muss aber kontrolliert werden!

Vollständige Rückmeldung an den Betroffnen bei keinen weiteren Maßnahmen nach Art 12 (4) DSGVO nicht vergessen!

Die Datenschutzerklärung muss leicht erreichbar und verständlich sein!

Betroffenenrechte erleichern:

> Identitätsnachweis nicht als Erschwernis mißbrauchen!

>> "Phantasie-Email" wie etwa huhu@yahoo.de ist akzeptabel, wenn vorher schon bekannt und zuordenbar.

> Verlangen eines Identitätsnachweis ist nicht fristhemmend!

> Bei Zusendung einer Ausweiskopie diese in das Auskunftsbegehren integrieren!

> Zustellung mit Post mit Vermerk „Eigenhändig" und „Nicht an Postbevollmächtigte" kostet € 3,30 – und das muss es wert sein!

Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
WIFI WKO
VALID: 07/2021

Das ist ein best practice Beispiel für einen Hinweis auf CCTV (Closed Circuit Television - Videoüberwachung)

Hinweis vor Beginn der Überwachung!

Hinweis auch anbringen, wenn es sich nur um Kameraattrappen handelt!

Der Nachweis, dass es Attrappen sind muss erbringbar sein, also Kaufbelege aufbewahren!

Wenn Festplattenrekorder verbaut sind, die Einschübe versiegeln!

Abschließend noch zwei Buchtipps

DSGVO und DSG

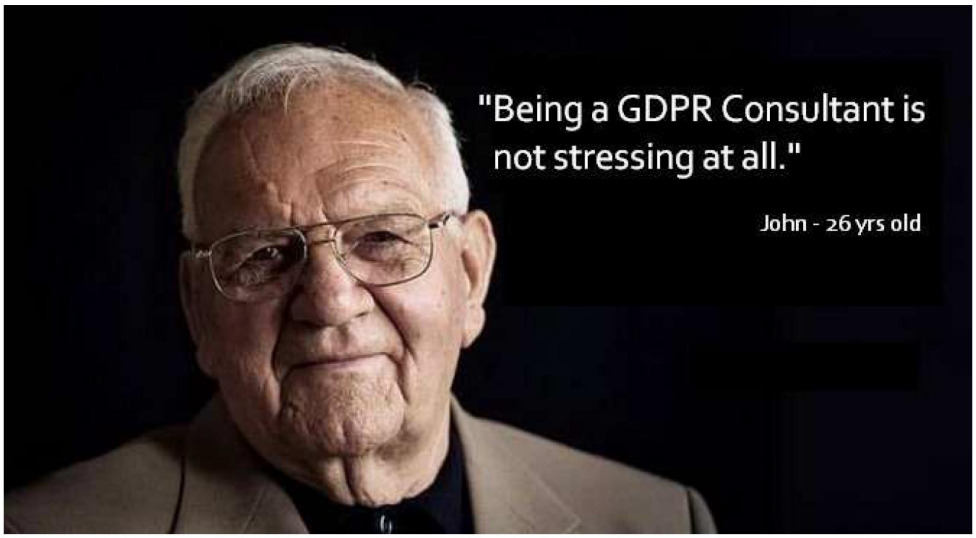
ISBN: 978-3-7097-0184-3

Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
VALID: 07/2021

"Datenschutz neu" für Gemeinden

PDF kostenlos: http://ux9.de/THZm0IsU

Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0056
VALID: 07/2021



Dietmar Mühlböck
Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB1810056
WIFI WKO
VALID: 07.2021

Vielen Dank für Ihre Aufmerksamkeit!

Ich bin für Sie gerne erreichbar:

Telefon – 0664 9534121

Fax – 0512 219921 2787

Threema - C66RWPCN

Email - dm@dsgvo-fit.co.at