20 Millionen Euro unter dem Meer

Die Datenschutzgrundverordnung für Designer*innen

Wie haltet ihr es denn mit dem Datenschutz, wurden wir noch nie gefragt. Entsprechend haben wir uns, zu unserer Schande, bisher nur am Rand damit beschäftigt. Aber gut, wir sind ja auch kein großes Unternehmen, wir wenden uns nur an Geschäftskunden, wir kaufen oder verkaufen keine Adressdaten und wir machen kein Finanzscoring mit Big Data. Da betrifft uns doch der Datenschutz gar nicht.

Diese Haltung ist unter (solo)selbstständigen Designer*innen und kleinen Agenturen verbreitet. Und falsch. Das war sie bisher zu Zeiten des ›alten‹ Bundesdatenschutzgesetzes (BDSG) und das ist sie auch ab dem 25. Mai 2018 mit Geltung der Datenschutzgrundverordnung (DSGVO) und der damit verbundenen Neufassung des Bundesdatenschutzgesetzes (BDSG-neu).

Der einzige Unterschied: Bisher waren die Konsequenzen für Verstöße gegen das BDSG vernachlässigenswert – mit den neuen Regelungen ändert sich das: Es können Bußgelder verhängt werden, die laut Gesetzesbegründung weh tun sollen. Je nach Verstoß drohen Bußgelder bis zu einer Höhe von 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes, je nachdem, was höher ist.

Deshalb liest man an vielen Stellen von der DSGVO und dem Ungemach, das mit ihr drohe. Das ist auch der Grund, warum in vielen Unternehmen emsig an der Umsetzung gearbeitet oder zumindest über die Umsetzung nachgedacht wird. Denn Nichtstun kann echt teuer werden.

Mit drei Kolleg*innen arbeite ich in einer als Gesellschaft bürgerlichen Rechts (GbR) organisierten Agentur für Kommunikation. Vor allem kleinen und mittelständischen Unternehmen und Organisationen bieten wir die ganze Palette des Kommunikationsdesigns an. Nachdem wir nicht nur in designfremden Publikationen über die DSGVO lasen, sondern auch der uns etwas näher stehende f:mp. zu Seminaren einlud, wurde klar, das betrifft wohl auch uns.

Viele Artikel und Hinweise stellten Behauptungen auf (»Für kleine Unternehmen kein Datenschutzbeauftragter nötig«, »Ohne Datenschutzmanagementsystem geht nix«) und geizten mit Quellen. Nach einiger Zeit fruchtloser Recherche in Beiträgen *über* die DSGVO, wagte ich einen Blick *in* die DSGVO und das BDSG-neu und kann das nur jedem empfehlen. Ja, das ist teilweise kompliziert geschrieben; ja, es gibt Schachtelsätze und ja, manches bietet viel Raum für Interpretation. Aber ich glaube, für uns als Einzelunternehmer*innen, die nicht hauptsächlich personenbezogene Daten verarbeiten, reicht der laienhafte Blick aus. Außerdem übernehmen wir dann selbst Verantwortung und können zumindest sagen: so habe ich das interpretiert. Wir haben uns in der Agentur entschieden, uns selbst mit dem Thema

zu beschäftigen – vielleicht schreiben wir in fünf Jahren einen Artikel darüber, wie man die DSGVO lieber nicht umsetzen sollte, weil wir 20 Millionen Euro finden müssen, um ein Bußgeld zu begleichen – wer weiß. Als Unternehmer*innen müsst ihr das Risiko selbst einschätzen.

Ein Blick in die Datenschutzgrundverordnung

Neben der nicht besonders übersichtlichen offiziellen Veröffentlichung der DSGVO im Amtsblatt der Europäischen Union gibt es auch andere übersichtlichere Darstellungen. Ich verlinke im Folgenden auf erstere von dejure.org.

Für die Eiligen: Wenn ihr diesen Text am 24. Mai 2018 lest und einfach nur ganz schnell ein paar Hinweise haben wollt, wie wir uns an die Umsetzung gemacht haben, springt direkt zum Abschnitt »Aber was machen wir jetzt konkret?«, der bis dahin erschienen sein wird.

Betrifft uns das neue Datenschutzrecht überhaupt?

Meine Kolleg*innen zweifelten: »Betrifft uns das denn *wirklich*? Wir machen doch nur …« Deshalb ein relativ ausführlicher Einstieg. Wer schon überzeugt ist, dass die DSGVO uns betrifft, kann einfach zum nächsten Abschnitt springen.

Wer personenbezogene Daten[1] verarbeitet[2] und das nicht ausschließlich zur »Ausübung persönlicher oder familiärer Tätigkeiten« (Art. 2 Abs. 2 Buchst. c DSGVO) tut, muss sich an die Regeln der DSGVO halten[3]. Und um ganz genau zu sein: Wenn Daten von Personen betroffen sind, die sich in der Union befinden, ist dabei egal, ob wir in der EU arbeiten (oder nicht) oder die Verarbeitung in der EU stattfindet (oder nicht) (vgl. Art. 3 Abs. 1 und 2 DSGVO). Da wir in Deutschland arbeiten ist auf uns auch das BDSG-neu anzuwenden, da wir als »nicht öffentliche Stelle« (§ 2 Abs. 4 BDSG-neu)

»Daten im Inland« (§ 1 Abs. 4 Nr. 1 BDSG-neu) verarbeiten. Weil wir »über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten« entscheiden, sind wir »Verantwortliche« (Art. 4 Nr. 7 DSGVO).

Mein Kollege Otto wandte ein, er habe doch nur ein richtiges Adressbuch zum Anfassen und sammle die Visitenkarten seiner Kund*innen in einer Kiste. Aber er schreibt nicht nur die Firmennamen sondern auch die Vor- und Nachnamen seiner Ansprechpartner*innen auf und verarbeitet damit personenbezogene Daten. »Aber da steht doch ›in einem Dateisystem‹ (Art. 2 Abs. 1 DSGVO)« – ja, aber ein Dateisystem muss nicht elektronisch sein. So lange es sich um eine strukturierte Sammlung handelt, die nach bestimmten Kriterien zugänglich ist (Art. 4 Nr. 6 DSGVO) – ein Adressbuch enthält gewöhnlich alphabetisch sortiert Namen und Adressen –, ist die Verordnung anzuwenden. Das nervt vielleicht, aber wir kommen da nicht drum herum.

Dürfen wir personenbezogene Daten verarbeiten?

Nein. Es sei denn, ein Gesetz erlaubt es uns.

Diese Antwort fanden meine Kolleg*innen eher unbefriedigend. Aber ich finde es wichtig, den Grundsatz, der hier sichtbar wird, herauszustellen: Personenbezogene Daten sind schützenswert und ihre Verarbeitung ist nur in engen Grenzen erlaubt.

Für uns sind (soweit wir das derzeit überblicken) drei Regelungen relevant:

- Einwilligung: Die betroffene Person hat der

Verarbeitung für bestimmte Zwecke zugestimmt (vgl. Art. 6 Abs. 1 Buchst. a DSGVO).

- Vertragserfüllung: Die Verarbeitung ist für die Erfüllung eines Vertrags mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen (vgl. Art. 6 Abs. 1 Buchst. b DSGVO).
- Interessenabwägung: Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person überwiegen (vgl. Art. 6 Abs. 1 Buchst. f DSGVO).

In diesen drei Regeln stecken vermutlich mehrere Bände juristischer Literatur[4]. Aber wir lassen das erstmal so stehen.

Dann folgt die Frage nach dem »Wie«: Wie dürfen die personenbezogenen Daten verarbeitet werden? Artikel 5 Absatz 1 DSGVO legt u.a. diese Grundsätze fest:

- Rechtmäßigkeit: Es muss eine Erlaubnis (siehe oben) für die Verarbeitung geben.
- Verarbeitung nach Treu und Glauben.
- Transparenz: Die Verarbeitung muss in einer nachvollziehbaren Weise erfolgen.
- Zweckbindung: Der Zweck oder die Zwecke müssen vorher bestimmt sein.
- Datenminimierung: Nicht mehr Daten als notwendig verarbeiten.
- Speicherbegrenzung: Nicht mehr nötige Daten sind zu löschen.

In Absatz 2 wird bestimmt, dass der

Verantwortliche die Einhaltung dieser Grundsätze nachweisen muss. Und wenn die Verarbeitung auf einer Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO) beruht, muss der Verantwortliche nachweisen können, dass die betroffene Person tatsächlich eingewilligt hat (Art. 7 Abs. 1 DSGVO).

Wir haben also …

Dokumentationspflichten

Hier steckt ein großer Teil der Arbeit, denn neben der Pflicht, Einwilligungen und Datenverarbeitungen zu dokumentieren, müssen wir auch nachweisen können, welche »technischen und organisatorischen Maßnahmen« wir umsetzen, um sicherzustellen, dass die DSGVO eingehalten wird (vgl. Art. 24 Abs. 1 DSGVO). Zusätzlich müssen wir ein Verzeichnis der Verarbeitungstätigkeiten (vgl. Art. 30 DSGVO) führen.

Als ich das meinen Kolleg*innen erzählte, meinte Katharina: »Aber da gibts doch bestimmt Ausnahmen für kleine Unternehmen, oder?!« Zumindest was das Verarbeitungsverzeichnis angeht, gibt es eine Ausnahme – aber die gilt nicht für uns (und vermutlich auch für sonst niemanden). Die Pflicht ein Verarbeitungsverzeichnis zu führen, trifft Unternehmen mit weniger als 250 Mitarbeitenden nicht – das ist schön, aber hier kommen die Einschränkungen (in Art. 30 Abs. 5 DSGVO) –, es sei denn:

- »die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Person« – ohne das juristisch wirklich zu verstehen, ich wäre überrascht, wenn das auf uns zuträfe.

- »die Verarbeitung erfolgt nicht nur gelegentlich« – das ist das Problem: ›gelegentlich‹, was heißt das wohl?
- »es erfolgt eine Verarbeitung besonderer Datenkategorien« (vgl. Art. 9 und Art. 10 DSGVO) – das betrifft uns auch nicht.

Katharina klebte kurz an diesem ›gelegentlich‹: Aber wir schreiben regelmäßig E-Mails und Briefe (in deren Adressen personenbezogene Daten vorkommen), wir verwalten unsere Kund*innenliste, wir betreiben eine Website, deren Besucher*innen mit einer Zugriffsstatistik erfasst werden – es würde mich überraschen, wenn in der Juristerei das alles mit dem Begriff ›gelegentlich‹ umschrieben werden könnte. Und auch Leute mit juristischer Fachkenntnis sehen das so[5].

Na gut, da kommen wir also auch nicht drum herum.

Wir wollen wissen, was mit unseren Daten passiert!

Klingt gut, oder? Ist es grundsätzlich auch – die Frage ist, ob die DSGVO das so geschickt umsetzt, aber bevor sie entweder angepasst oder Gerichtsentscheidungen die Buchstaben des Gesetzes anders auslegen, haben wir folgende Situation:

Um dem Grundsatz der Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO) gerecht zu werden, müssen wir die betroffene Person über die Verarbeitung personenbezogener Daten informieren (vgl. Art. 12, 13 DSGVO). Das ganze muss »in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache« (Art. 12 Abs. 1 DSGVO) passieren.

Damit diese Informationen »leicht zugänglich« sind, bietet es sich an, sie – wie bisher aufgrund der Erfordernisse aus § 13 Telemediengesetz (TMG) – in einer Datenschutzerklärung auf der Website zu veröffentlichen, die wie das »Impressum« nicht versteckt wird, sondern eben »leicht zugänglich« ist.

Das ist der erste, der leichte Schritt (wie wir ihn bei uns ausführen, steht in Teil 2 »Aber was machen wir *konkret*?«). Und dann wird es, nun ja, lästig. Denn bei der Erhebung personenbezogener Daten ist der betroffenen Person »zum Zeitpunkt der Erhebung dieser Daten Folgendes« (Art. 13 Abs. 1 DSGVO) mitzuteilen[6]:

- Name und Kontaktdaten der Verantwortlichen (Buchst. a),
- die Zwecke und die Rechtsgrundlage der Verarbeitung (Buchst. c),
- falls die Verarbeitung auf einer Interessenabwägung beruht (siehe oben), »die berechtigten Interessen, die von dem Verantwortlichen […] verfolgt werden« (Buchst. d) und
- falls die Daten weitergegeben werden: die Empfänger der Daten (Buchst. e).

Na gut, das ist jetzt doch nicht so viel, aber dann kommt Artikel 13 Absatz 2 DSGVO und dort geht es weiter[7]:

- die Dauer der Speicherung (Buchst. a),
- das Bestehen des Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch sowie auf Datenübertragbarkeit (Buchst. b),
- falls die Verarbeitung auf Einwilligung

beruht, das Bestehen des Rechts auf Widerruf der Einwilligung (Buchst. c),
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (Buchst. d) und
- der Hinweis, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die Daten bereitzustellen und welche Folgen die Nichtbereitstellung hätte (Buchst. e).

Nur zur Wiederholung: Diese Informationen sind »zum Zeitpunkt der Erhebung« mitzuteilen. Das heißt, wenn wir von einer neuen potenziellen Kundin angerufen werden und dabei deren Name und Telefonnummer in unsere Kundendatenbank aufnehmen (oder sie in unser Adressbuch schreiben), müssten wir dann nach Artikel 13 DSGVO wirklich Folgendes sagen?!

> Wir, zappo [Agentur für Kommunikation] Hellriegel-Stauder, Hailperin, Kracheel, Landgraf GbR, Scharnhorststr. 25, 10115 Berlin, erreichbar unter der Nummer, unter der Sie uns gerade angerufen haben, 030-2045 0308, erheben Ihren Namen und Ihre Telefonnummer um auszuloten, ob wir mit Ihnen ins Geschäft kommen können, also aufgrund vorvertraglicher Maßnahmen nach Artikel 6 Absatz 1 Buchstabe b der Datenschutzgrundverordnung. Ihre Daten geben wir nicht weiter, eine Übertragung in ein Drittland findet nicht statt. Speichern werden wir Ihre Daten bis sie nicht mehr erforderlich sind; das ist

> entweder, bis zum Vertragsabschluss oder bis klar ist, dass kein Vertrag zustande kommen wird. Sie haben das Recht, Auskunft zu verlangen, Ihre Daten berichtigen, löschen oder deren Verarbeitung einschränken zu lassen sowie der Verarbeitung zu widersprechen. Ebenso haben Sie das Recht auf Datenübertragbarkeit. Sie können sich bei jeder Datenschutzbehörde über die Verarbeitung Ihrer Daten beschweren; für uns zuständig ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit (Friedrichstr. 219, 10969 Berlin, Telefon: 030-138 890). Wir benötigen die Daten, um mit Ihnen in Vertragsverhandlungen eintreten zu können. Sie sind nicht verpflichtet, uns die Daten zur Verfügung zu stellen, dann können wir jedoch keine Vertragsverhandlungen miteinander führen.

Dass das nicht wirklich praktikabel ist, aber nach den Buchstaben des Gesetzes notwendig, sehen auch Datenschutzfachleute so.[8]

Betroffene Personen haben noch weitere Rechte und wir damit Pflichten: Auskunftsrecht (Art. 15 DSGVO und § 34 BDSG-neu), Recht auf Berichtigung (Art. 16 DSGVO), Recht auf Löschung (Art. 17 DSGVO und § 35 BDSG-neu) und Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Diese werden uns vermutlich nur im Einzelfall betreffen, aber wir haben schon mal davon gehört und wissen um ihre Wichtigkeit.

Brauchen wir eine*n Datenschutzbeauftragte*n?

Wenn wir also unsere Dokumentations- und Informationspflichten erfüllt haben (werden), muss sich dann einer von uns noch zur oder zum Datenschutzbeauftragten weiterbilden und knappe Arbeitszeit mit dem Datenschutz verbringen?

In einem bereits verlinkten Artikel heißt es:

> Einen Datenschutzbeauftragten bestellen muss ein Unternehmen nur, wenn sich mindestens zehn Mitarbeiter regelmäßig mit solchen Daten beschäftigen.

Das klingt gut, aber wo findet sich die gesetzliche Grundlage? Artikel 37 DSGVO bestimmt, wann ein*e Datenschutzbeauftragte*r benannt werden muss: Nämlich, wenn es sich

- um eine »Behörde oder öffentliche Stelle« handelt (Abs. 1 Buchst. a),
- die Verarbeitungen »eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen« (Abs. 1 Buchst. b) oder
- die Kerntätigkeit »in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9« oder Artikel 10 DSGVO besteht (Abs. 1 Buchst. c).

Nach der DSGVO brauchen wir also keine*n Datenschutzbeauftragte*n, aber wo kommt die Zahl mit den zehn Beschäftigten her?

Einzelne Normen der Verordnung dürfen die nationalen Gesetzgeber selbst enger fassen. Deshalb müssen wir auch einen Blick in § 38 Abs. 1 BDSG-neu werfen. Danach müssen Verantwortliche (also wir) auch dann eine*n Datenschutzbeauftragte*n benennen, wenn sie

- »in der Regel mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten« beschäftigen (§ 38 Abs. 1 Satz 1 BDSG-neu), oder
- Verarbeitungen vornehmen, »die einer Datenschutz-Folgenabschätzung […] unterliegen« (§ 38 Abs. 1 Satz 2 BDSG-neu), oder
- »personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung […] oder für Zwecke der Markt- oder Meinungsforschung« verarbeiten (§ 38 Abs. 1 Satz 2 BDSG-neu).

Den ersten und der letzten Punkt können wir einfach so auszuschließen, weil wir unser Geschäft kennen. Aber was ist denn bitte eine Datenschutz-Folgenabschätzung?

Und dann noch eine Datenschutz-Folgenabschätzung?!

Jetzt ist es langsam genug, oder? Ich würde jedenfalls gerne dazu kommen, was wir denn eigentlich *machen*, um den Anforderungen der DSGVO und des BDSG-neu gerecht zu werden. Stattdessen noch eine Datenschutz-Folgenabschätzung (DSFA)!

Aber gute Nachrichten, wir machen es uns einfach: Wir haben einen Blick in Artikel 35 DSGVO geworfen und die Stichworte° klingen einfach nicht nach dem, was wir so machen. Wir arbeiten als Designer*innen, Lektor*innen und Texter*innen, wir betreiben Websites auf denen Leute unsere Arbeit sehen und unsere Kontaktdaten aufrufen können – das scheint sehr weit weg von den Anforderungen an eine Datenschutz-Folgenabschätzung. Wir haben uns deshalb entschieden, hier vorerst untätig zu

bleiben.

Wenn wir vermuten würden, dass wir zu einer DSFA verpflichtet sein könnten, etwa weil wir eine datenhungrige App entwickelt haben und vertreiben oder vielleicht ein Webportal betreiben, das Standortdaten verarbeitet, dann würden wir externen Sachverstand anzapfen. (Wer da etwas tiefer einsteigen will und nach Lektüre des Artikel 35 DSGVO am überlegen ist, findet z.B. im Blog des Rechtsanwalts Stephan Hansen-Oest Hinweise zur DSFA mit weiteren Literaturempfehlungen.)

Aber was machen wir jetzt *konkret*?

Die Frage ist: Worüber reden wir eigentlich? Wer nicht die eigenen datenschutzaffinen Freund*innen mit dem Fakt der rechtskonformen Datenverarbeitung und der Freude eines einwandfreien Verfahrensverzeichnisses und der Dokumentation der technischen und organisatorischen Maßnahmen beeindrucken will, der wird vor allem Kummer (= Haftung und Geldbußen) vermeiden wollen.

Kummer kann vor allem dort entstehen, wo von außen sichtbar wird, was nicht rechtskonform läuft. Was dann möglicherweise nicht nur gegen die DSGVO verstieße, sondern auch nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) von Mitbewerber*innen abgemahnt werden könnte. Das ist also die Priorität und daraus ergeben sich (fast) automatisch die anderen Schritte.

Aber wie wir das konkret umsetzen, schreibe ich in einem zweiten Beitrag, denn dazu müssen wir es

ja erstmal machen und das ist im Arbeitsalltag gar nicht so leicht.

---

[1] Das sind alle Daten, die sich auf eine natürliche Person beziehen, also Namen, Adressen, Geburtsdatum, Standortdaten, Online-Kennungen wie IP-Adressen, usw. (vgl. Art. 4 Nr. 1 DSGVO). Manchmal erwähne ich in diesem Beitrag nur »Daten«, aber auch dann meine ich »personenbezogene Daten«.

[2] Damit ist hier (verkürzt) der Umgang mit diesen Daten gemeint, dazu gehört u.a. Daten zu erheben, zu erfassen, zu organisieren, zu ordnen, zu speichern, anzupassen, zu verwenden, zu löschen oder zu vernichten (vgl. Art. 4 Nr. 2 DSGVO). Mit anderen Worten: alles.

[3] Ausnahmen, die es dazu noch geben mag, betreffen uns als kleinere Agentur für Kommunikation nicht.

[4] Was sind ›vorvertragliche Maßnahmen‹ genau, was ist ›erforderlich‹, was sind ›berechtigte Interessen‹ und wie stellt man fest, dass nicht andere Rechte ›überwiegen‹, …?

[5] Siehe z.B. GDD-Praxishilfe DS-GVO V – Verzeichnis von Verarbeitungstätigkeiten, Version 1.0, Stand April 2017; abzurufen in der Liste der Praxishilfen DS-GVO der GDD.

[6] Schaut ruhig selbst in Artikel 13 Absatz 1, denn ich habe mir erlaubt, hier einige Punkte wegzulassen, die für uns nicht relevant sind: Datenschutzbeauftragte*r (Abs. 1 Buchst. b), Übermittlung an Drittländer (Abs. 1 Buchst. f),

[7] Ich habe mir erlaubt, den Hinweis auf automatisierte Entscheidungsfindung einschließlich Profiling (Art. 13 Abs. 2 Buchst. f) wegzulassen.

[8] Nebenbei: Die Kirchen, die ihre eigenen Datenschutzgesetze erlassen, haben das etwas praxisnäher geregelt.

[9] »voraussichtlich ein *hohes* Risiko für die Rechte und Freiheiten natürlicher Personen« (Hervorhebung durch mich; Art. 35 Abs. 1 DSGVO); »systematische und umfassende Bewertung persönlicher Aspekte« (Art. 35 Abs. 3 Buchst. a DSGVO); »umfangreiche Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9« oder Artikel 10 DSGVO (Art. 35 Abs. 3 Buchst. b DSGVO)