Datenschutz in Agenturen

TEIL 2
DATENSCHUTZ UND DIE ANFORDERUNGEN DER DSGVO IN DER AGENTUR UMSETZEN

DATENSCHUTZ IN AGENTUREN

TEIL 2

UMSETZUNG DER DATENSCHUTZ ANFORDERUNGEN IN DEN AGENTUREN

Inhalt

Dieses Whitepaper ist Bestandteil einer Serie von insgesamt drei Beiträgen.

Während sich Teil 1 und der 3. Teil Ader Serie auf die Umsetzung der Anforderungen der Datenschutzgrundverordnung in Agentursoftware konzentrieren, geht es in diesem 2. Teil um das, was Agenturen in Bezug auf den Datenschutz beachten und jetzt umsetzen müssen.

Serie

Die Artikelserie beinhaltet die folgenden Teile:

Teil 1: Worum geht es in der DSGVO, Erklärung wesentlicher Artikel und was müssen demnach Software-Produkte können?
Teil 2: Was müssen Agenturen nun beachten? Beschreibung weiterer Artikel und Schritte zur Umsetzung
Teil 3: Die DSGVO und die Umsetzung durch Software und Anbieter?

Einleitung

Datenschutz ist hierzulande eigentlich nichts Neues. Der Datenschutz in Deutschland wurde (u.a.) im Bundesdatenschutzgesetz geregelt. Und Unternehmen, die sich damit auseinandergesetzt und um die Anwendung und Einhaltung der Gesetze gekümmert haben, werden kaum Probleme mit der Umsetzung der neuen Verordnung haben. Soweit der erhobene Zeigefinger – ist es doch kein Geheimnis und auch nichts Seltenes, dass viele KMU und auch Agenturen hier etwas „verschlafen“ haben.

Dass es jetzt für viele so brisant wird, liegt unter anderem an einer sehr wesentlichen Neuerung der DSGVO gegenüber dem BDSG: Für Verstöße drohen empfindliche Strafen – und zwar das bis zu 66fache früherer Bußgelder! Also jetzt „ran an die Daten“…

Dabei ist für Agenturen die Thematik unter zwei Aspekten zu betrachten: Einerseits die Umsetzung der Anforderungen in der Agentur selbst, also der eigene Umgang mit Daten und andererseits die Berücksichtigung des Datenschutzes im Kundeninteresse (Datenschutzerklärungen auf den Kundenwebsites, Impressuminhalte etc.). In diesem Beitrag geht es um die Agentur-internen Aufgaben.

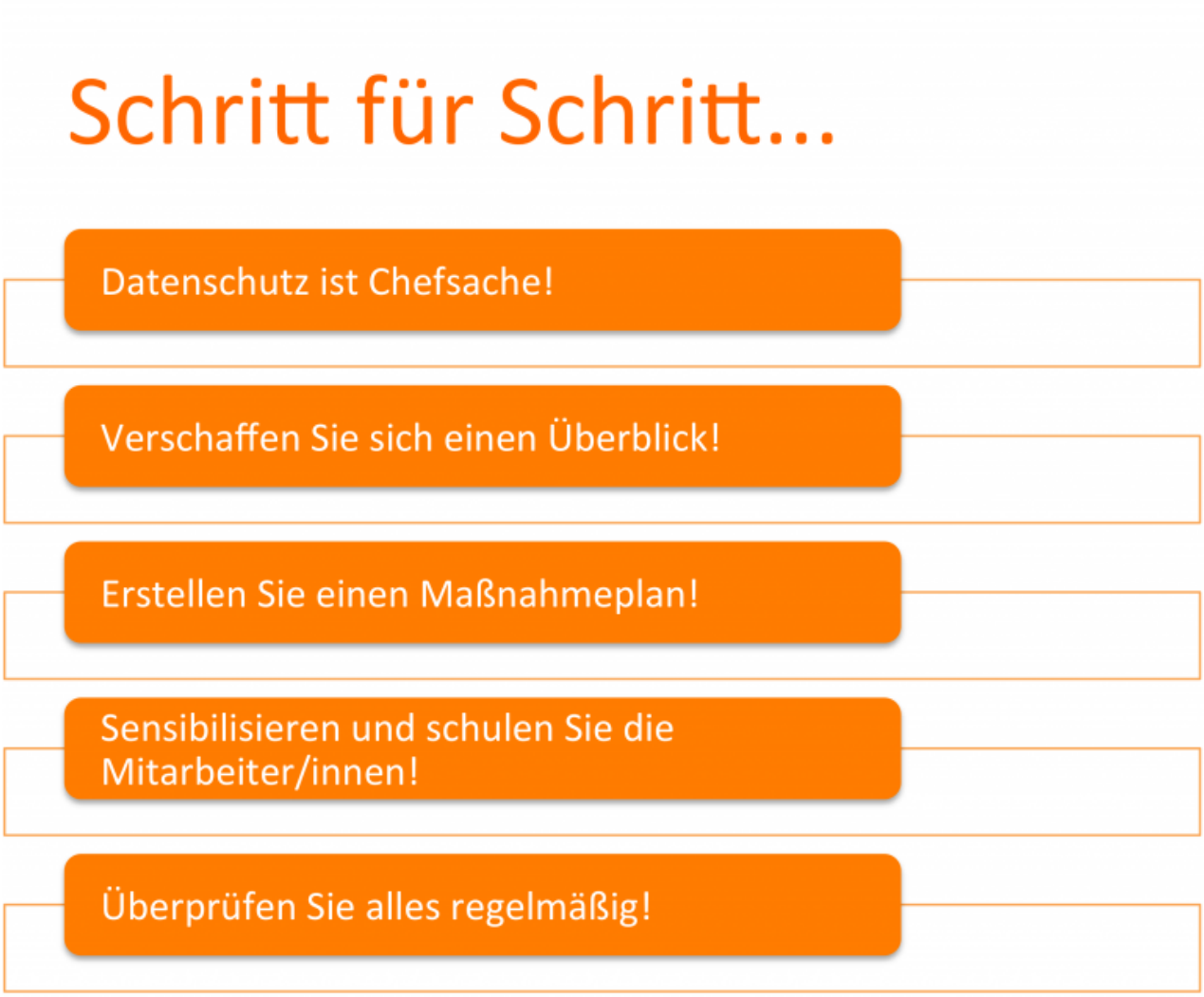
Zusammenfassung der wesentlichen Punkte im unmittelbaren Umgang mit Daten

Im ersten Teil wurden die wesentlichen Aspekte und Artikel aus der Datenschutzgrundverordnung ausführlich dargestellt, die vor allem im Zusammenhang mit dem unmittelbaren Datenhandling und der Nutzung von Software zu berücksichtigen sind.

- „Einwilligung“ (Art.6) und Nachweispflicht (Art.7)
- „Vertraulichkeit“ und „Integrität“ (Art.5)
- Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18)
- Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16)
- Technischer Datenschutz

In diesem Beitrag geht es um die Frage, wie die Umsetzung in der Agentur selbst aussehen kann und welche Aufgaben bewältigt werden müssen.

AUFGABEN FÜR DIE AGENTUREN



1. GRUNDSÄTZLICHE KLÄRUNGEN: WELCHE VERORDNUNGEN GELTEN FÜR DIE AGENTUR?

Selbstverständlich gilt die Einhaltung der Datenschutzgrundverordnung für alle Unternehmen. Gleichzeitig gibt es einige Regelungen, die nicht unbedingt anzuwenden sind – oder bei denen die Vermutung nahe liegt. Bevor an die konkrete Maßnahmenplanung gegangen wird, sollten diese Fragen geklärt sein: Muss ein Verzeichnis erstellt werden? Besteht die Notwendigkeit einer Folgenabschätzung? Brauchen wir eine/n Datenschutzbeauftragte/n?

Verarbeitungsverzeichnis (Art. 30 der DSGVO)

Grundsätzlich müssen nur Unternehmen ein Verarbeitungsverzeichnis (früher „Verfahrensverzeichnis“) erstellen, die mehr als 250 Mitarbeiter/innen beschäftigen. Allerdings – keine Regel ohne Ausnahme – gilt dies nur, wenn in der Agentur …

- nur gelegentlich Daten verarbeitet werden. Hierbei ist zu beachten, dass „gelegentlich“ nicht definiert ist. Ist z.B. ein Gewinnspiel pro Jahr, für das Daten erhoben und verarbeitet werden, gelegentlich oder durch die Regelmäßigkeit schon nicht mehr?

- durch die Datenverarbeitung kein Risiko für die Rechte und Freiheiten der Betroffenen entsteht. Hier ist das Problem der Nachweispflicht.

- keine Daten verarbeitet werden, die unter besondere Datenkategorien gemäß Art. 9 und Art. 10 fallen. Dazu gehören z.B. solche zur ethnischen Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen etc. Auch hier ist die Abgrenzung schwierig und liegt die Beweislast bei der Agentur.

Im Grunde bedeutet dies, dass alle, die Daten verarbeiten, mit der Erstellung eines Verarbeitungsverzeichnisses auf der sicheren Seite sind, denn auch Freiberufler und Klein(st)unternehmen erheben, verarbeiten und nutzen Daten von Mitarbeiter/innen, Kunden und Lieferanten bzw. deren Ansprechpartner/innen, Geschäftspartner, Netzwerk-Kollegen usw. Gut, wenn im Falle einer Prüfung ein – gut gepflegtes – Verzeichnis vorgelegt werden kann! Auch ist es vielleicht sinnvoller, ein Verzeichnis der Verarbeitungstätigkeiten aufzustellen, statt Zeit und Kreativität in die Begründung der Freistellung zu investieren.

Folgenabschätzung (Art. 35)

In einer Datenschutzfolgeabschätzung – im alten BDSG noch „Vorabkontrolle“ genannt – sollen die Risiken der Datenspeicherung für die Persönlichkeitsrechte von Betroffenen eingeschätzt und die Rechtmäßigkeit ihrer Erhebung beurteilt werden. Auch hier liegen die Kategorien nach Art. 9 und 10 zugrunde – sowie die Artikel, die auf die Notwendigkeit und Verhältnismäßigkeit zielen, wie auch die Regelungen zur Datenminimierung und Speicherbegrenzung. Sie ist z.B. notwendig, wenn systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden – wobei auch hier die Definition des Begriffs „umfangreich“ bislang ungeklärt ist – und wenn ein „voraussichtlich hohes Risiko“ mit der Verarbeitung von Daten verbunden ist.

Der Versand eines Newsletter Ihrer Agentur an Interessenten per Email hat voraussichtlich einen geringen Schutzbedarf. Eine Veröffentlichung der Adressen wäre zwar nicht schön, aber für die

Betroffenen auch nicht bedrohlich. Anders liegt der Fall, wenn es sich um den Newsletter an Vereinsmitglieder handelt. Die Urlaubsplanung der Agentur in Excel hat dagegen einen „normalen“ Schutzbedarf. Die Überwachung des Eingangsbereichs per Videokamera einen normalen bis hohen, je nachdem ob z.B. die Bilder aufgezeichnet werden oder nicht.

Datenschutzbeauftragter (Art. 38)

Ein Datenschutzbeauftragter muss bestellt werden, wenn personenbezogene Daten automatisiert verarbeitet werden und wenn mindestens zehn Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Und auch wenn es um besonders sensible Daten geht, wie z.B. Bonitätsprüfung oder Gesundheitsdaten, ist ein Datenschutzbeauftragter notwendig. Die Zahl der Personen enthält auch Teilzeitkräfte, Auszubildende, Trainees und Geschäftsführer.

Dabei steht es frei, ob die Aufgaben intern an einen Mitarbeiter, eine Mitarbeiterin übergeben werden oder ob ein externer Datenschutzbeauftragter bestellt wird. Beides hat seine Vor- und Nachteile: Mitarbeiter/innen kennen die Agentur und die Abläufe bereits, sind mit den Prozessen vertraut. Andererseits kann hier bei Entscheidungen ggf. eher ein Interessenkonflikt entstehen. Zudem ist die Weiterbildung zum Datenschutzbeauftragten kostspielig und zeitaufwendig. Externe Datenschutzbeauftragte bringen hingegen dieses Wissen und Experten-Erfahrung bereits mit und bereichern die Agentur mit einer objektiven Sichtweise.

Fällt Ihnen in diesen drei Fällen die Bewertung schwer, inwieweit was für Ihre Agentur zutreffend ist, sollten Sie auf jeden Fall juristische Beratung in Anspruch nehmen!

2. SAMMLUNG DER DATEN IN DER AGENTUR UND IHRER WEGE

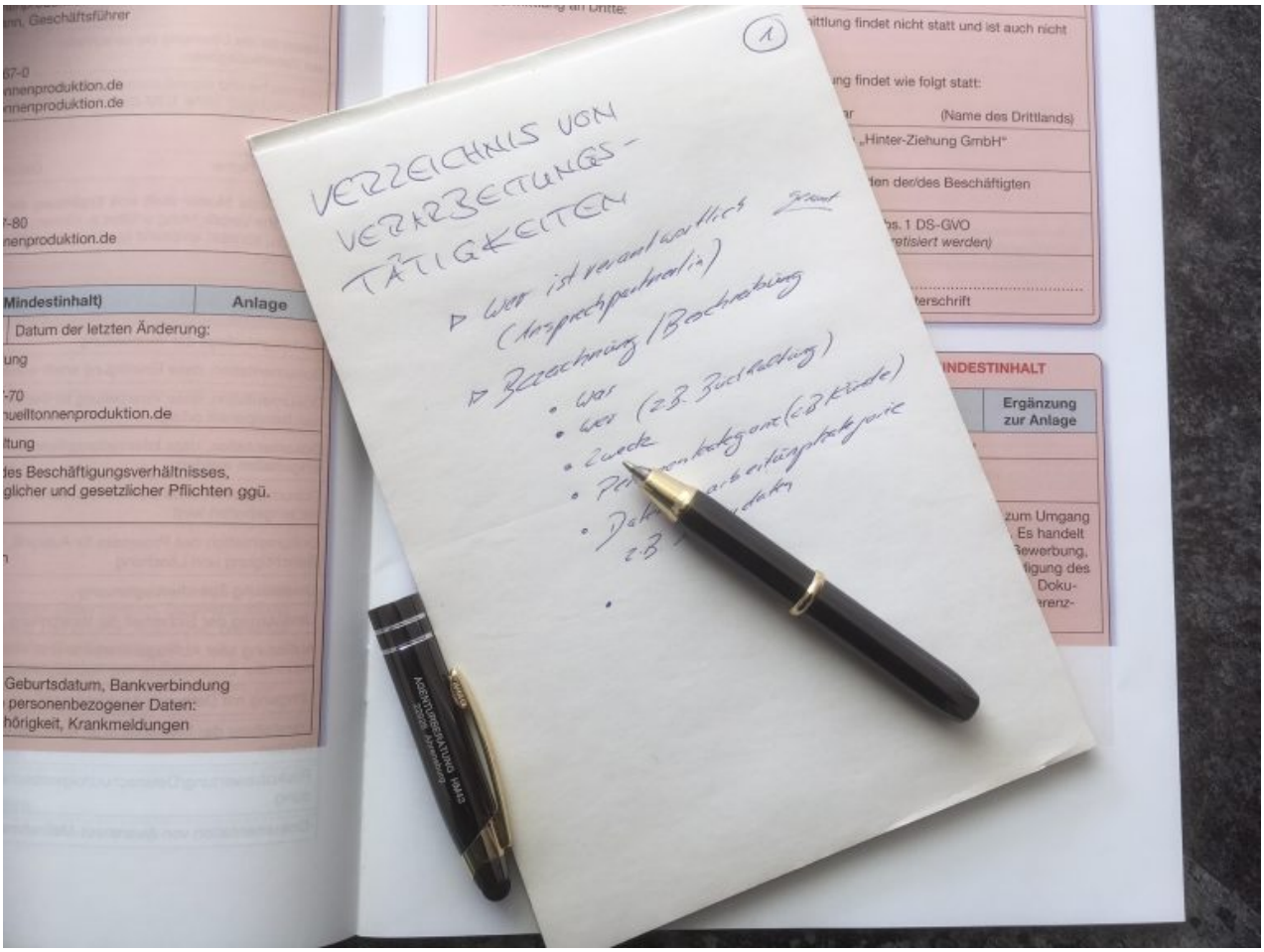
Die wesentliche Aufgabe besteht darin, sich einen Überblick zu verschaffen:

- Welche Daten werden an welcher Stelle von wem und aus welchem Grund und zu welchem weiteren Zweck womit erfasst, wie werden sie verarbeitet und wohin gehen sie eventuell?

Die detaillierte Beantwortung dieser Fragen stellt dann ja im Grunde auch schon die Basis für das Verzeichnis der Verarbeitungstätigkeiten dar.

Betrachtet werden wirklich alle Daten: Die Informationen über Mitarbeiter/innen, Kunden, Lieferanten, Partner, Newsletter-Empfänger, die Kartei von Interessenten… Also alle Daten von

Personen mit denen Sie in irgendeiner Form zu tun haben und deren Daten Sie speichern, verarbeiten, nutzen.



In diese Prüfung werden auch die Wege einbezogen, die die gesammelten Daten gehen oder gehen soll(t)en. Wo werden sie abgelegt oder gespeichert? Sind hier die Zugriffe und Berechtigungen geklärt? Auf welchen Datenträgern werden sie gesichert? Wie sieht es mit dem Backup aus? Kennen Sie die Datenschutzregeln des Cloud-Anbieters? Haben Sie ein Datensicherungskonzept?

Besondere Beachtung findet hierbei – besonders bei Agenturen – die Art und Weise, wie Sie an Daten gelangen und welche verschlungenen Wege Daten – teils ohne Ihr aktives Dazutun – gehen, wenn Daten für das Marketing verwendet werden. Versenden Sie einen Newsletter? Nutzen Sie Google Analytics? Bieten Sie RSS-Feeds an oder lassen Sie zu, dass Besucher der

Website Kommentare abonnieren? Haben Sie die Datenschutzerklärung auf Ihrer Homepage den aktuellen Erfordernissen angepasst?

Prozesse beschreiben

Eine gute Herangehensweise, um sich der Datensammlung bewusst zu werden , ist die Auflistung und Analyse aller Prozesse, bei denen personenbezogene Daten verarbeitet werden. Beschreiben Sie die Prozesse und erstellen Sie Ablaufdiagramme. Spannen Sie den Bogen von der Kundenakquise bis zur Rechnungslegung, von Administration und Buchhaltung und (ggf. je nach Agenturgröße) Personalabteilung bis zur IT. Wie laufen Bewerbungsverfahren? Wie erfolgt die Kundenakquise? Wo landen die Informationen über die Skills der Freelancer? Welche Daten benötigt die Rechnungslegung? Usw.

Da Sie gehalten sind, im Rahmen des Verarbeitungsverzeichnisses die jeweilige Rechtsgrundlage anzugeben, auf deren Basis die Datenverarbeitung erfolgt, ist es durchaus sinnvoll, dies gleich im Rahmen der Prozessbeschreibung zu tun. Dies stellt gleichzeitig eine gute Möglichkeit dar, sich auf diesem Wege mit dem Datenschutz und den Anforderungen der DSGVO auseinanderzusetzen.

Beteiligte und Tools

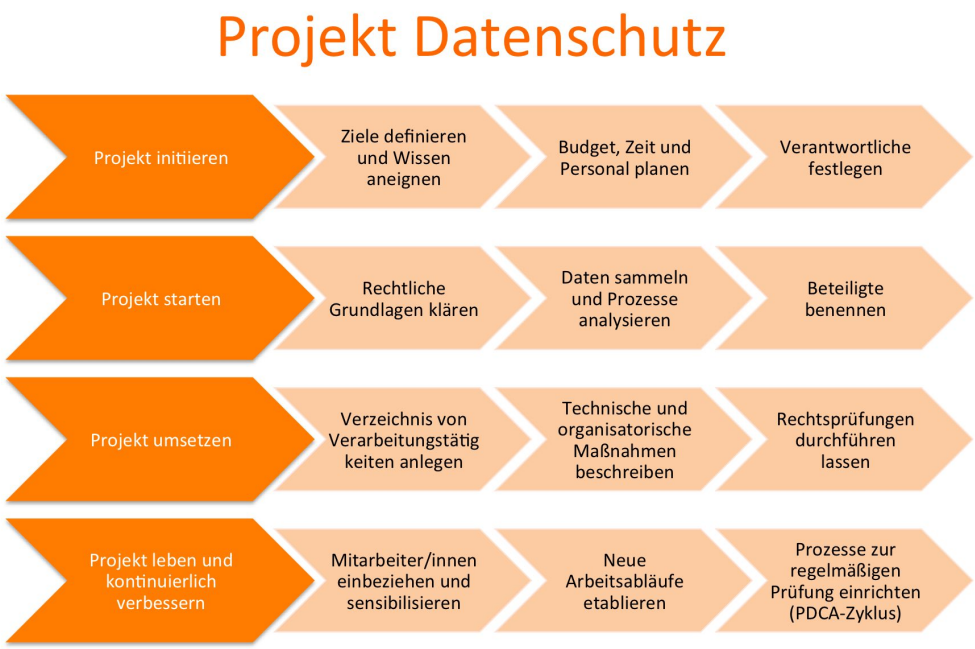
Mit der Sammlung der Daten und der Beschreibung der Prozesse einher geht die Auflistung aller externen und internen Prozessbeteiligten sowie der eingesetzten Tools, Werkzeuge, Verfahren. Werden diese entsprechend benannt, ist es später einfacher, die den Elementen zugehörenden Verträge anzupassen oder zu ergänzen und zu dokumentieren. Hier geht es z.B. um Mitarbeiter/innen und beispielsweise die Vertraulichkeitsverpflichtung, um den Cloudanbieter oder die externe Buchhalterin und die Dienstleistungsverträge, um die Sicherung des Serverraums und das Passwort-Management…

Wer sich ausreichend mit den „W-Fragen“ auseinandersetzt – wer macht was wann womit warum und wie – hat zwar viel Arbeit vor sich, kann die Aufgabe aber um so strukturierter umsetzen. Hier sind die, die bereits ein Zertifizierungsverfahren durchlaufen oder ein Agenturhandbuch erstellt haben, im Vorteil. Ziel ist es, ein Verzeichnis von Verarbeitungstätigkeiten als Basis für das Datenschutz-Management zu erstellen, das dann auch zur Erfüllung der Nachweispflicht dienen kann.

3. AUFGABEN UND VERANTWORTLICHKEITEN FESTHALTEN – PROJEKTPLANUNG

Wie nun kann das Riesenpaket an Aufgaben, das da auf die Agentur zukommt, so in einen Maßnahmenplan übergeleitet werden, dass die Aufgaben agenturgerecht – heißt den stressigen Agenturalltag berücksichtigend – abgearbeitet werden können?

Setzen Sie ein Projekt auf!



Um die Komplexität zu erfassen und in eine geordnete Reihe zu bringen, ist es sinnvoll, ein Projekt „Datenschutz in der Agentur“ zu starten. Dabei spielt es keine Rolle, ob Sie dies mit klassischen oder agilen Methoden tun. Wichtig ist, dass die Aufgaben, Arbeitspakete, Meilensteine benannt und in einem Projektplan visualisiert sowie mit Zuständigkeiten versehen werden.

Am Anfang steht die Aneignung eines soliden Basiswissen, um das Projekt in Angriff nehmen zu können: Wichtige Begriffe und Grundsätze sollten allen, die mit dem Projekt betraut werden sollen, bekannt sein – insbesondere auch der Geschäftsführung, da letztlich sie für die Einhaltung der Vorschriften zuständig ist.

Die nächsten Schritte sind die Zieldefinition und die Planung von Zeit, Budget und Personal. Es ist wichtig, dass Sie sich bewusst machen, dass die Aufgaben nicht neben dem Agenturgeschäft mal eben erledigt werden können. Planen Sie deshalb ausreichende finanzielle und personelle Ressourcen ein.

Die Bestimmung von Zielen geht es natürlich in erster Linie einfach darum, die von den Behörden auferlegten Forderungen umzusetzen. Trotzdem sind weitere Ziele denkbar, beispielsweise kann ein effizienter und gut dokumentierter Datenschutz die Agentur für Geschäftspartner, Kunden und Mitarbeiter attraktiver machen und somit Wettbewerbsvorteile sichern.

Verantwortliche festlegen

Für das Gesamtpaket Datenschutz ist zunächst rein rechtlich gesehen die Geschäftsführung verantwortlich. Für die praktische Realisierung ist die Bestimmung von konkret Verantwortlichen notwendig – damit es nicht geschieht, dass sich in der Agentur niemand direkt verantwortlich fühlt: Wer hat die Pflicht, welche Aspekte der DSGVO umzusetzen? Diese Zuständigkeiten werden am Besten im initialen Datenschutz-Kickoff-Workshop namentlich benannt, festgelegt und im Agenturhandbuch hinterlegt.

Grundsätzlich ist eine geteilte Zuständigkeit sinnvoll und die Bestimmung einer Koordinatorin/eines Koordinators empfehlenswert. Wie sehr die Verantwortlichkeit gesplittet werden muss, kommt natürlich auf die Größe der Agentur an und welche Management-Aufgaben von wem erledigt werden. Gibt es z.B. eine eigene Personalabteilung, ist diese für die Einhaltung des Mitarbeiter-Datenschutzes zuständig etc.

Unabhängig davon ist zu klären, ob die Agentur eine/n Datenschutzbeauftragte/n – egal ob intern oder extern – bestellen muss. Siehe hierzu auch den Beitrag im Blog „Brauchen Sie einen Datenschutzbeauftragten?“

Wobei die Verantwortlichkeit des Datenschutzbeauftragten nicht mit der oben angesprochenen Koordinationsfunktion verwechselt werden sollte, da laut DS-GVO Datenschutzbeauftragte nicht mehr die operativen Aufgaben (wie Schulungen oder Vorabkontrollen) verantworten, sondern die Stellung eines Kontrollorgans einnehmen. Kern der Rechtsstellung des/der Datenschutzbeauftragten ist seine/ihre Unabhängigkeit.

Splitten Sie die Aufgaben und Zuständigkeiten der Agenturgröße angemessen. Während in einem kleinen Designbüro die Funktion eines Datenschutz-Managers ausreichend ist, sollte eine 50-Mitarbeiter-Agentur ein Datenschutz-Team einsetzt werden.

Projektstart und -umsetzung

Auf die beiden zum Projektstart gehörenden wesentlichen Aufgabenpakete „Rechtliche Grundlagen klären“, „Daten sammeln, Prozesse beschreiben“ und „Beteiligte benennen“ wurde im letzten Teil bereits ausführlich eingegangen.

Sind diese Tätigkeiten umgesetzt, haben Sie bereits eine gute Grundlage, um nun das Verzeichnis von Verarbeitungstätigkeiten anzulegen und auch die technischen und organisatorischen Maßnahmen (TOM) zu beschreiben.

Zu den umzusetzenden Maßnahmen gehören dann all die, die damit einhergehen: Die Anpassung der Verträge mit zum Beispiel Ihrem Cloud-Anbieter, der externen Buchhalterin, den Freelancern und festen Mitarbeiter/innen beispielsweise oder die Anpassung der Datenschutzerklärung auf Ihrer Website, neue Passwort-Vorgaben oder auch die Prüfung Ihrer Agentursoftware auf datenschutzrechtliche Anforderungen… Möglicherweise ergibt die Datensammlung ja auch, dass Sie gar nicht von allen, deren Daten Sie erhoben haben, das Einverständnis haben und müssen dies nun ggf. nachholen.

4. MITARBEITER SCHULEN UND SENSIBILISIEREN

Damit der Datenschutz in der Agentur gelebt werden kann, ist eine sehr wesentliche Aufgabe in der nächsten Projektphase „Projekt leben und kontinuierlich verbessern“ die Schulung und Sensibilisierung aller Mitarbeiter/innen.

Alle Mitarbeiter/innen müssen die Grundsätze des Datenschutzes kennen! Deshalb ist eine Grundlagen-Schulung, in der diese Grundsätze thematisiert werden, unumgänglich. Bei der tiefergehenden Schulung muss dagegen nicht nach dem Gießkannen-Prinzip vorgegangen werden. Vielmehr ist es wichtig die Mitarbeiter/innen entlang ihrer Zuständigkeitsbereiche und Aufgaben (Personal, Buchhaltung, Beratung, IT etc.) in der Agentur geschult werden und sich auskennen.

Die Grundsätze werden in Kapitel 2 DSGVO, Artikel 5 bis 11 definiert. Auf einige Prinzipien wurde im 1. Teil der Serie mit den Themen „Einwilligung“ (Art.6) und Nachweispflicht (Art.7), „Vertraulichkeit“ und „Integrität“ (Art.5), Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18) sowie Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16) bereits eingegangen.

Bleiben noch – und sind gerade für die Mitarbeitersensibilisierung besonders bedeutsam – die Grundsätze Datenminimierung, Zweckbindung und Richtigkeit (alle Art. 5), sowie die Grundsätze der „Verarbeitung besonderer Kategorien personenbezogener Daten“ (Art. 9) und „Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist“ (Art. 11).

Datenminimierung

Wesentlich ist hier vor allem das Prinzip der Datenminimierung. Dies bedeutet, dass nur diejenigen Daten verarbeitet werden dürfen, die für den (definierten) Zweck notwendig sind und nicht darüber hinausgehen. Die Erfassung und Nutzung personenbezogener Daten muss auf das notwendige Maß beschränkt werden.

Datenschutz beginnt mit der Überlegung, welche Daten eigentlich für die Geschäftstätigkeit wirklich erforderlich sind und welche Sorgfalt ihrer Sammlung und Nutzung geboten ist. Leider stehen nicht wenige auf dem verbreiteten Standpunkt, dass mehr besser ist als weniger, selbst dann, wenn es für das Mehr keine wirkliche Notwendigkeit gibt.

Bietet die Agentur einen Newsletter an, so ist im Grunde nur die E-Mail Adresse erforderlich. Soll aus Gründen der personalisierten Ansprache auch Anrede, Titel, Vorname und Nachname erfasst werden, muss die ausdrückliche Einwilligung zur Speicherung und Verarbeitung eingeholt werden – zusätzlich zur Information, wofür und wie lange die Daten gespeichert werden.

Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Verarbeitung der Daten muss also einem eindeutigen Zweck dienen und die Daten dürfen nur für diesen konkreten Zweck verwendet werden. Diese Zwecke müssen bereits bei der Erhebung personenbezogener Daten festgelegt sein.

Beispielsweise dürfen Sie Liefer- und Rechnungsadressen speichern und für den konkreten Fall der Lieferung von Waren oder der Zustellung Ihrer Rechnung verarbeiten – allerdings dürfen Sie diese Daten nicht ohne ausdrückliche Einwilligung für den Versand Ihrer Imagebroschüre verwenden.

Richtigkeit

Die verwendeten Daten müssen sachlich richtig sein und ggf. auch auf dem neuesten Stand, wenn dies für den Verarbeitungszweck erforderlich ist. Dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Richtigkeit bedeutet nichts anderes als dass die erhobenen Daten den Tatsachen entsprechen müssen. Gleichzeitig ist dafür Sorge zu tragen, dass die Daten auf dem neuesten Stand sind und dass falsche oder fehlerhafte Daten korrigiert oder gelöscht werden.

Besondere/sensible Daten

Die Erhebung und Verarbeitung sog. sensibler Daten ist nur unter den in Artikel 9 bezeichneten besonderen Voraussetzungen erlaubt. Unter sensiblen Daten werden alle Informationen verstanden, aus denen „die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen“ sowie „genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“.

Erlaubt ist deren Verarbeitung nur bei entsprechender ausdrücklicher, explizit auf die Verarbeitung der konkret zu benennenden Daten bezogenen Einwilligung oder in den sonstigen sehr restriktiv auszulegenden Fällen (z.B. im Zusammenhang mit dem Arbeitsrecht, dem Recht der sozialen Sicherheit bzw. dem Sozialschutz, dem Schutz lebenswichtiger Interessen, Gesundheitsvorsorge usw.).

Hier ist eine Sensibilisierung besonders notwendig, da die Datenerfassung diskriminieren kann, outen oder vor anderen bloß stellen. Teils können sogar physische, materielle oder immaterielle Schäden, für den Betroffenen entstehen.

Ob eine Mitarbeiterin der römisch/katholischen Kirche angehört, ist prinzipiell für die Ausübung ihrer Tätigkeit unerheblich, darf allerdings in der Lohnbuchhaltung erfasst werden, da es für die Berechnung der Kirchensteuer notwendig ist. Unterhalten sich Mitarbeiter/innen über einen Kunden und dessen Zahlungsmoral, so kann dies – je nach Öffentlichkeit und Zusammenhang – z.B. bei einem kleinen Unternehmen erhebliche Folgen durch Rufschädigung zeitigen. Deshalb gehört diese Information – aus ggf. der Agentursoftware – auch nicht in die allgemeinen Stammdaten des Kunden und dürfen lediglich einem bestimmten Personenkreis (z.B. Buchhaltung, Beratung) zugänglich gemacht werden.

Identifizierung

Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

Bei der Datenverarbeitung muss geprüft werden, ob ein Personenbezug und damit die Identifizierbarkeit der betroffenen Person für die Verarbeitungszwecke erforderlich ist: Daten sollen nur so lange in einer die Person identifizierenden Weise gespeichert werden dürfen, wie es für die Verarbeitungszwecke erforderlich ist.

Gleichzeitig ergibt sich aus dem Gebot der Datenminimierung und der Speicherbegrenzung nicht nur ein Wegfall der Verpflichtung der weiteren Speicherung der Identifizierungsdaten, sondern eine konkrete Verpflichtung zur Löschung.

Wird also die Zeiterfassung eines Mitarbeiters lediglich zum Zwecke der Aufwandschätzung oder Rentabilität gespeichert, ist die namentliche Auswertung unnötig und nicht zulässig. Das Stundenprotokoll eines Minijobers allerdings muss für den Nachweises der Einhaltung des Mindestlohns namentlich gespeichert werden.

Rechenschaftspflicht

Der/die Verantwortliche ist für die Einhaltung der in Artikel 5 DSGVO Abs. 1 genannten Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können.

5. REGELMÄßIGE ÜBERPRÜFUNG! (PDCA)

Die Frage der regelmäßigen Überprüfung ist keine Frage des eigenen Bewertungsmaßstabes, wann eine erneute Kontrolle ansteht. Vielmehr sieht die DSGVO an mehreren Stellen vor, dass Sie Ihren Datenschutz, dessen Organisation und Dokumentation und somit auch Arbeitsabläufe regelmäßig überprüfen. Vor allem immer dann, wenn sich daran etwas ändert oder Sie neue Prozesse einführen. Wird also z.B. ein neues Tool für die Zeiterfassung eingeführt, müssen die entsprechenden Änderungen im Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden.

„Der Verantwortliche setzt … geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.“

Hier wird im Wesentlichen ein PDCA-Zyklus (Plan– Do–Check–Act) oder kontinuierlicher Verbesserungsprozess (KVP) beschrieben, der dafür sorgt, dass Ihr Datenschutz laufend angepasst, verbessert und geprüft werden muss.

- **Planen (plan):** Vor der Umsetzung wird der Prozess geplant bzw. das Thema eingegrenzt und beschrieben und die Maßnahmen inkl. Verbesserungspotential und –ziel geplant.

- **Durchführen (do):** Hier werden die Maßnahmen terminiert, durchgeführt und dokumentiert.

- **Überprüfen (check):** Die in der vorhergehenden Phase erzielten Ergebnisse werden zusammengefasst und überprüft und ggf. visualisiert.

- **Agieren/verbessern (act):** Der sich aus den vorherigen Phasen ergebende Prozess wird in der Agentur eingeführt (als Standard festgelegt) und regelmäßig auf Einhaltung überprüft.

Viel Erfolg bei der Umsetzung!