SUHLRIE
Zahlen bewegen – Zukunft gestalten.

Collaborato Training

Bis zum 25.Mai 2018 muss sie umgesetzt sein!
Info zur Umsetzung
EU - Datenschutzgrundverordnung

Kurz Vorab: Wie es zu diesem Text kommt:

Bei dem Versuch mich, Susanna Suhlrie, über die Anforderungen der EU-DSGVO zu informieren habe ich mitunter wirklich die Orientierung verloren. Mir geht es auf 2 Perspektiven darum es zu verstehen, zum einen für mein eigenes Unternehmen, zum anderen im Interesse all meiner Kunden und Kundinnen, Mit vielen Knoten im Kopf habe ich mich, wie so oft, mit dem Kollegen Günther A. Biebl von Collaborato Training ausgetauscht.

Unsere Erkenntnisse haben wir hier zusammengestellt. Unseren Frust und Verwirrung, die zum Teil groß war und auch noch ist, haben wir versucht, rauszulassen. Die EU-DSGVO scheint für uns ein Thema zu sein, bei dem, je mehr du versuchst es zu verstehen, sich die Fragezeichen potenzieren.

Insofern ist dieser Leitfaden von uns nach bestem Wissen und Gewissen erstellt – ohne Anspruch auf Vollständigkeit und ohne jegliche Gewähr. Wir freuen uns, wenn er Ihnen nutzt.

Was ist zu beachten? Welche Maßnahmen müssen Sie individuell in Angriff nehmen?

Ist mein Unternehmen betroffen?

Mit 99,99 % Wahrscheinlichkeit: Ja.

Denn betroffen ist jeder Unternehmer und jedes Unternehmen vom Freiberufler (bspw. Anwalt, Architekt) über den Kleinunternehmer (bspw. Kaufmann, Gewerbetreibender, GbR, Einmann-GmbH) bis hin zum Konzern.

Vorausgesetzt: Sie verarbeiten personenbezogene Daten (automatisiert oder nicht-automatisiert).

Personenbezogene Daten sind bereits die Daten der Mitarbeiter, der Kunden, der Lieferanten, der Netzwerk- und Kooperationspartner, wie auch die IP-Adresse von Webseitenbesuchern. Das heißt also, das neue Datenschutzrecht betrifft tatsächlich jeden, der in irgendeiner Art und Weise zum Beispiel eine Kundendatei führt oder ein CRM-System nutzt oder auch nur seine Teilnehmerdaten digital erfasst bzw. verwaltet.
Sie verstehen?

Worum geht es denn überhaupt?

Datenschutzrecht regelt, für welche Zwecke und in welchem Umfang personenbezogene Daten eines anderen verarbeitet werden dürfen.

Das Datenschutzrecht wird ab dem 25.05.2018 wesentlich strenger. Was vor allem trifft: Verstöße werden umfassender verfolgt. (Hierzu heißt es, dass mehr Personal bei der Aufsichtsbehörden bereit gestellt wird und immaterielle Schadensersatzansprüche Betroffener geschaffen werden, etc.) Die Bußgelder steigen exorbitant an auf bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes des Unternehmens (je nachdem, welche Summe höher ist). Die genauen Kriterien hierfür finden sich im Art. 83 und 84 DSGVO.

Was ist konkret zu tun?

A. Informationspflichten

Sie müssen bei der Erhebung der Daten die Person, um deren Daten es geht (= den/die Betroffene(n)) umfangreich informieren. Diese Informationspflichten werden mit der DSGVO ausgeweitet. Beispiele für künftige Informationen, die Sie erteilen müssen sind:

a. Speicherdauer der Daten,
b. Quellen, aus denen die Daten stammen,
c. Widerruflichkeit de Einwilligung,
d. Hinweise auf die Rechte auf Sperrung, Löschung, Berichtigung,
e. Hinweise auf (mögliche) Übermittlung ins EU-Ausland und Mitteilung der Rechtsgrundlage der Übermittlung.

Damit sind alle Datenschutzhinweise, alle Einwilligungserklärungen und alle Datenschutzbelehrungen anzupassen. Denken Sie daran, dass eine Auslandsübermittlung schon dann stattfindet, wenn die Daten über Tools, Plugins, Apps o.ä. von US-Anbietern verarbeitet werden.

B. Einwilligung

Die Einwilligung durch die Betroffenen bleibt eine Möglichkeit der legalen Datenverarbeitung.

ABER: Die Voraussetzungen für eine wirksame Einwilligung werden verschärft und die Kopplung der Einwilligung mit der Erhebung nicht zwingend erforderlicher Daten kann die Einwilligung unwirksam machen.

Daher sind alle Einwilligungserklärungen, die Sie aktuell verwenden, anzupassen, damit auch künftig eine wirksame Einwilligung möglich ist.

C. Datenschutzfolgenabschätzung

Die neue DSGVO verpflichtet Sie alle künftigen Datenverarbeitungsvorgänge darauf zu prüfen, ob voraussichtlich ein hohes Risiko für die Betroffenen besteht. Das Risiko kann aufgrund Art, Umfang, besonderer Umstände oder Zwecke der Datenverarbeitung bestehen.

Ein Beispiel hierfür: ein unverschlüsseltes Kontaktformular (= ohne http**s**://)

Sie müssen also immer diese Prüfung vornehmen und dann, wenn ein solches Risiko nicht auszuschließen ist, eine Abwägung des Nutzens mit den Folgen in Ansehung der Risiken vornehmen.

Prüfung und Abwägung sind exakt vorzunehmen und schriftlich zu dokumentieren, denn Sie müssen jederzeit die Rechtsmäßigkeit der bei Ihnen vorgenommenen Datenverarbeitungen nachweisen können (das gilt für alle Verarbeitungsvorgänge). Damit besteht also in Zukunft auch die Pflicht, umfangreiche Risikoanalysen vorzunehmen und diese gemeinsam mit den geplanten Abhilfemaßnahmen formgerecht zu dokumentieren.

Diese Prüfung und Dokumentation muss jetzt für Ihre Datenverarbeitungen erfolgen und künftig ist sicherzustellen, dass vor Beginn jeder neuen Datenverarbeitung eine solche Prüfung und Abwägung erfolgt.

D. Datenschutzbeauftragter

Auch nach neuem Recht muss ab 10 Mitarbeitern, die mit der Datenverarbeitung beschäftigt sind, ein Datenschutzbeauftragter im Unternehmen bestellt werden. Daneben gelten aber über die DSGVO weitere Bestellungsgründe, nämlich dann, wenn es zur Kerntätigkeit des Unternehmens gehört:

a. die umfangreiche regelmäßige & systematische **Überwachung** von betroffenen Personen oder
b. die umfangreiche Verarbeitung **sensitiver** Daten.

Der Datenschutzbeauftragte bekommt auch eine höhere Verantwortung und weitreichendere Befugnisse.

E. Meldepflichten

Künftig ist bei jeder "Datenpanne" eine Meldung an die Aufsichtsbehörde zu machen. Es genügt, wenn eine Daten-Kompromittierung möglich war/ist.

Lt. Wiktionary spricht man von einer Kompromittierung, wenn ein System manipuliert, angegriffen, gestört wird, besonders ein Datenbanksystem.

Natürlich ist dann auch zu melden, welche Daten betroffen und, welche Maßnahmen getroffen wurden, um die Panne zu beheben und zu verhindern, dass ein vergleichbarer Vorfall erneut entsteht.

Natürlich sind auch alle diese Vorfälle – auch die nicht meldepflichtigen – schriftlich zu dokumentieren und ein Protokoll darüber zu führen. Die Aufsichtsbehörden haben Anspruch jederzeit Einsicht in diese Dokumentation zu nehmen.

Zu den nicht meldepflichtigen gehören wohl folgende, die im Erwägungsgrund 75 der DSGVO definiert sind. Hierhandelt es sich um „die Verletzung des Schutzes personenbezogener Daten, die voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt."

F. Privacy by Default & Privacy by Design

Künftig ist es erforderlich schon in der Entwicklung die Datenschutzgrundsätze einzuhalten. Damit ist schon die Entwicklungsabteilung zu sensibilisieren und zu schulen, dass das zu entwickelnde Produkt die Grundsätze der Datensparsamkeit, Speicherbegrenzung, Datenminimierung etc. berücksichtigt.

Das Pendant dazu ist der Grundsatz, dass marktreife Produkte so voreingestellt sein müssen, dass nur die zwingend erforderlichen Datenübermittlungen freigeschaltet sind und alle weiteren vom Nutzer selbst aktiviert werden müssen (=Opt In).. Damit muss also besonderer Wert darauf gelegt werden, wie das Produkt auf den Markt kommt und auch wie der zugrundeliegende Nutzungsvertrag gestaltet wird. Denn dadurch kann Einfluss auf die zwingend erforderlichen Datenverarbeitungen genommen werden.

G. Datenübertragbarkeit

Ab dem 25.05.2018 müssen Sie sicherstellen, dass die Kundendaten, die Sie direkt bei Ihrem Kunden erhoben haben, strukturiert in Standarddateiformate eingespielt und an andere Anbieter, bspw. einen Wettbewerber, übertragen werden können. Denn die DSGVO sieht vor, dass der Kunde einen Anspruch auf eine solche Datenübertragung hat. Standard bedeutet hierbei wohl: strukturiert, gängig, maschinenlesbar.

H. Dokumentation & Verantwortlichkeiten

Alle Pflichten und Maßnahmen nach der DSGVO müssen von Ihnen dokumentiert werden.

Für die Durchführung der neuen Pflichten, wie auch für die Dokumentation derselben und für den Erhalt der Beweisführungsmöglichkeiten zur Einhaltung aller Pflichten müssen Sie Ihre internen Prozesse prüfen und anpassen, sowie geeignete Mitarbeiter auswählen, Verantwortlichkeiten vergeben, wie auch die betroffenen Mitarbeiter schulen und einweisen.

I. Verarbeitungsverzeichnis

Nach Art. 30 DSGVO müssen Sie ein Verzeichnis aller (!) Verarbeitungsvorgänge personenbezogener Daten aufstellen und pflegen, also aktuell halten.

Die Erstellung dieses Verzeichnisses betrifft jedes Unternehmen, dass unter die DSGVO fällt (siehe oben) und ist Ausgangspunkt jeder DSGVO-Compliance.

Wieso kann das nicht der Datenschutzbeauftragte tun, wenn wir einen haben?
Wichtig: Da der Datenschutzbeauftragte die Vollständigkeit des Verarbeitungsverzeichnisses zu prüfen hat, bestünde bei seiner Beauftragung mit der Erstellung des Verzeichnisses eine Interessenkollision. Der (interne oder externe) Datenschutzbeauftragte darf also weder mit der Erstellung noch mit der Pflege des Verarbeitungsverzeichnisses beauftragt werden!

Vorlagen und Muster für ein Verarbeitungsverzeichnis können Sie im Internet finden. Ob und inwieweit diese taugen, müssen Sie selber beurteilen.

Die Pflicht gilt auch für Auftragsverarbeiter bzgl. der im Auftrag verarbeiteten Daten. Das heißt, dass Unternehmen, die für andere Daten verarbeiten nicht nur ihre eigenen Verarbeitungen, sondern auch diese Auftragsverarbeitungen auflisten müssen. Das betrifft bspw. Cloud-Services, aber auch die Verarbeitung von User-Daten auf dem eigenen Webserver und die Durchführung von Fernwartungsdiensten.

Und nun?:

Überlegen Sie an welchen dieser hier aufgeführten Punkte Sie anpassen müssen und welche Schritte Sie hierzu umsetzen müssen:

A	Informationspflichten	
B	Einwilligung	
C	Datenschutzfolgenabschätzung	
D	Datenschutzbeauftragter	
E	Meldepflichten	
F	Privacy by Default & Privacy by Design	
G	Datenübertragbarkeit	
H	Dokumentation und Verantwortlichkeit	
I	Verarbeitungsverzeichnis	

Unser Praxistipp: In einer Kladde nach und nach notieren, welche Daten überhaupt im Unternehmen erhoben werden. Dann ergänzen Wozu? Wie? Wie werden Sie gespeichert? Wie lange? Etc.
Und immer wenn einem hierzu etwas ein- und auffällt, diese Information ergänzen. So entsteht ein immer besserer Überblick worum es eigentlich im eigenen Unternehmen bei den erhobenen Daten geht.

Was ist noch zu tun:

Erste Maßnahmen im Online Marketing:

In der Datenschutzerklärung haben Sie darüber zu informieren, welche personenbezogenen Daten Sie und die Ihrer Website angeschlossenen Dienste erheben, wie sie diese verarbeiten, archivieren, etc. Für die einzelnen Dienste muss hier auch eine sogenannte Opt-Out Lösung vorliegen)

Impressum
Die DSGVO ändert nichts an den Anforderungen an das Impressum.
Es bleibt dabei:

Es muss klar und leicht erkennbar sein (nicht „Info" – sondern „Impressum" oder „Kontakt") (auch bei der Smartphone oder Tablet-Ansicht),

unmittelbar erreichbar (mit maximal zwei Klicks),
ständig verfügbar und mit fest vorgegebene Inhalten, die Grundlagen sind zu finden in TMG, § 55 Abs. 2, RStV, §§ 2 und 3 DL-InfoV

Achtung: Der Burger-Button  zu dem häufig das Menü der Webseite in der Handyansicht steckt dann den direkten Zugang zum Menüpunkt „Impressum". Evtl. ist es sinnvoll den Link zum Impressum (auch) in der Fußzeile einzufügen.

Datenschutzerklärung
Auf Ihrer Website muss die Datenschutzerklärung von jeder Seite aus zu finden und mit 2 Klicks zu erreichen sein (wie es auch für das Impressum gilt).
Achtung: Bitte überprüfen, dass der Cookie Hinweis bei der Tablet oder Smartphone-Ansicht das Impressum und die Datenschutzerklärung nicht verdeckt!

In der Datenschutzerklärung haben Sie darüber zu informieren, welche personenbezogenen Daten Sie und die Ihrer Website angeschlossene Dienste erheben, wie sie diese verarbeiten, archivieren, etc. Für die einzelnen Dienste muss hier auch eine sogenannte Opt-Out[1] Lösung vorliegen). Die Inhalte, die in der DSGVO zu beachten sind, finden Sie u.a. in § 13 DSGVO:

- Namen und Kontaktdaten des Verantwortlichen,
- sowie gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung (Newsletter, Kontaktformular, Bewerbung,…)
- Rechtsgrundlage der Verarbeitung (Nennung des Paragraphen)
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Ggfls. die Absicht, die Daten an ein Drittland zu übermitteln
- Speicherdauer der Daten
- Hinweis auf die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrechts, Datenübertragbarkeit)Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Falls Sie eine automatisierte Entscheidungsfindung einsetzen:

[1] Opt-Out: User muss sich von dem Service auch abmelden können

- Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, inkl.
- aussagekräftige Informationen über die involvierte Logik sowie
- die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung

Uffz, das klingt wild. Wir gehen davon aus, dass eine erste Hilfestellung hierzu durch DSG-Generatoren möglich ist. Rechtssicherheit wird es hier wohl nur mit juristischem Fachrat geben.

HTTPS vs. HTTP (Kontaktformular)

Stellen Sie sicher, dass ihre Website SSL-verschlüsselt ist. Wenn im Browser vor dem Namen Ihrer Domain „https“ erscheint anstatt „http“, ist Ihre Website ssl-verschlüsselt. Sie erkennen es auch an dem meist grünen Schloss-Symbol davor. Sicher | https:// Sollte hier ein Ausrufezeichen stehen, hat die Umstellung auf https:// nicht vollständig geklappt.

Berücksichtigen und informieren müssen Sie sich über die Folgen und legale Nutzung, wie die Informationspflicht im Hinblick auf:

Besuchermessung (Tracking)

Verwenden Sie Cookies? Der User muss der Verwendung explizit zustimmen! Eine konkludente Zustimmung wie in Formulierungen dieser Art: „Wenn Sie weitersurfen, gehen wir von einer Zustimmung aus“ reicht nach aktueller Meinung dann nicht mehr.

IP-Adresse

Die IP-Adresse ist die Netzwerkadresse eines Computers. Daraus kann unter Umständen auf den Nutzer geschlossen werden. Frage ist also: Wird diese gespeichert? Wozu und wie lange? Evtl. speichert Ihr Provider ja schon ohne Ihr zutun die IP-Adresse! Einfach nachfragen und klären.

Remarketing und Conversion Tracking

Werden Ihre Shop-Besucher auf anderen, fremden Webseiten noch mal mit dem eben betrachteten Produkt konfrontiert z.B. in einem Werbebanner, spricht man von Remarketing.

Social Plugins, eingebettete Inhalte (Shariff)

Klassische „Teilen-Buttons“ unter dem Artikel melden an die jeweiligen sozialen Netzwerke, dass der Besucher sich gerade auf dieser Seite befindet. (Genauer: die IP-Adresse wird übermittelt). Es gibt datensparsamere Lösungen wie 2-Klick-Buttons oder Shariff-Buttons. Hier wird erst nach der Nutzeraktion (Klicken auf das Logo) ein Kontakt zu dem jeweiligen Netzwerk hergestellt.

Newsletter

Für Newsletter gilt: Sie können nicht sicher sein, dass der Nutzer der das Anmeldeformular ausgefüllt hat auch der Eigentümer der verwendeten Mailadresse ist. Deshalb müssen Sie sich das zusätzlich Bestätigen lassen und diese Bestätigung auch aufbewahren. (= Double Opt-In). Meist wird das mit einer Mail gelöst die den Empfänger auffordert einen Link anzuklicken. Erst danach ist der Newsletter freigeschaltet. Natürlich findet sich in jedem Newsletter auch ein Link zu abmelden und eine Absenderinformation. Vorsichtige Personen lassen sich jede versendete Bestätigungsmail noch mal in Kopie an ein weiteres Postfach zur Aufbewahrung und zum Nachweis senden.
Weiterer Punkt bei den Newsletter ist: Die Systeme zeigen gerne an ob ein User die Mail geöffnet hat oder ob es einen der Links im Newsletter angeklickt hat. Meist wird diese „Öffnungsrate“ als Erfolgsmesser benutzt. Wenn das gemacht wird, handelt es sich natürlich um weiteres Tracking, über das der User in der Datenschutzerklärung informiert werden muss.

Verträge mit Dienstleistern (wie dem Webhoster) VDiA

Die heißen „Vereinbarung zur Datenverarbeitung im Auftrag“ oder Data Processing Agreement und können per Email bei den entsprechenden Diensten angefordert werden.

OWASP Top 10

Webanwendungen mit der Sie persönliche Daten verarbeiten sollten gegen Hackerangriffe ausrichtend geschützt sein. Diese Liste zählt die zehn wichtigsten Schwachstellen auf, gegen die Ihre Anwendung gesichert sein sollte. Die Liste wird regelmäßig aktualisiert.
https://www.owasp.org

Google Fonts, Youtube und CDN

Wenn Ihre Webseite Schriften von Google verwendet – viele moderne Webseiten tun das – wird die Schrift jedes mal bei Google geladen und Google bekommt so die IP-Adresse Ihrer Besucher. Dasselbe gilt für Content Delivery Networks (CDN). Hier werden Teile der Seite gar nicht von Ihrem Provider ausgeliefert sondern von einem Dritten z.B. um Ladezeiten zu beschleunigen. Wenn ich das richtig verstehe, sollte sich das dann in der Datenschutzerklärung oder sogar per Vertrag zur Auftragsdatenverarbeitung wiederspiegeln. Auch Youtube-Videos setzen ungefragt Cookies und melden die IP-Adresse an Google. Sie lassen sich aber auch über den „erweiterten Datenschutzmodus“ cookiefrei oder mit einem lokalen Vorschaubild sogar Datenschutzkonform umsetzen.[2]

Hilfreiche Links für den Freund des schnellen Klicks

Datenschutzerklärungs-Generatoren für die Webseite:

- Kostenfrei: https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/
- https://www.e-recht24.de/datenschutzgrundverordnung.html

Weiterführende Links – für den kompletten Durchblicksstrudel (NOT!):

Gesetzestext: **https://dsgvo-gesetz.de/**

Wikipedia: **https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung**

Speziell für WordPress-Webseiten (sowieso das beste CMS) ☺

- WordPress-Technik-Hinweise vom BSI:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_web_server_checkliste_WordPress.pdf
- WordPress-Plugins

https://de.wordpress.org/plugins/google-analytics-opt-out/

https://de.wordpress.org/plugins/wp-gdpr-compliance/

https://de.wordpress.org/plugins/shariff/

[2] https://www.heise.de/ct/ausgabe/2016-1-YouTube-Videos-datenschutzkonform-einbetten-3046316.html