Webseite MORZ nach DSGVO

Autoren: Jakob Vidic, Claus Meierhofer
Stand: 11.03.2019

Inhaltsverzeichnis:

Theoretische Vorarbeit

Anlass:

Am 24.5.18 tritt die neue Datenschutzverordnung in Kraft und wird eine Abmahnwelle hinter sich herziehen. Unser Internetauftritt muss fit gemacht werden für die neuen Bestimmungen. Problematisch sind nach einem ersten Check: Cookies, Morz-Kalender, Kontaktformulare und die Googlefonts.

Grundsätzliches:

- Transparenter!
- Datenminimierung!
- Informationspflicht.

Klären:

- Was haben wir eigentlich für einen Rechtsstatus? Unternehmen sind wir nicht und Privatperson auch nicht.
- Ist unsere Einwilligungserklärung der Eltern ausreichend?
- Inwieweit bin ich als ITler und Webseitenersteller für Fehler auch zivilrechtlich haftbar?

Fragen / Entscheidungen:

- Sollen wir grundsätzlich auf umfangreiche Webseite verzichten?
- Sollen wir grundsätzlich Inhalte nur mit Anmeldung zugänglich machen?
- Welche Daten erheben wir auf der Webseite?
- Wie lange sind die Daten gespeichert

Derzeit problematisch:

- Webseite erhebt über Skripte und Plugins Daten. Z. B. protokolliert der Spamfilter IP-Adressen, um so potentielle Gefahren zu blockieren. Aber auch die Googlefonts und recaptcha erheben statistische Daten... Diese müssen abgeschaltet oder ausgetauscht werden.
- Impressum muss ergänzt werden um...
- Datenschutzbeauftragter muss genannt werden. Er muss den Nachweis führen über die Maßnahmen, die wir zum Schutz der Daten ergreifen. Aus dem Berater wird ein Überwacher!
- Wir sind nachweispflichtig. Fettes Bußgeld, wenn wir unsere Datenschutzbemühungen nicht nachweisen können.

TODO:

- Erst mal vom Netz gehen
- Datenschutzbeauftragter benennen
- Impressum anpassen (Kontakt, Erreichbarkeit)
- Einverständniserklärung für Webseite aktualisieren
- SSL-Zertifikat beantragen (https://www.belwue.de/produkte/dienste/webhosting/eu-datenschutz.html)
- Webseite auf https umstellen , erzwingen in .htacess mit Skript. (Belwue-Link) oer (https://andreashecht-blog.de/4183/)

- Kontaktformular konform machen (https://www.ithelps.at/blog/99-online-marketing/768-dsgvo-website-checkliste-2018#kontaktformular)
- Google-Analytics konform machen (https://www.kloos.at/blog/google-analytics-datenschutzkonform-nutzen/)
- Plugins konform machen: Dazu Webseite aufrufen und mit rechter Maustaste auf Untersuchen klicken. Dann Network klicken und Seite neu laden. Entsprechende Plugins deaktivieren oder Entwickler kontaktieren.
- Dokumentation schreiben über unsere Daten, die wir erheben
- Ggf. Cookie-Banner für Zustimmung oder Ablehnung installieren (https://de.wordpress.org/plugins/cookie-notice/)
- Generator für Datenschutzerklärung nutzen, alte ersetzen (https://www.ratgeberrecht.eu/leistungen/muster-datenschutzerklaerung.html)
- Protokollblog auf Webseite, wo wir unsere Schritte dokumentieren

Welche Daten erheben wir?

Belwue (unser Hoster):

- Datum und Uhrzeit des Zugriffs
- Vollständige IP-Adresse des zugreifendem Geräts
- abgerufene Datei oder Funktion mit Abrufmethode (GET oder POST)
- verwendetes Protokoll
- Ergebnis des Abrufs (HTTP Status)
- Zahl der übertragenen Bytes
- Im Error-Logfile noch zusätzlich den aufgetretenen Fehler

Wordpress (core):

- upgedatet und DSGVO-Konform

Wordpress (plugins) überprüfen:

- recaptcha:
- Googlefonts:
- akismet Antispam
- all-in-one-calendar
- erident custom login
- antispam-bee
- email-users
- si-contact-form

Grundsätzliches zu Bildern:

- Grundsätzlich Veröffentlichungsverbot.
- Altersabhängig, Eltern müssen zustimmen.
- Kein Foto ohne Zustimmung.
- Auch bei Gruppenfotos! Immer!
- Tipp: Bei Klassenfahrten Sondergenehmigung einholen. Bei Klassenfotos Schüler vor der Aufnahme selektieren.
- Lehrer müssen vor Veröffentlichung Einverständniserklärung kontrollieren und ggf. einholen.

Besprechung Schulleitung 8.11.2018:

- Schmalspurfassung
- Datenschutzbeauftragter ist von Behörde, SSLörrach, Scherer, Bezeichnung, auf Seite vom Schulamt Lörrach ist das Beispiel.
- Fotos aus dem Archiv entfernen.
- Imagebilder sind auszutauschen. Beispiel: Kletterwand,
- Wie können wir nachvollziehen, welche Schüler einverstanden sind, und welche nicht.

Praktische Umsetzung

Erste Schritte zur technischen Umsetzung am 12.11.2018

- Mit sFTP: BN: aa024707, server: sftp://pubwww7.belwue.de, PW: S7C*yS6b auf Server eingewählt. Im Stammverzeichnis htdoc eine Datei .htaccess erstellt.
- SSL-Zertifikat von Belwue kostenlos installieren lassen. Aktiviert mit .htaccess (https://www.belwue.de/produkte/dienste/webhosting/eu-datenschutz.html).

Weitere Schritte zur technischen Umsetzung am 14.11.2018

- Speicherung von Daten überprüft. Unser Webhoster Belwue erhebt folgende Daten:
    - Datum und Uhrzeit des Zugriffs
    - Vollständige IP-Adresse des zugreifendem Geräts
    - abgerufene Datei oder Funktion mit Abrufmethode (GET oder POST)
    - verwendetes Protokoll
    - Ergebnis des Abrufs (HTTP Status)
    - Zahl der übertragenen Bytes
    - Im Error-Logfile noch zusätzlich den aufgetretenen Fehler
- Diese Daten werden 14 Tage lang aufgehoben
- Datensparsamkeit überprüft:
    - Verzicht auf Googlemaps mit selbst erstellter Landkarte
    - Verzicht auf Youtube-Videos
    - Datenschutzfreundliches AntispamBee statt Akismet aktiviert
- GoogleFonts: Wir vewenden folgende Googleschriften: http://fonts.googleapis.com/css?family=Patrick+Hand|Open+Sans'.
    - Beide Schriften mit sftp in extra erstellten Ordner “Schriften” kopiert. Pfad: ...htdoc/wp/schriften
    - css-code der style.css unseres Childtheme angepasst mit folgendem Code:

```
/* Ab hier eigene Modifikationen */
/* folgende zwei eintraege speichern die schriften auf unserem Server */
/* open-sans-regular - latin */
@font-face {
  font-family: 'Open Sans';
  font-style: normal;
  font-weight: 400;
  src: url('../schriften/open-sans-v15-latin-regular.eot'); /* IE9 Compat Modes */
  src: local('Open Sans Regular'), local('OpenSans-Regular'),
       url('../schriften/open-sans-v15-latin-regular.eot?#iefix')
format('embedded-opentype'), /* IE6-IE8 */
       url('../schriften/open-sans-v15-latin-regular.woff2') format('woff2'), /* Super
Modern Browsers */
```

```
        url('../schriften/open-sans-v15-latin-regular.woff') format('woff'), /* Modern
Browsers */
        url('../schriften/open-sans-v15-latin-regular.ttf') format('truetype'), /* Safari,
Android, iOS */
        url('../schriften/open-sans-v15-latin-regular.svg#OpenSans') format('svg'); /*
Legacy iOS */
}

/* patrick-hand-regular - latin */
@font-face {
  font-family: 'Patrick Hand';
  font-style: normal;
  font-weight: 400;
  src: url('../schriften/patrick-hand-v11-latin-regular.eot'); /* IE9 Compat Modes */
  src: local('Patrick Hand'), local('PatrickHand-Regular'),
        url('../schriften/patrick-hand-v11-latin-regular.eot?#iefix')
format('embedded-opentype'), /* IE6-IE8 */
        url('../schriften/patrick-hand-v11-latin-regular.woff2') format('woff2'), /*
Super Modern Browsers */
        url('../schriften/patrick-hand-v11-latin-regular.woff') format('woff'), /* Modern
Browsers */
        url('../schriften/patrick-hand-v11-latin-regular.ttf') format('truetype'), /* Safari,
Android, iOS */
        url('../schriften/patrick-hand-v11-latin-regular.svg#PatrickHand')
format('svg'); /* Legacy iOS */
}
```

- Um sicher zu gehen, wird die Verbindung zu Googleserver mit Plugin **Remove Google Fonts References** deaktiviert.
- Funktion überprüft mit Firefox, Elemente untersuchen, Server. Funktioniert.

Technische Umsetzung am 21.11.2018

- Sicherung der kompletten Webseite auf lokalem Rechner
- Datenbanksicherung täglich um 23:00, letzte 7 Backups
- Personenzugriff Schüler und Lehrer aktualisiert, Benutzer gelöscht. Rollen überprüft.
- Aufforderung zu regelmäßigem Passwortwechsel über Gruppenmail. Zuletzt am 21.11.18
- Referrer leaks blockiert über folgenden Eintrag in die header.php des Themes. *<meta name="referrer" content="no-referrer">*
- Achtung: Noch nicht im Childtheme, ist also nach Update des Themes wieder neu einzutragen.
- Module und Plugins aktualisiert. Wird regelmäßig gemacht.

Technische Umsetzung am 28.11.2018

- Komplettsicherung mit Filezilla gemacht auf Schulserver.
- Childtheme mit functions.php ergänzt. Diese ergänzt die functions.php, um die referrer leaks zu blockieren. Test durchgeführt mit dem Ergebnis “Referrers not leaked”

Technische Umsetzung am 4.12.2018

- XMLRPC stellt ein Sicherheitsrisiko dar. Wird für Zugang von Wordpress-App verwendet. Datei über .htaccess im Rootverzeichnis blockiert. Kann bei Bedarf wieder aktiviert werden. Code:
    - <Files xmlrpc.php>
    - Order Deny,Allow
    - Deny from all
    - </Files>
- Unnötiges Plugin gelöscht: P3 (Plugin Performance Profiler)
- Fast secure Contact form deaktiviert. Es ist nicht mehr sicher. Ersatz muss her.

Datenschutzrechtliche Voreinstellungen

Wordpress bietet ab Version 4.9.6 einige Möglichkeiten, um den Forderungen der DSGVO gerecht zu werden.

Umsetzung der Voreinstellungen 11.12.2018:

- Blogfunktion / Kommentare deaktiviert.
- Datenminimierung. Es werden nur tatsächlich notwendige Daten erhoben. So z. B. die Anmeldedaten eines Redakteurs (Nachname, Vorname, E-Mailadresse, Spitzname, hochgeladene Bilder, Registrierungsdatum - mehr nicht)
- Auf Anfrage nach Speicherung von personenbezogenen Daten, kann Wordpress diese exportieren, um sie der Person zukommen zu lassen (Werkzeuge - personenbezogene Daten exportieren)
- Kontaktformular deaktiviert
- Cookie-Check: Firefox nutzen oder: http://www.cookie-checker.com/
- Cookie-Banner oder Hinweis recherchiert. Die DSGVO verlangt einen Hinweis auf Cookies. Zumindest in der Datenschutzerklärung muss der Hinweis rein, oder besser noch als Cookiebanner.
- Laut dem Ratgeber https://www.webtimiser.de/cookie-plugins-wordpress/ für das Plugin Cookie-Notice entschieden. Hat 900000 Installation und volle Wertungszahl.

Umsetzung der Voreinstellungen am 19.12.2018:

- Cookie-Notice installiert. Möglichkeit zur Ablehnung von Cookies aktiviert. Mit Impressum verlinkt.
- Datenschutzerklärung mit Hilfe von erecht24 generiert. Platzierung auf jeder Seite im Footer.
- Datenschutzerklärung beinhaltet Hinweis auf Rechte der Nutzer.
- Beschwerdestelle: Datenschutzbeauftragter Schulamt Lörrach mit Kontaktdaten genannt
- Speicherdauer und Löschfristen unseres Providers Belwue in der Datenschutzerklärung ergänzt.

Umsetzung der Datenschutzerklärung am 21.01.2019

- Text von E-Recht auf Webseite implementiert. Format angepasst. Inhalte überprüft.
- Neue Version Wordpress 5.0.2
- Impressum mit Hilfe von E-Recht erstellt und angefordert.
- Impressum auf Webseite platziert, von jeder Seite erreichbar

Umsetzung der Kontaktformulare am 26.1.2019

- Bei den Kontaktformularen setzen wir einen Hinweis auf die Datenschutzerklärung und beschreiben, was wir mit den Daten machen.
- Außerdem brauchen wir von Belwue einen Datenverarbeitungsvertrag. Erledigt.
- Als Plugin kommt ninjaforms in Frage. Kostet für mehrere E-Mail-Adressen 69 Euro im Jahr.
- Contact7 installiert. Dinosaurier unter den Kontaktformularen, lässt sich aber DSGVO-Konform machen (siehe Link unten). Weitere Gründe dafür:
- Contact7 speichert die E-Mails nicht ab
- Contact7 unterstützt reCaptcha
- Jedes Kontaktformular erhält angepassten Code, der die Besucher dazu zwingt, sich mit unserer Datenschutzerklärung auseinander zu setzen. Müssen mit einem Häkchen Zustimmung erteilen.
- Als Spamschutz die Erweiterung Honeypot installiert. Sie lockt die Spambots in einen für die Benutzer unsichtbaren “Honigtopf”. Link dazu: Contact Form 7 Honeypot. Dadurch können wir auf das reCaptcha verzichten.
- Für verschiedene Empfänger: https://contactform7.com/selectable-recipient-with-pipes/

Umsetzung des Kalender-Plugins am 04.02.2019

- registriert bei timely, unserem Kalenderplugin.
- Freeversion gebucht für einen Kalender. BN: mh@morz.de, PW: wu...t
- Nur ausgewählte Termine kommen in Zukunft in Kalender

Umsetzung Kontaktformular am 11.03.2019

- Reste von altem Kontaktformular gelöscht
- Kontaktformular für Sekretariat, Webteam und Lehrer veröffentlicht.

Vertrag zur Auftragsverarbeitung

Umsetzung der Auftragsverarbeitung am 28.01.2019:

- Vertrag von Belwue über Auftragsdatenverarbeitung eingeholt. In Sekretariat hinterlegt.
- Im Prinzip bräuchten wir wohl auch einen von Google für Googlefonts, Googlekalender und recaptcha. Vorsorglich recaptcha deinstalliert. Spamschutz in den Kontatkformularen wird jetzt mit einem Honeypot realisiert. Googlefonts sind auch lokal auf unserem Server gespeichert.

TODO:

- ~~Kalender Kostenübernahme Schulleitung fragen (Jakob)~~
- ~~Backup Sicherung (Jakob)~~
- ~~Googlefonts einbetten (Claus)~~
- ~~Ersatzbild für DSGVO Ersatz (Jakob)~~
- ~~refferer leaks ins header.php des childtheme (claus)~~
- ~~Bilder mit Personen aus Mediengallery löschen~~
- ~~Impressum anpassen~~
- ~~Datenverarbeitungsvertrag von Belwue anfordern~~
- ~~Dokumentation für DSGVO erstellen~~

- ~~Contact Form DSGVO konform machen~~
- Googlekalender DSGVO-konform? Abklären!
- ~~Kalender Plugin~~
- ~~Möglichkeit der Einwilligung beim Seitenstart platzieren~~
- Name des Datenschutzbeauftragten ins Impressum
- ~~Datenschutzerklärung dsgvo~~

Links:

- https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen (viel zu unkonkret, Behördendeutsch)
- https://www.ithelps.at/blog/99-online-marketing/768-dsgvo-website-checkliste-2018 (nützliche Tipps, Checklisten)
- https://www.ithelps.at/images/2018/04/dsgvo/DSGVO-Website-Checkliste-2018.pdf (checkliste)
- https://datenschutz-schule.info/ (Grundlage mit toller Downloadcheckliste)
- https://wp-ninjas.de/wordpress-google-fonts (Googlefonts blockieren)
- https://www.elmastudio.de/wordpress-theme-anpassungen-mit-hilfe-von-child-themes/ (Child-Theme anpassen)
- https://www.webtimiser.de/wordpress-child-theme-erstellen/ (functions.php)
- https://webbkoll.dataskydd.net/en (Webseite testen)
- https://www.webtimiser.de/wordpress-4-9-6-datenschutz-update/ (Wordpress Voreinstellungen Datenschutz)
- https://www.tippscout.de/firefox-ueberpruefen-ob-eine-seite-cookies-speichert_tipp_4153.html (Cookies anzeigen lassen in Firefox)
- Kontaktformular: https://ninjaforms.com/gdpr-compliance-wordpress-forms/
- Kontaktformular Contact7 DSGVO-Konform: https://marcus-luepke.info/datenschutzgrundverordnung-wordpress-plugin-contact-form-7-anpassen/