Datenschutz in Agenturen

TEIL 1
DIE EU-DATENSCHUTZGRUNDVERORDNUNG UND IHRE AUSWIRKUNGEN AUF UNTERNEHMENSSOFTWARE

DATENSCHUTZ IN AGENTUREN

TEIL 1 DIE EU-DATENSCHUTZGRUNDVERORDNUNG UND IHRE AUSWIRKUNGEN AUF UNTERNEHMENSSOFTWARE

Einleitung

Die neue Datenschutzgrundverordnung ist eines genau nicht mehr, nämlich neu. Trotzdem beginnen viele Unternehmen und auch Agenturen erst jetzt, sich mit den Aufgaben, die diese Verordnung mit sich bringt, auseinanderzusetzen. Hier kommt auf manche noch ein großes Stück Arbeit zu – vor allem auf die, die bisher Datenschutz als etwas eingestuft haben, das nur für „große" Firmen gilt und die sich das Bundesdatenschutzgesetz eher beiläufig angesehen haben. Dies gilt teilweise auch für Software-Anbieter, die sich gerade um die neuen Regelungen des Datenschutzes und deren Auswirkungen auf funktionale Anforderungen noch nicht in Gänze gekümmert haben.

Inhalt

In dieser Artikelserie wird den folgenden Fragen nachgegangen:

- Worum geht es und was müssen Software-Produkte können? (Teil 1)
- Was müssen Agenturen nun beachten? (Teil 2)
- Welche Funktionen bietet welche Agentursoftware? (Teil 3)

Im ersten Teil geht es schwerpunktmäßig um diejenigen Bestimmungen der Verordnung die für die Umsetzung in entsprechenden Software-Produkten relevant sind, z.B. das „Recht auf Löschung". Der zweite Teil wird dann die Bestimmungen näher beleuchten, die sich strukturell und organisatorisch auf die Agentur auswirken werden, wie beispielsweise die Regelung zur Datenminimierung. Hier geht es hauptsächlich um den Umgang mit Daten im Agenturalltag und weniger um die Auswirkungen im Marketing. Hierzu gibt es anderes aussagekräftiges Material. Zudem haben die Agenturen an dieser Stelle schon recht genau hingesehen. Der dritte Teil wird das Ergebnis einer zwischenzeitlich bei den Anbietern von Agentursoftware laufenden Befragung zur Umsetzung der Anforderung in ihren Produkten vorstellen.

ES IST SOWEIT!

Zwei Jahre hatten Unternehmen Zeit, die neue Datenschutzverordnung umzusetzen, nun tritt sie in Kraft. Ab dem 25. Mai 2018 gelten zwei grundsätzliche Regelungen für den Datenschutz:

- Die EU-Datenschutzgrundverordnung (DSGVO-EU) und
- das novellierte Bundesdatenschutzgesetz, das als Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) in Kraft treten wird.

Eine Besonderheit der Verordnung dürfte ursächlich damit zu tun haben, dass jetzt um die Umsetzung gerungen wird: Für Verstöße drohen empfindliche Strafen – und zwar das bis zu 66fache früherer Bußgelder!

GRUNDSÄTZLICHES STATEMENT

Zunächst ein grundsätzliches Statement: Auch, wenn manche die Folgen, die die Umsetzung der Anforderungen des Datenschutzes mit sich bringen, störend oder lästig empfinden (und auch, wenn er an manchen Stellen noch nicht tief genug greift): Es ist gut, dass es ihn gibt!

Gerade im Zuge von „Big Data“ einerseits und Globalisierung andererseits gewinnt Datenschutz zunehmend an Bedeutung. Der Schutz persönlicher Daten ist im Informations-Zeitalter unerlässlich und stellt ein wesentliches und grundrechtlich verbürgtes Grundrecht dar. Gleichzeitig sind Datenschutz und Datensicherheit auch im wirtschaftlichen Zusammenhang unerlässlich und können sogar einen Qualitäts- und Wettbewerbsfaktor bedeuten.

UM WAS GEHT ES?

Ganz allgemein geht es im neuen Gesetz bzw. der neuen Verordnung um eine Stärkung der Verbraucherrechte und explizit um den Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ über „Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.“ (Art.1) Kurz gesagt, um unser aller Recht auf Privatsphäre und informationelle Selbstbestimmung.

Dieser Schutz gilt auch für die Erhebung persönlicher Daten im B2B Bereich, insbesondere im Kontakt mit Ansprechpersonen von Geschäftspartnern – Kunden wie Lieferanten und andere Partner – wie auch der eigenen Mitarbeiter/innen. Diese Daten werden in den unterschiedlichsten Bereichen von Unternehmens- bzw. Agentursoftware erhoben. In diesem ersten Teil der Artikelserie

sollen all die Bestimmungen betrachtet werden, die eine funktionale Umsetzung in Software erfordern.

Wenn Sie im Folgenden bestimmte neue Anforderungen nicht finden, wie z.B. Datenminimierung oder Meldepflicht, dann deshalb, weil diese Bestimmungen keine Auswirkung auf Unternehmens-/ Agentursoftware haben. Sie sind Gegenstand des 2. Teils der Serie (siehe oben).

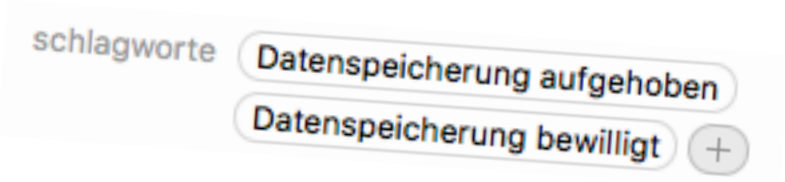
THEMA „EINWILLIGUNG" (ART.6) UND NACHWEISPFLICHT (ART.7)

Worum geht es?

Werden in der Agentur personenbezogene Daten gespeichert, muss dazu die Einwilligung der betroffenen Person vorliegen. Diese Einwilligung muss schriftlich dokumentiert sein und durch die Agentur auch nachgewiesen werden können. Wichtig ist also die Dokumentation der Einwilligung in die Datenverarbeitung. Dies kann über Kategorien oder sog. „Tags", besser über Notizen am Datensatz oder durch gespeicherte Dokument der Einwilligung erfolgen.

Ebenfalls genehmigungspflichtig ist die Weitergabe von Daten an Dritte. Etwa an einen externen Dienstleister für den Versand eines Mailings oder den Export einer Teilnehmerliste.

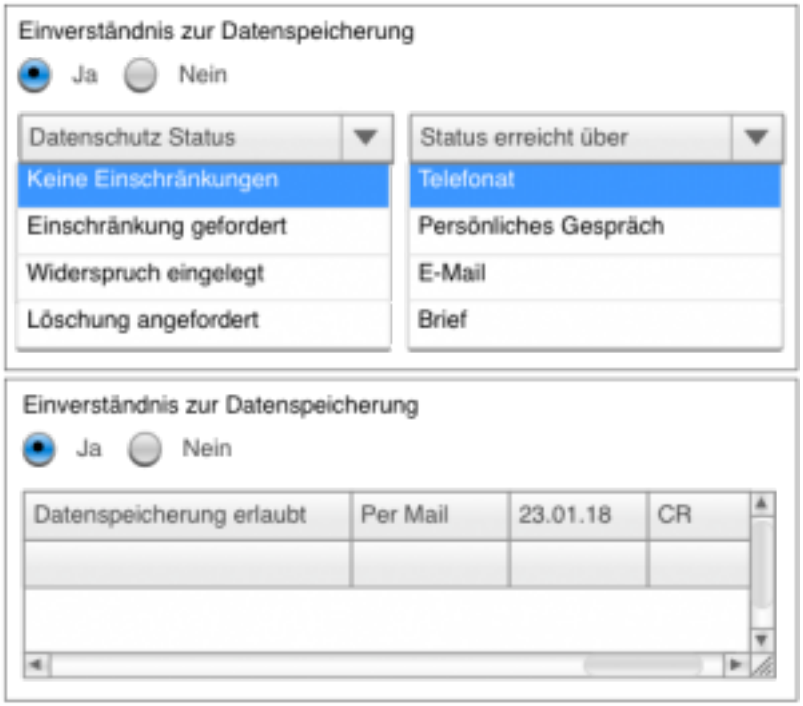
Die Einwilligung in die Datenspeicherung impliziert das Recht auf Widerruf.



Was bedeutet das für die Software?

Hier werden gleich mehrere – vermutlich für die meisten Produkte neue – funktionale Anforderungen angesprochen. Erforderlich sind:

- Möglichkeiten zur Bestimmung der gegebenen Einwilligung
- Möglichkeit zum Entzug der gegebenen Einwilligung
- Hinterlegung von Zeitpunkt und Art der gegebenen Einwilligung
- Festhalten des aktuellen Status der Person

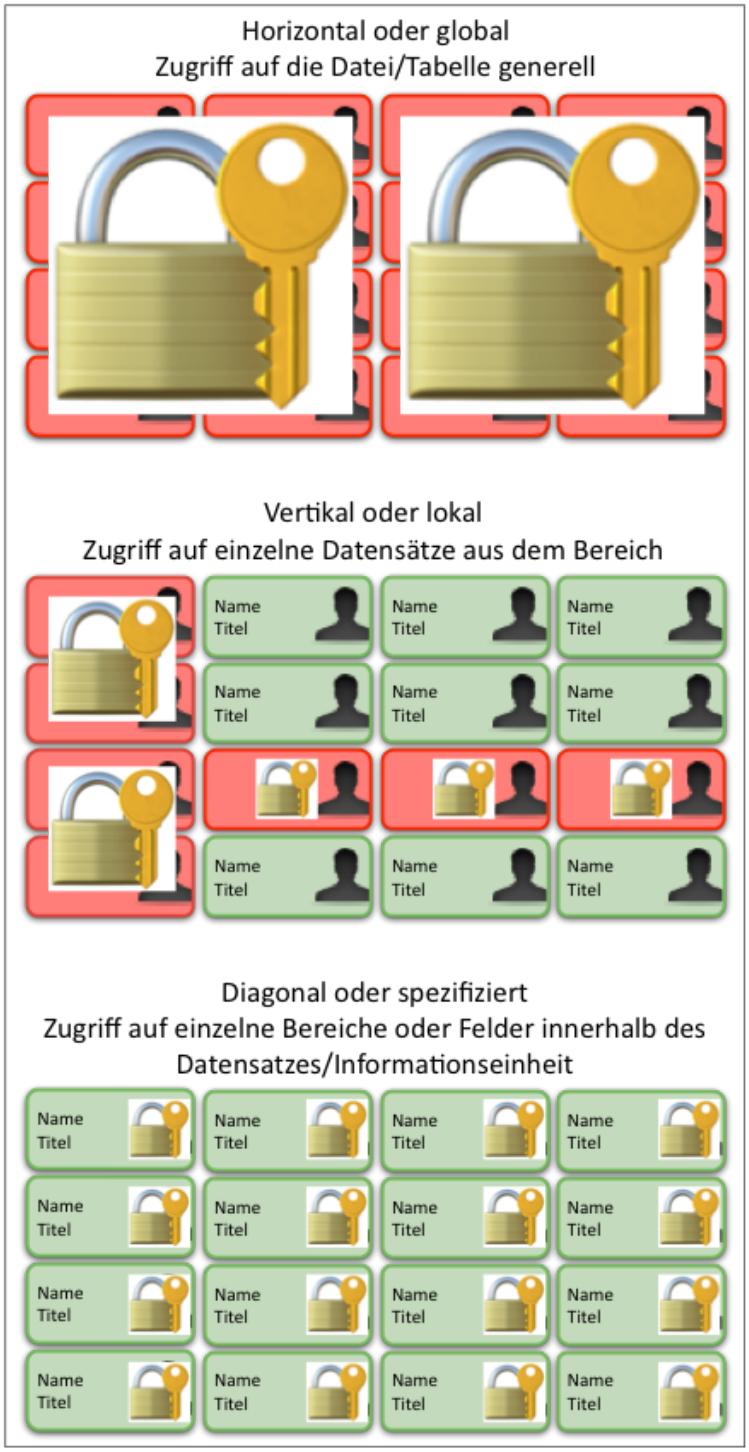


Letzteres ist vor allem wichtig für das Filtern von Personendatensätzen, um beispielsweise einen Mailingverteiler zu erstellen. Weshalb meines Erachtens das Festhalten entsprechender Status-Informationen in „Schlagwort-Wolken“ oder über Tags zwar für eine Übergangsphase denkbar ist, aber auf Dauer nicht ausreichend sein dürfte.

Die Umsetzung könnte beispielsweise erreicht werden über…

- Checkboxen, über die gekennzeichnet wird, ob die Person ihre Zustimmung gegeben hat
- Felder mit Datum und Art, da ggf. ein Nachweis darüber erbracht werden muss
- Auswahlfeld für den Status
- Fortlaufendes Feld zur Protokollierung von Änderungen

THEMA „VERTRAULICHKEIT" UND „INTEGRITÄT" (ART.5)

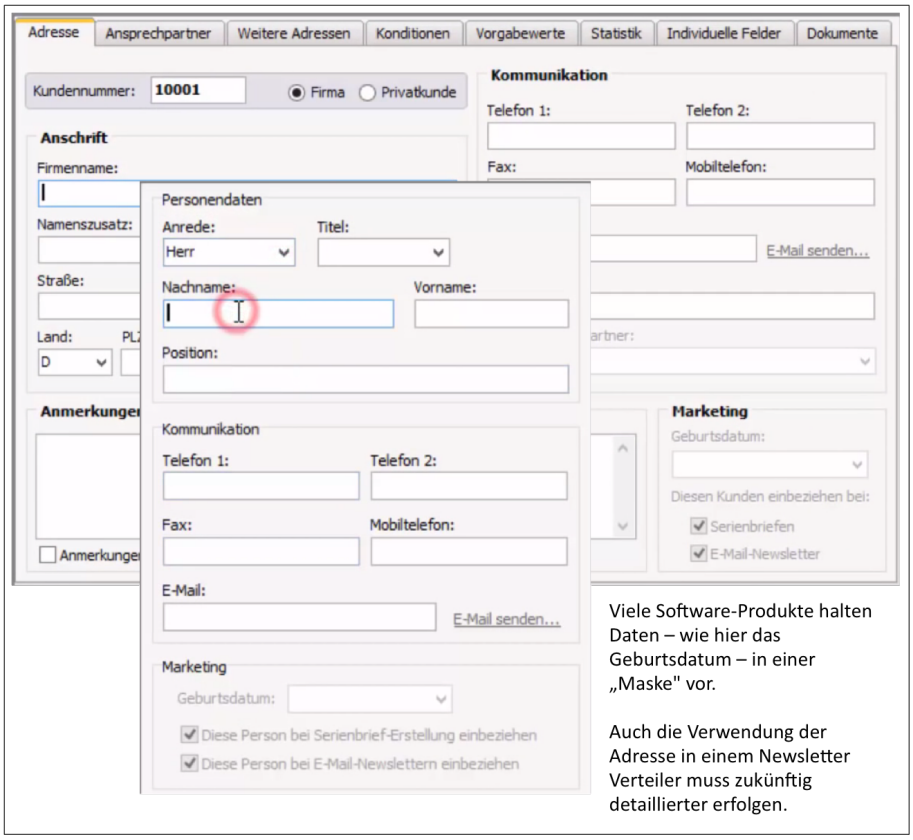


Worum geht es?

Die in der Agentur gespeicherten Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit gewährleistet wird. Hier ist sowohl der Schutz vor (un-)bewusstem Zugriff als auch vor (un-)beabsichtigtem Verlust oder Zerstörung der Daten angesprochen.

Was bedeutet das für die Software?

Zunächst müssen erhobene Daten vor unbefugtem Zugriff geschützt werden. Hier werden viele unterschiedliche Funktionen angesprochen, die sich auf die Rechtesystematik der Software auswirken. Die Systeme müssen Mechanismen zur Verfügung stellen, die verhindern, dass unberechtigte Personen Daten einsehen können, die dem Datenschutz unterliegen. Das System muss dafür geeignete Berechtigungskonzepte vorweisen können, die den Zugriff, das Löschen, die Weiterverarbeitung innerhalb und den Export regulieren (privacy by design).



Viele Software-Produkte halten Daten – wie hier das Geburtsdatum – in einer „Maske" vor.

Auch die Verwendung der Adresse in einem Newsletter Verteiler muss zukünftig detaillierter erfolgen.

Im Prinzip wird hier die Notwendigkeit eines horizontalen, eines vertikalen und eines diagonalen Rechtekonzepts angesprochen. Es sollte also nicht nur möglich sein, eine Tabelle für Anwender komplett zu sperren, sondern auch einzelne Datensätze einer Tabelle. Beispielsweise alle Personen, die ein VIP-Kennzeichen haben. Während diese beiden ersten Varianten in den meisten Systemen bereits vorhanden sind oder sein sollten, wird das zusätzlich notwendige Zugriffsrecht für manche Anbieter eine Herausforderung darstellen: die Möglichkeit, sensible von unsensiblen Daten zu trennen.

So halten viele Software-Lösungen CRM-Daten lediglich in einer Ebene/einem Fenster bereit, so dass nicht zwischen sensiblen und weniger sensiblen Daten unterschieden wird, geschweige denn mit einem spezifischen Zugriffsrecht belegt werden können.

Die oben genannten Berechtigungskonzepte sollen laut DSGVO auch als Voreinstellungen vorhanden sein. Beispielsweise in Form von Rollen-Berechtigungen. Wird dann ein neuer User in der Datenbank angelegt, sollte sichergestellt sein, dass Daten erst dann gesehen werden können, wenn eine Rolle mit entsprechend hinterlegten Berechtigungen zugewiesen worden ist. Vorher darf es keinerlei Zugriffsmöglichkeiten auf (personenbezogene) Daten geben. (privacy/data protection by default).

Datum	Uhrzeit	AP	Aktion
01.12.17	10:15	Carlotta M.	Datensatz archiviert
16.03.14	13:03	Sarah Y.	Straße geändert
11.04.10	15:44	Renate L.	Rechnung Nr. xxx
20.12.09	11:56	Christian H.	zum Verteiler Weihnachtspost hinzugefügt
09.09.09	09:10	Sabine S.	Auftragsabwicklung
26.06.09	08:22	Christian H.	Angebot versendet
23.06.09	17:34	Christian H.	Anfrage über Webformular

Um den Weg der Daten auch innerhalb eines Nutzungsrechtes kontrollieren zu können, wäre das Protokollieren diesbezüglicher Änderungen zwar nicht zwingend notwendig, aber eine gute zusätzliche Funktion.

THEMA DATENSPEICHERUNG: BEGRENZUNG UND LÖSCHUNG (ART.5, 17, 18)

Worum geht es?

Wurden Daten nun mit Erlaubnis erfasst und dafür gesorgt, dass nur Berechtigte Zugriff auf sie haben, ist sicherzustellen, dass Daten nur so lange gespeichert werden, wie es für den Verarbeitungszweck notwendig ist und gelöscht werden, wenn dies verlangt wird oder eben durch Wegfall des Nutzungszwecks angezeigt ist.

An diesem Punkt wird besonders deutlich, warum die Vorordnung nur ebendies ist und kein gemeingültiges Gesetz. Denn sog. „Öffnungsklauseln“ erlauben den Bezug auf spezifische Länderrechte innerhalb der EU – z.B. fiskalische Aufbewahrungsfristen. Eine Person kann nicht komplett gelöscht werden, wenn die Daten noch für andere Zwecke gesetzlich gefordert vorgehalten werden müssen.

Bedeutsam ist an dieser Stelle auch, dass in der Verordnung – anders als im deutschen Datenschutzgesetz der Begriff der „Sperrung“ auftaucht. Denn im obigen wie auch im folgenden Fall kann es begründet sein, einen Personendatensatz nicht zu löschen, sondern nur zu sperren. Nehmen wir an, Sie haben Adressen eingekauft um einen Mailingversand durchzuführen. Nun meldet sich Herr X mit der Bitte um Löschung seiner Daten, was Sie auch unverzüglich erledigen. Irgendwann kaufen Sie wieder Adressen für einen weiteren Versand – und die vermeintlich gelöschte Adresse ist wieder enthalten, was Herrn X nicht sehr freuen dürfte. An dieser Stelle wäre also eine Datensatzsperrung mit einem entsprechenden Vermerk weitaus sinnvoller…

Was bedeutet das für die Software?

Datensätze sollten also gelöscht und gesperrt werden können. Hier gilt es einige Hürden in der Software-Entwicklung zu nehmen. Denn es geht nicht nur um die Löschung eines Personendatensatzes aus beispielweise einer Tabelle mit Ansprechpersonen Ihrer Kunden. Sondern auch um die Beseitigung der „Spuren“, die diese Person ggf. in der Software hinterlassen hat, also z.B. Backups, Links etc..

In der Software müssen Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, entfernt, andere archiviert und wieder andere gesperrt werden können. Um den beschriebenen unterschiedlichen Aspekten Rechnung tragen zu können, ist die Schaffung einer Daten-Anonymisierung angezeigt.

Dies betrifft natürlich auch Mitarbeiter-Daten. Hier unterliegen z.B. ggf. An- und Abwesenheitsdaten einer Aufbewahrungsfrist, während es möglich sein muss, andere Daten unverzüglich zu löschen.

Datum	Uhrzeit	AP	Aktion
23.07.17	10:15	Carlotta M.	Datenspeicherung geändert auf "Löschung"
05.11.14	13:03	Sarah Y.	Straße geändert
01.12.12	15:44	Renate L.	Handynummer geändert
12.02.10	17:34	Christian H.	zum Verteiler Weihnachtspost hinzugefügt
12.02.10	17:34	Sabine S.	Hausnummer geändert
12.02.10	17:34	Christian H.	Straße geändert
12.02.10	17:34	Christian H.	Geburtsdatum erfasst

Anforderungen:

- Grundsätzlich ist es also gut, wenn die geforderte Löschung bei der Person vermerkt werden kann (siehe oben).
- Verwendete Daten aus dem Personendatensatz in anderen Bereichen können gelöscht oder anonymisiert werden. Beispielsweise der Verweis auf einen Ansprechpartner in einer Kontakthistorie, wie sie in CRM-Bereichen von Software gängig ist.
- Gesperrte Personendaten dürfen nicht mehr nutzbar und einsehbar sein.
- Eine Protokoll-Funktion zeichnet Änderungen am Personendatensatz – also auch Sperr-Vermerke und dergl. – auf.
- Ein denkbarer technischer Lösungsansatz für den Spagat zwischen Löschung und Aufbewahrungsfrist der Personendaten könnte sein, Vermerke über die Archivierung, Löschung oder Sperrung einer Person in einer – grundsätzlich gesperrten – gesonderten Tabelle („Blacklist") zu speichern. Hierdurch könnte auch der Gefahr eines nicht mehr aktuellen Informationsstands durch die Notwendigkeit einer Backup-Einspielung begegnet werden.
- Nach personenbezogenen verbundenen Datensätzen (Kontaktbericht, Memo, gespeicherte Emails…) muss gesucht werden können, um sie zu löschen.

THEMA INFORMATION/AUSKUNFT UND TRANSPARENZ (ART.5, 12, 13, 15, 16)

Worum geht es?

Auskunft über gespeicherte personenbezogene Daten	
Name	Schäfer
Vorname	Christian
Titel	
Funktion im Unternehmen	Projektleiter
Straße/Nummer	Alte Landstraße 22
PLZ/Ort	12345 Musterstadt
Telefonnummer	
Mobilnummer	0175 123456
Telefon privat	
Geburtsdatum	22. Nov. 74
Pers. Anrede	Lieber Christian

Jede/r Betroffene hat ein Informationsrecht, das über die Risiken, Vorschriften und Rechte im Zusammenhang mit der Verarbeitung seiner/ihrer Daten aufgeklärt. Unternehmen müssen dokumentieren wie personenbezogene Daten erhoben, verwendet und verarbeitet werden. Das berührt an dieser Stelle ggf. die Information über die Datenhaltung in Cloudsoftware. Möglicherweise ist hier ein Zertifikat oder Datenschutzsiegel des Anbieters hilfreich.

Hinzu kommt ein Auskunftsrecht darüber, welche Daten gespeichert und (wofür) genutzt werden. Hier schließt sich das Recht auf Korrektur der Daten an., da eine Korrektur ja eine vorherige Einsichtnahme der bestehenden Daten voraussetzt. Meldet sich also ein Geschäftspartner mit der Bitte um entsprechende Auskünfte bei Ihnen, sollten Sie diese Informationen liefern können.

Was bedeutet das für die Software?

Aus der Software kann ein Dokument erstellt werden, das die personenbezogenen Daten zusammenfasst und an den oder die Betroffene gesendet werden kann.

THEMA TECHNISCHER DATENSCHUTZ

Worum geht es?

Sehr viele der Anforderungen setzen entsprechende Datenverarbeitungssysteme voraus. IT-Systeme müssen so ausgelegt sein, dass die Einhaltung der DSGVO möglich ist. Dies belangt die bereits angesprochenen Anforderungen an Zugriffsregelungen „Privacy by Design“ und Privacy by Default“, angesprochen sind jedoch auch alle Konzepte die dazu führen geeignet sind, für die Sicherheit der Daten allgemein zu sorgen.

Was bedeutet das für die Software resp. für den Umgang mit ihr?

Diese Anforderung hat viele unterschiedliche Aspekte:

- „Datenschutz“ meint den Schutz vor unbefugtem Zugriff. Dazu gehören die oben angesprochenen Maßnahmen in der Software, um Daten sicher zu bewahren und zu nutzen. Allerdings gehört dazu auch der sorgsame Umgang mit deren Speicherung und Pflege. Hier sind sowohl mobile Zugriffe durch Nutzer/innen angesprochen wie auch die Wartung und Pflege durch Software-Anbieter oder –Entwickler. Natürlich ist hier auch der Anbieter gefragt, wobei die Agentur als Verantwortliche in den Verträgen auf diesbezügliche Passagen achten müssen.

- Unter „Datensicherheit“ lassen sich allgemein Datensicherungskonzepte (Backup-Systeme etc.) subsumieren wie auch die sichere Verwahrung der Daten auf externen Serversystemen (Hosting, Cloud, externes Daten-Backup usw.). Die Konzepte haben insbesondere dafür Sorge zu tragen, dass Daten nicht in falsche Hände geraten. Auch hier sind sowohl Sie wie auch die Anbieter von Hosting-Services angesprochen. Achten Sie auf eine Datenhaltung auf deutschen oder mind. EU-Servern und auf eine ausreichende Zertifizierung des Hosting-Anbieters.

Der Artikel hat gezeigt, dass die Anforderungen des Datenschutzes auch an Software-Systeme nicht trivial sind. Viele Anbieter werden mit deren Umsetzung in ihren Systemen und der baldigen Lieferung eines entsprechenden Updates zu kämpfen haben. Es liegt natürlich in Ihrem ureigenen Interesse, hier nachdrücklich auf eine datenschutzkonforme Version Ihrer Software oder mindestens auf eine klare Terminierung dafür zu dringen. Den aktuellen Stand Ihres Systems können Sie beim Anbieter erfragen oder im 3. Teil einsehen.

Wichtig an dieser Stelle erscheint mir der zusätzliche Hinweis, dass „Management by Excel“ zukünftig keine Option mehr sein kann. Doch dazu mehr in einem weiteren Beitrag hier im Agentur | Software | Magazin.

In den beiden nächsten Folgen geht es um Datenschutz in der Agentur und die Umsetzung der Anforderungen an den Datenschutz in unterschiedlicher Agentursoftware. Senden Sie mir gerne Ihre Fragen dazu oder schreiben Sie einen Kommentar!