PSP
MÜNCHEN

White Paper

Datenschutz durch Technikgestaltung

Was muss eine Software leisten?

Autor: Dr. Axel-Michael Wagner

[September 2018]

ZUSAMMENFASSUNG

Dieses White Paper widmet sich der Frage, wie Softwarehersteller die Anforderung eines Datenschutzes durch Technikgestaltung in Software-Features ummünzen können, die letztlich auch als Mehrwert und damit Verkaufsargument nutzbar sind. Denn je mehr die Einhaltung der DSGVO-Anforderungen an unternehmensinterne Prozesse durch Software unterstützt wird, desto mehr werden diese Prozesse rationalisiert, ihre Kosten gesenkt und ihre Verlässlichkeit gesteigert.

PSP
MÜNCHEN

Inhalt

- Was hat ein Softwarehersteller mit Datenschutz zu tun?
- Anhand welcher Kriterien muss der Verantwortliche seine Entscheidung treffen?
- Was bedeutet das nun in der Praxis?
- Wie kann eine Software datenschutzfreundlich ausgestaltet werden?
- Beispielsfälle
  - Metadaten/„Track Record“
  - Kapselung und granulare Berechtigungskonzepte
  - Übermittlung in ein Drittland
  - Löschfristen und „Legal Hold“
  - Bearbeitung von Auskunftsrechten
  - Datenübertragbarkeit
  - Einwilligung/Koppelungsverbot
- Schlusswort

Einleitung

Seit dem 25. Mai 2018 gilt die **EU-Datenschutzgrundverordnung** (**DSGVO**). Viele Vorgaben der DSGVO bieten erheblichen Interpretationsspielraum. Eine solche vage Vorgabe lässt sich aus Art. 25 Abs. 1 DSGVO im Hinblick auf Software entnehmen, mit der personenbezogene Daten verarbeitet werden. Die Botschaft kann plakativ so zusammengefasst werden: „Software soll möglichst datenschutzfreundlich sein“. Das würde wohl jeder intuitiv auch angemessen finden: Wenn es datenschutzrechtliche Vorgaben gibt und heutzutage große Teile unseres (Arbeits- und Privat-) Lebens virtuell „in“ Software-Umgebungen stattfinden, dann sollte doch wohl schon die Software-Umgebung möglichst viel Datenschutz leisten und dadurch die „Bediener“ von den Mühen befreien, bei der Anwendung einer Software über die Auslegung von Datenschutzvorschriften nachsinnieren zu müssen. Wenn man allerdings über die eine oder andere App, Social Media Plattform oder in Unternehmen genutzte Software datenschutzrechtlich vertieft nachdenkt, kommt man nicht selten zu der Einschätzung, diese Software so, wie sie ist, besser nicht zu benutzen, weil man sie kaum benutzen kann, ohne dass irgendjemand gegen Datenschutzrecht verstößt.

Der Europäische Gerichtshof entschied etwa im Juni 2018, dass der Betreiber einer Facebook Fanpage alleine durch das Betreiben dieser Fanpage für Datenschutzverstöße (mit-) haftet, die Facebook in Form mangelnder Aufklärung der Benutzer über ihre Tracking-Methoden begeht. Die Entscheidung beruht übrigens noch auf der Vorgängerregelung der DSGVO, einer EU-Richtlinie zum Datenschutz aus dem Jahr 1995, welche von der DSGVO „nur" weiterentwickelt wurde. Die datenschutzrechtliche „gemeinsame Verantwortlichkeit" für Fehler der Plattform-Software von Facebook – entweder wurde der Benutzer zu viel getrackt oder er wurde zu wenig aufgeklärt – bestand, ohne dass der Fanpage-Betreiber wissen konnte, was Facebook eigentlich genau macht. Hier wurde, wie man es unter der Geltung der DSGVO sagen würde, durch den Fanpage-Betreiber schon im Vorfeld zu wenig „Datenschutz durch Technikgestaltung" betrieben: Die für die Fanpage eingesetzte Software von Facebook war nicht datenschutzfreundlich genug, im Gegenteil, ihre Anwendung verstieß gegen geltendes Datenschutzrecht. Man mag es für übertrieben halten, einem „einfachen" Fanpage-Betreiber solche „Vorfeld"-Pflichten zur rechtlichen und technischen Prüfung der von ihm eingesetzten Mittel für die Verarbeitung personenbezogener Daten aufzubürden, aber das Stadium, in dem man versuchen könnte, solche Pflichten – also die Gesetze – zu ändern, ist erst einmal vorbei. Die vom Europäischen Gerichtshof entschiedene „gemeinsame Verantwortlichkeit" des Plattform-Betreibers und des Betreibers des Angebots auf der Plattform für Datenschutzverstöße – als Folge eines unbedachten Einsatzes der Plattform – bestand schon seit 1995, als es Facebook noch gar nicht gab; es hatte nur zwischenzeitlich niemand den Europäischen Gerichtshof danach befragt.

Was hat ein Softwarehersteller mit Datenschutz zu tun?

Adressat von Art. 25 DSGVO ist nicht der Softwarehersteller, sondern derjenige, der personenbezogene Daten verantwortlich verarbeitet („Verantwortlicher"). Das bedeutet aber nur auf den ersten Blick, dass der Softwarehersteller „nichts machen muss". Schließlich trifft der Verantwortliche Beschaffungsentscheidungen, und wenn sich ein Verantwortlicher zwischen der datenschutzfreundlichen Software A und der nicht ganz so datenschutzfreundlichen Software B entscheiden muss, dann gibt ihm die DSGVO die Richtung vor. In der Sprache der DSGVO heißt das, dass der Verantwortliche „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung [...] geeignete technische [...] Maßnahmen [...] trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze [...] wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen". Das ist es, was man umgangssprachlich als „datenschutzfreundlich" bezeichnet. Wir kommen später noch darauf zurück, was genau das für die Ausgestaltung einer Software bedeutet. Man erkennt aber hier bereits, dass diese Pflicht des Verantwortlichen erhebliche Folgewirkungen für den Softwarehersteller, d. h. für die Ausgestaltung der Software und letztlich auch für den Verkaufserfolg, haben muss.

Anhand welcher Kriterien muss der Verantwortliche seine Entscheidung treffen?

So wie „Datenschutzfreundlichkeit" kein Schwarz-/Weiß-Begriff, sondern ein sehr langgezogener Graukeil ist, so liegt es auch bei der Verpflichtung des Verantwortlichen, „der datenschutzfreundlichen Software" den Vorzug zu geben. Diese Pflicht besteht nicht unter allen Umständen, sondern der Aufwand, der vom Verantwortlichen betrieben werden muss, muss im Verhältnis zum Nutzen stehen. Das drückt die DSGVO – sonst wäre es nicht die DSGVO – durch eine sehr abstrakte Begriffskette aus, nämlich „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen". Nachfolgend soll diese Formel etwas genauer untersucht und für die Praxis aufbereitet werden.

Stand der Technik

Bei „Stand der Technik“ geht es natürlich um die datenschutzrechtlich relevanten Aspekte, nicht darum, ob die Benutzeroberfläche neusten Ästhetik-Anforderungen genügt. Was diese Aspekte sind, wird weiter unten noch eingehender behandelt. Da bislang bei der Strukturierung von Software wenig bis gar nicht auf „Datenschutzfreundlichkeit“ geachtet wurde, dürfte der diesbezügliche Stand der Technik derzeit noch häufig gering sein; es ist also noch genügend „Luft nach oben“. Was genau im Bereich bestimmter Softwaretypen wie DMS-System, ERP-System, CRM-System, Personalverwaltungssoftware, Buchhaltungssoftware, Apps, Social Media Plattformen etc. der „Stand der Technik“ ist, kann durchaus schwierig zu bestimmen sein. Wenn ein Anbieter vorprescht und bestimmte Funktionen implementiert, bildet dann der Rest des Marktes nicht mehr den „Stand der Technik“ ab? Umgekehrt lässt sich zumindest festhalten, dass Verantwortliche, die Software nutzen, die jedenfalls nicht mehr dem Stand der Technik entspricht, im Falle einer Auseinandersetzung mit den Datenschutzaufsichtsbehörden oder vor Gericht einen schweren Stand haben werden. Und je mehr datenschutzfreundliche Funktionen in gängige Software integriert werden, desto deutlicher werden ältere Versionen und andere Produkte dem Stand der Technik „hinterherhinken“.

Implementierungskosten

Neben dem Stand der Technik spielen die Implementierungskosten eine weitere Rolle. Kostet die datenschutzfreundliche Software A fünfmal so viel wie die nicht gleichermaßen datenschutzfreundliche Software B, kann das ein schlagendes Argument sein, dennoch B anzuschaffen, ohne gegen Art. 25 DSGVO zu verstoßen. So drastisch wird der Unterschied in der Praxis aber meist nicht sein. Die Beantwortung dieser Frage kann natürlich durch völlig unterschiedliche Lizenzmodelle erschwert sein, durch unterschiedliche Anwendungsszenarien (on-premise vs. Cloud), durch unterschiedlichen Customizing-Aufwand und durch unterschiedliche Möglichkeiten, die günstigere Software durch individuelle Zusatzentwicklungen auf ein datenschutzfreundlicheres Niveau zu heben. Hingegen wird die Argumentation mit den Implementierungskosten immer dann schwierig, wenn die Software vom Verantwortlichen selbst entwickelt wird (etwa bei der App-Entwicklung): Hier liegt keine Situation vor, in der ein Verantwortlicher auf dasjenige Angebot begrenzt ist, „das der Markt hergibt“. Die Pflicht zur Prüfung bei der Beschaffung wird hier zur unmittelbaren Pflicht, die eigene Software von vornherein datenschutzfreundlich auszugestalten, denn der Softwareentwickler ist hier selbst der datenschutzrechtlich Verantwortliche.

Art, Umfang, Umstände und Zwecke der Verarbeitung

Weiter sind Art, Umfang, Umstände und Zwecke der Verarbeitung personenbezogener Daten einzubeziehen. Es liegt etwa auf der Hand, dass ein Verantwortlicher mehr um die Datenschutzfreundlichkeit der von ihm eingesetzten Software bemüht sein muss, wenn er damit Millionen oder Milliarden von Datensätzen, die personenbezogene Daten enthalten, verarbeitet, als wenn es um eine Excel-Liste mit fünf Adressen zur wöchentlichen Brotauslieferung geht. Dasselbe gilt für die Umstände (z. B. Einsatz von Cloud-Lösungen in Drittstaaten) und Zwecke (z. B. Ermöglichung von Scoring-Bewertungen oder automatisierten Entscheidungen). Letztlich geht es hier, wie auch beim nachfolgenden Punkt, um eine Abwägung der mit der späteren Datenverarbeitung verbundenen Risiken.

Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Die „Eintrittswahrscheinlichkeit und Schwere" der Risiken für die „Rechte und Freiheiten" der betroffenen Personen, die der Datenverarbeitung innewohnen, verlangen explizit eine Abwägung zwischen Nutzen und Risiko. Welche Rechte und Freiheiten genau gemeint sind, wird von der DSGVO nicht weiter erläutert. Letztlich geht es darum, welchen Schaden das „Abhandenkommen" personenbezogener Daten (d. h. diese gelangen in die Hände von „Unbefugten") oder eine sonstige „Datenpanne" auslösen kann, d. h. eine solche Offenlegung, Verarbeitung oder Weitergabe der Daten, die nicht der DSGVO entspricht. Es sind also die möglichen Datenschutzverletzungen zu bestimmen, die durch die Software mit verursacht werden können, und diese dann zu gewichten. Das können intuitiv einleuchtende Fälle sein, etwa das – zunächst unerkannte – „Absaugen" von Log-In-Daten von Accounts oder Kundenprofilen und die Verwendung der im Account befindlichen Daten (z. B. Kreditkartendaten) zu Zwecken der finanziellen Schädigung und des Identitätsdiebstahls. Wie der eingangs geschilderte Facebook-Fall zeigt, kann auch ein exzessives, nicht ausreichend dokumentiertes Tracking des Benutzers ebenso einen „worst case" bilden. Auch Verzögerungen bei der Bearbeitung von Betroffenenrechten, etwa wenn der Betroffene Auskunft über seine personenbezogenen Daten verlangt, die vom Verantwortlichen verarbeitet werden, und der Verantwortliche diese Daten nicht in angemessener Zeit in seinen Systemen lokalisieren kann, können relevant sein.

Was bedeutet das nun in der Praxis?

Letztlich lassen sich diese viel- oder auch wenigsagenden Elemente zu der Formel zusammenfassen: Je schlimmer die Auswirkungen eines Datenschutzverstoßes sind, der innerhalb einer Software-Umgebung oder sonst von Software verursacht wird, desto mehr muss in Software investiert werden, die solche Datenschutzverstöße verhindert. Wo hier die Grenze genau liegt, ist jedoch völlig offen – der Schwarze Peter wurde hier erst den Verantwortlichen, dann (im Streitfall) den Gerichten zugeschoben. Man kann sich über diese „Schwammigkeit" vielleicht mit der Einsicht hinwegtrösten, dass eine Verletzung dieser Regelung „nur" das halbe Maximal-Bußgeld der DSGVO nach sich zieht, also EUR 10 Mio. oder, falls dies mehr ist, 2 % des weltweiten Gruppenumsatzes. Aber auch im Angesicht dieser Sanktion wird eine Risikoabwägung in den meisten Fällen wohl dazu führen, „im Zweifel" noch eine Nummer sicherer zu gehen, selbst wenn man eigentlich als Verantwortlicher überzeugt ist, das Richtige getan zu haben. Denn wenn doch ein software-vermittelter Datenschutzverstoß eintritt, wird eine Behörde oder ein Gericht aufgrund allgemeiner psychologischer Grundsätze („Nachher ist man immer schlauer") immer behaupten können, dass man genau diesen Verstoß hätte vorhersehen und durch bessere Technikgestaltung vermeiden müssen.

Wie praxisrelevant ist nun überhaupt eine solche Pflicht des Verantwortlichen, auf möglichst datenschutzfreundliche Technik setzen zu müssen? Mangels einschlägiger Gerichtsurteile zur DSGVO lässt sich diese Frage auf zweierlei Arten beantworten. Einerseits könnte es sein, dass insbesondere dann, wenn eine Datenschutzverletzung stattgefunden hat und die Ursache dafür untersucht wird – etwa im Rahmen eines Audits –, die datenschutzfreundliche Ausgestaltung der eingesetzten technischen Systeme im Zentrum stehen kann. Steht die Datenschutzverletzung, wie dies in der Praxis oft der Fall sein wird, nämlich im Zusammenhang mit dem Einsatz von Software, wirft dies unmittelbar die Frage auf, ob die Software geeignet und richtig eingerichtet war, um Datenschutzverstöße zu verhindern. Dabei ist auch mit einzubeziehen, dass die Beweislast, die DSGVO eingehalten zu haben, beim Verantwortlichen liegt. Andererseits könnte es sein, dass es kein einziges Gerichtsurteil geben wird, in dem je ein Verstoß gegen Art. 25 DSGVO festgestellt wird, weil der Fokus der zuständigen Behörden und der initiierten gerichtlichen Verfahren auf denjenigen Regelungen der DSGVO liegt, die den primären Verstoß betreffen. Erteilt der Verantwortliche etwa eine falsche Auskunft auf ein vom Betroffenen geltend gemachtes Auskunftsrecht hin, so liegt eine – mit dem Maximal-Bußgeld bewehrte – Verletzung der Betroffenenrechte vor; ob diese durch nicht datenschutzfreundliche Software,

nachlässige Mitarbeiter oder andere Umstände verursacht wurde, ist dann zunächst einmal weniger relevant. Zudem können und müssen technische Maßnahmen, die Datenschutzverstöße verhindern, aber unverhältnismäßig aufwendig oder am Markt nicht vorhanden sind, durch organisatorische Maßnahmen beim Verantwortlichen kompensiert werden. Ein Datenschutzverstoß ist also nie „nur" ein Problem der nicht datenschutzfreundlichen Software bzw. zwangsläufig ursächlich darauf zurückzuführen, sondern immer ein Problem des zugehörigen Gesamtkomplexes von technischen und organisatorischen Maßnahmen (TOMs), mithin der Prozesse und Kontrollen in ihrer Gesamtheit, beim Verantwortlichen.

Am Rande soll auch noch erwähnt werden, dass es Juristen gibt, die der Meinung sind, die Verpflichtung zu Datenschutz durch Technikgestaltung sei – kurz gesagt – unwirksam bzw. irrelevant. Denn hierdurch würden dem Verantwortlichen (sog. präventive „Vorfeld"-) Pflichten zu einem Zeitpunkt aufgebürdet, zu dem er noch gar keine personenbezogenen Daten verarbeitet hat, sodass das Datenschutzrecht hier noch gar nicht eingreifen dürfe. Das wäre so ähnlich wie die Verpflichtung, nur stumpfe Messer zu erwerben, damit Menschen gar nicht erst durch scharfe Messer zu Schaden kommen können. Wenn aber die Verarbeitung personenbezogener Daten erst einmal begonnen hat, müsse der Verantwortliche ohnehin sämtliche Datenschutzregelungen und –grundsätze einhalten, gleich, ob er dies mit datenschutzfreundlicher oder datenschutzfeindlicher Technik umsetzt. Aufgrund der datenschutzrechtlichen Dokumentationspflichten gehe es daher beim Datenschutz durch Technikgestaltung um das Protokollieren der Planung und Weiterentwicklung des verwendeten Datenverarbeitungssystems, nicht aber um dessen inhaltliche Ausgestaltung. Man darf gespannt sein, wie solche „aushebelnden" Juristen-Argumentationen dereinst vor Gericht (und auf hoher See) durchschlagen, aber bis dahin sei aus Erwägungsgrund 78 zur DSGVO zitiert: „In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen."

Wie kann eine Software datenschutzfreundlich ausgestaltet werden?

Es ist also letztlich unklar, in welchen Fällen genau welche Intensität von Bemühen um datenschutzfreundliche Software durch den Verantwortlichen gefordert wird und wie relevant diese Pflicht in der Praxis ausfällt. Wie so häufig gerät dadurch die Frage, mit welchen ggf. „provisorischen" Lösungen geltendes Recht eingehalten wird, zur Risikoabwägung des Verpflichteten, in die auch sein „Kostenbewusstsein" einfließt. In dieser Situation ist es daher vorteilhaft, wenn dem Verpflichteten Software angeboten werden kann, die für sich in Anspruch nimmt, genau diese Pflicht zum Datenschutz durch Technikgestaltung praktisch „von selbst" zu erfüllen.

Selbst wenn aber die spezifische Verpflichtung, Datenschutz durch Technikgestaltung zu betreiben, vom Verantwortlichen mit den obigen Argumenten als in der Praxis irrelevant abgetan wird, ist datenschutzfreundliche Software gleichwohl aus einem anderen Grund für den Verantwortlichen wichtig. **Denn je mehr Datenschutzaktivität durch Software unterstützt und schrittweise „automatisiert" wird, desto mehr werden die entsprechenden Prozesse rationalisiert, deren Kosten gesenkt und die Verlässlichkeit gesteigert.**

Zwar führen, wie oben bereits angedeutet, für den Verantwortlichen häufig verschiedene alternative Wege zur DSGVO-Konformität. Die DSGVO sieht „technische und organisatorische Maßnahmen" vor. Kurz gesagt sind organisatorische Maßnahmen Anweisungen an Mitarbeiter, während technische Maßnahmen Vorkehrungen (bzw. bestimmte Ausgestaltungen) im Bereich von Hard- und Software sind. In gewissen Grenzen sind organisatorische und technische Maßnahmen kommunizierende Röhren, d. h. man kann eine bestimmte Maßnahme zur datenschutzkonformen Verarbeitung oder zur Abschirmung der Daten gegen nicht datenschutzkonforme Verarbeitung alternativ organisatorisch oder technisch fassen. Daraus folgt vordergründig, dass nicht alles „vollautomatisierte" Datenschutz-Compliance durch Software sein muss. Dazu ein einfaches Beispiel: Man kann den Zugang zu einem PC mit personenbezogenen Daten mit einem Anmeldepasswort beschränken (technische Maßnahme) oder ein 24-Stunden-Wachpersonal beschäftigen, das die strikte Anweisung hat, nur denjenigen an den PC zu lassen, der dem Wachmann das richtige Passwort ins Ohr flüstert (organisatorische Maßnahme). Aber dennoch: Je mehr ein Unternehmen – auch nach außen hin, also gegenüber Dritten – durch Software „handelt", desto eher wird es unmöglich oder zumindest unverhältnismäßig teuer (wie im genannten Beispiel), Datenschutz-Konformität „nur" durch organisatorische Maßnahmen sicherzustellen. Ein „händischer" Prozess mit entsprechenden Organisationsrichtlinien, Personalaufwand, Schulungen etc. wird in aller Regel

kostenintensiver, fehleranfälliger und langsamer sein als ein durch Software automatisierter Prozess, soweit er automatisierbar ist. Dabei verschieben sich die Grenzen des Automatisierbaren permanent durch die technische Weiterentwicklung. Gerade deshalb ist Datenschutz durch Technikgestaltung – insbesondere Softwaregestaltung – für den Verantwortlichen unabhängig von der rechtlichen Verpflichtung bedeutsam, indem er günstiger und effizienter ist, vorausgesetzt, er wird richtig umgesetzt.

Wenn sich ein Softwarehersteller also „top-down" der Frage nähert, wie er seine Software datenschutzfreundlicher gestalten soll, wird er sich zunächst zumindest mit dem nachfolgend geschilderten Analysebedarf konfrontiert sehen.

Der Lebenszyklus eines personenbezogenen Datums als Ausgangspunkt

Bei der Beantwortung der Frage, welche Anforderungen die DSGVO an den „typischen" Verantwortlichen, der die Software nutzt, stellt, und welche dieser Anforderungen inwieweit durch Softwarefunktionen erfüllt oder unterstützt werden können, kann das „lifecycle"-Modell eines individuellen personenbezogenen Datums hilfreich sein. Hierbei wird der „Lebensweg" eines typisierten personenbezogenen Datums – bzw. eines entsprechenden Datensatzes – von der ursprünglichen Erhebung über die Verwendung, Übermittlung, Zusammenführung mit anderen Daten etc. bis hin zur Löschung nachverfolgt. Hilfreich ist es dabei, über den „Tellerrand" der eigenen Software hinaus zu denken, d. h. auch solche Prozesse mit einzubeziehen, in denen das Datum beim Verantwortlichen (oder darüber hinaus) in irgendeiner Form (etwa über integrierte Schnittstellen) verarbeitet wird, ohne dass diese Verarbeitung unmittelbar innerhalb der Software erfolgt. In jeder Phase gelten spezifische datenschutzrechtliche Anforderungen an den (erlaubten) Umgang mit dem personenbezogenen Datum (Wer darf wie zu welchem Zweck mit den Daten umgehen?), an die Aufzeichnung von Metadaten über diesen Umgang (Wie kann man den richtigem Umgang nachweisen?), an die Kapselung bzw. Abschirmung des Datums gegen Eingriffe (unbefugten Umgang) bzw. „Abhandenkommen" (Wie kann eine Datenpanne vermieden werden?) sowie an die Ermöglichung bzw. Vereinfachung der Bearbeitung von später geltend gemachten Betroffenenrechten (Wie kann man Betroffenenrechte sicher und zuverlässig „auf Knopfdruck" erfüllen?).

Wie tief soll man ins Glas schauen?

Wie immer kann man das vorstehend beschriebene Vorgehen – Ermittlung der einschlägigen DSGVO-Vorgaben anhand einer Lebenszyklusanalyse eines typischerweise von der Software verarbeiteten personenbezogenen Datums – sehr holzschnittartig („aus der Vogelflugperspektive") oder sehr granular gestalten, frei nach dem Motto: „Juristisch kann man alles beliebig kompliziert machen". Aus IT-Sicht könnte man sagen: Wenn man jedes Bit durch jeden Chip verfolgt, dann kann z. B. jede Netzwerkübertragung selbst auf niedrigsten OSI-Schichten rechtlich relevant sein. Das mag zwar auf den ersten Blick übertrieben klingen, aber selbst technische Hilfsmechanismen wie die Verwendung von Cache-Speichern zur Beschleunigung von Datenverarbeitungsvorgängen können mit (rechtlich) relevantem Missbrauchspotenzial behaftet sein (wie z. B. die jüngst identifizierten sog. „Spectre"-Fehler im Mikrocode gängiger Prozessoren zeigen). Alternativ sollte eher auf einer „funktionalen bzw. Anwendungsebene" angesetzt und über so manchen „rein technischen Mechanismus" hinweggesehen werden. Juristisch gibt es insoweit bislang keine klare Sichtweise. Die Datenschutzbehörden sprechen von einem „mittleren Granularitätsmaßstab", was nur böswillige Menschen als „wir wissen es auch nicht genau" interpretieren würden.

Scharfer Code, unscharfes Recht

Neben der Granularität der Betrachtungsweise ist die Frage, was man wie konkret umsetzt bzw. ausgestaltet, auch damit verknüpft, wie man die Regelungen der DSGVO auslegt. Da dies verbindlich nur der Europäische Gerichtshof vermag (siehe den Facebook-Fall), wird, bis eines Tages alle Einzelheiten geklärt sind, immer eine mehr oder weniger erhebliche Rechtsunsicherheit verbleiben. Diese Rechtsunsicherheit trifft zwar in erster Linie den Verantwortlichen, aber reflexartig auch den Softwarehersteller. Dies gilt insbesondere dann, wenn Datenschutzrecht tatsächlich automatisiert, also „in Code gegossen" wird, denn in diesem Fall setzt die Software eine bestimmte Lesart (Auslegung) des Datenschutzrechts um. Solange hingegen nur die Inhaltsdaten einer Softwareumgebung – also ganz banal: Was der Benutzer in ein Feld schreibt – je nach unterschiedlicher Lesart der DSGVO unterschiedlich auszufüllen sind, spielt die Interpretationsbedürftigkeit der DSGVO für den Softwarehersteller auf den ersten Blick keine Rolle. Doch Vorsicht: Je mehr datenschutzrelevante Mechanismen bzw. Informationen – sinnbildlich gesprochen – in Freitextfelder verschoben werden, um die DSGVO-Interpretation dem Verantwortlichen zu überlassen, desto weniger „datenschutzfreundlich" wird die Software. Die (möglicherweise nicht einlösbare) Idealvorstellung des Gesetzgebers dürfte ein Datenschutz-Compliance-Management-System sein, das so vollständig und für jeden Einzelfall eines personenbezogenen Datums so „fehlerfrei" wie

möglich funktioniert, was im Grunde nur durch Automatisierung erreichbar ist, und da würden Freitextfelder, die sich am Ende als (absichtlich oder unabsichtlich) falsch ausgefüllt erweisen, nur stören.

Je mehr Datenschutz, desto tiefgreifender der Änderungsbedarf

Hand in Hand mit dem vorgenannten Aspekt der rechtlichen Unsicherheit bei der Umsetzung stellt sich die weitere Frage, wie tiefgreifend eine Software umgestaltet werden soll, um datenschutzfreundlich zu werden. Um eine konkrete Lösung zur Erhöhung der Datenschutzfreundlichkeit von Software umzusetzen, werden sich aus der Sicht des Softwareherstellers und auf der Basis der bestehenden Softwarearchitektur häufig zwei alternative Wege anbieten. Einerseits kann die Software dadurch ergänzt werden, dass zusätzliche Felder und Funktionen geschaffen werden. Ein Beispiel wäre die Einfügung des Feldes „Datenherkunft“ in einem Datenbank-Frontend als zusätzliches Freitext- oder Auswahlfeld. Andererseits kann die Architektur der Software bzw. des zugrunde liegenden Datenmodells tiefgreifend geändert werden. Ein Beispiel wäre die Einführung automatischer Löschroutinen in ein Dokumenten Management System, das bislang strukturell und technisch gar keine Löschung vorsieht (d. h. von möglichst „ewiger Archivierung ausgeht“). Beide Varianten lösen regelmäßig sehr unterschiedliche Dimensionen von Entwicklungsaufwand (im Sinne von Kosten, Zeit und möglicherweise unvorhergesehenen Folgeproblemen) aus. „Quick Wins“ sind mit ergänzenden Eingriffen leicht erzielbar. Strukturelle Fortschritte in Sachen Datenschutzfreundlichkeit werden meist einen substantiellen Eingriff im Sinne eines teilweisen Redesigns der Software und der verwendeten Datenmodelle erfordern.

Auf einer einsamen Insel

Ein großes Problem der mit dem schönen Wort „IT-Landschaft“ bezeichneten Ansammlung von verschiedenen Systemen, Systemumgebungen und Hardware-Plattformen der meisten Unternehmen ist die mühsame Kommunikation der vielen IT-Inseln untereinander. Über Jahrzehnte gewachsen, immer wieder flickschusternd aufeinander angepasst, ist das Funktionieren der Datenschnittstellen zwischen den Insellösungen der heilige Gral der Unternehmens-IT. Eine einheitliche Plattform bzw. Datenbank, über die in einem Unternehmen alles, aber auch wirklich alles abgewickelt werden kann, ist trotz anderslautender Beteuerungen bislang eine Utopie. Das bedeutet zwangsläufig, dass Konzepte, welche die gesamte IT-Landschaft eines Unternehmens umfassen, nicht vom Hersteller einer Teillösung gestaltet werden können. Aus der Perspektive der DSGVO wiederum ist es gleichgültig, ob der Verantwortliche ein System oder 100 vernetzte Insellösungen bei der Verarbeitung personenbezogener Daten einsetzt; am Ende müssen die DSGVO-Vorgaben vom Verantwortlichen im

gesamten Unternehmen umgesetzt werden. Das wiederum kann Ansporn sein, applikationsübergreifende Standards zu definieren und zu implementieren, etwa die Möglichkeit der Pseudonymisierung von Daten, die an ein anderes System übermittelt werden.

Beispielsfälle

Was heißt das nun alles konkret? Die DSGVO ist lang, komplex, unscharf und nicht in Java geschrieben. Es gibt aber dennoch viele Möglichkeiten, Software datenschutzfreundlich zu machen. Diese Möglichkeiten hängen sowohl davon ab, welche personenbezogenen Daten auf welche Weise in einer individuellen Software verarbeitet werden, als auch davon, welche DSGVO-Regelungen für die Verarbeitung einschlägig sind. Man kann folglich Softwarefunktionen und DSGVO-Anforderungen „mappen“ und dann – vorbehaltlich der bestehenden Auslegungsunschärfen der DSGVO – die jeweils „datenschutzfreundliche“ Anpassung der Funktionalität bestimmen. Bisweilen werden die sich hierbei eigentlich ergebenden Anpassungen die „freie Bedienbarkeit“ der Software derart einschränken, dass sich solche „Leitplanken“ sogar kontraproduktiv auswirken. Insbesondere dann, wenn eine softwaregestützte Lösung keinerlei Freiraum für individuelle Fälle bzw. Eingriffe erlaubt, kann eine schematische Befolgung der DSGVO ohne Möglichkeit einer händischen „Einzelfallprüfung“ – wenn die Software dies (noch) nicht beherrscht – zum DSGVO-Verstoß führen. Dann muss zusätzliche Flexibilität geschaffen werden. Bisweilen werden wiederum punktuelle Anpassungen datenschutzrechtlich keinen großen Gewinn bringen, wenn an einer anderen Stelle im Lebenszyklus des personenbezogenen Datums viel größere Gefahren (bzw. Datenschutzverstöße) drohen. So würde die Pseudonymisierung von personenbezogenen Daten innerhalb eines isolierten Verarbeitungsschrittes wenig bringen, wenn die Daten davor und danach in angrenzenden Systemen oder sogar im selben System nicht-pseudonym gespeichert und unverschlüsselt übertragen werden.

Um zu zeigen, was „Datenschutzfreundlichkeit“ im Detail bedeuten kann, folgen einige Beispiele, wie DSGVO-Vorgaben auf die Funktionalitäten einer Software „gemappt“ werden können. Diese Fälle folgen keiner granularen technischen Sichtweise, wie sie etwa in einem für Software-Entwickler lesenswerten ENISA-Papier aus dem Jahr 2014 („Privacy and Data Protection by Design – from policy to engineering“) zu finden sind. Dort geht

es neben acht allgemeinen Design-Prinzipien („minimise, hide, separate, aggregate, inform, control, enforce, demonstrate“), die sich auch aus der DSGVO heraus entwickeln lassen, um technische Fragen der Authentifizierung, der attributbasierten Berechtigungsnachweise, der Verschlüsselungstechniken, der Anonymisierung und Pseudonymisierung, des Datenschutzes in Datenbanken, der statistischen Offenlegungskontrollen, des datenschutzfreundlichen Data-Minings und Ähnliches. Die nachfolgenden Fälle hingegen behandeln vorrangig „top down“ die Auswirkungen von DSGVO-Vorgaben auf die Struktur der verwendeten Datenmodelle und die Funktionalitäten von Software gegenüber dem Bediener.

Metadaten/„Track Record“

Die DSGVO sieht vor, dass der Verantwortliche in der Lage sein muss, über die Verarbeitung jedes personenbezogenen Datums Rechenschaft abzulegen. Hier soll als Beispiel für die Verarbeitung die Übermittlung an einen Dritten dienen, beispielsweise wenn eine Konzerngesellschaft Kontaktdaten des zuständigen Mitarbeiters eines ihrer Kunden erhebt und konzernintern im Rahmen eines gruppenweiten CRM-Systems an die Holding-Gesellschaft weiter übermittelt. Scheidet der Mitarbeiter beim Kunden aus und verlangt von der betreffenden Konzerngesellschaft die Löschung seiner Daten, so muss dieses Löschungsverlangen auch an die das CRM-System betreibende Holding als Empfänger weitergegeben werden. Zu diesem Zweck muss bei der erhebenden Konzerngesellschaft aufgezeichnet werden, welche personenbezogenen Daten an welche Dritten weitergegeben wurden.

Allgemein gesprochen wäre eine Software, mit der personenbezogene Daten erhoben werden, unter anderem dann „datenschutzfreundlich“, wenn die einzelnen Nutzungshandlungen in Bezug auf die erhobenen und verarbeiteten personenbezogenen Daten als Metadaten mit Zeitstempel aufgezeichnet würden. Zu einem späteren Zeitpunkt, etwa wenn der Betroffene von seinen Betroffenenrechten Gebrauch macht (wie in der obigen Konstellation von seinem Löschungsrecht), kann dann nachvollzogen werden, was mit diesem personenbezogenen Datum „passiert“ ist (hier: an wen das Datum weitergegeben wurde).

Viele gängige Softwarelösungen protokollieren im Rahmen von Zeit- und Aktionsstempeln, mit denen Datenänderungen nachvollzogen werden können, auch den handelnden Mitarbeiter selbst, also diejenige Person, die personenbezogene Daten eines Betroffenen (z. B. eine Visitenkarte) originär eingibt, zu einem späteren Zeitpunkt berichtigt, die Übermittlung auslöst oder ausdruckt. Diese Form der Aufzeichnung kann jedoch mit dem datenschutzrechtlichen Grundsatz der Datenminimierung kollidieren, also mit der Vorgabe, dass die erhobenen Daten auf das für die Zwecke der Verarbeitung „notwendige" Maß zu beschränken sind. Der Verantwortliche – und vorgelagert der Softwarehersteller, der die Datenstrukturen definiert – muss sich daher überlegen, zu welchem Zweck die Protokollierung des jeweils handelnden Mitarbeiters erfolgen „muss". Gewöhnlich erfolgt eine solche Protokollierung zu Beweiszwecken, d. h. wenn später behauptet wird, die Daten seien nicht – wie protokolliert – an das Unternehmen A, sondern an das Unternehmen B übermittelt worden, kann der mit diesem Vorgang assoziierte Mitarbeiter benannt und als Zeuge befragt werden. Der Beweiswert der Zeugenaussage eines Mitarbeiters in einem „Massengeschäft" an Daten ist dabei allerdings sehr begrenzt. Eine geeignete datenschutzrechtliche „Garantie" für den Schutz des betroffenen Mitarbeiters kann dann möglicherweise – auch im Zusammenspiel mit anderen Maßnahmen – dessen Pseudonymisierung im Rahmen der Aufzeichnung und Wiedergabe solcher „Zugriffsstempel" sowie die endgültige Anonymisierung des Mitarbeiternamens bei dessen Ausscheiden sein. Die Implementation derartiger Funktionen erhöht dann wieder die Datenschutzfreundlichkeit – dieses Mal gegenüber dem eigenen Mitarbeiter. Dieses Beispiel verdeutlicht, dass guter Datenschutz durch Technikgestaltung nicht als Selbstzweck in eine Sammelwut von Metadaten, die ihrerseits wieder zusätzliche personenbezogene Daten sind, umschlagen darf. Dann hätte man tatsächlich den Teufel mit dem Beelzebub ausgetrieben.

Kapselung und granulare Berechtigungskonzepte

Als „Kapselung" personenbezogener Daten wird hier deren Uneinsehbarkeit bezeichnet, solange jemand, der die Daten einsehen möchte, sich nicht authentifiziert, d. h. seine Berechtigung nachgewiesen hat. Als anschauliches Beispiel mag hier das Szenario dienen, personenbezogene Daten in einem Dokument – beispielsweise einem PDF – zu „schwärzen" (oder durch Pseudonyme wie IDs zu ersetzen), d. h. der Empfänger des Dokuments kann diese zunächst nicht einsehen. Erst die Authentifizierung des Benutzers gegenüber dem System, das den Dokumenteninhalt anzeigt, kann die personenbezogenen Daten „freischalten". Diese Authentifizierung kann insbesondere an funktionale Rollen gekoppelt sein (Berechtigungskonzept): Wer über das Profil „Lohnbuchhaltung" verfügt, kann das personenbezogene Datum ansehen, wer über das Profil „Hausmeister" verfügt, nicht. Die „Freischaltung" kann auch automatisch stattfinden, wenn eine Person eines bestimmten Profils sich generell an

einem bestimmten System oder einer bestimmten Software anmeldet (Zugangs- oder Zugriffskontrolle). Die Daten sind also nicht frei mit bzw. im Dokument verfügbar, sondern gekapselt, und ein (rollenabhängiges) Berechtigungskonzept steuert den Zugriff. Das Dokument sieht aus der Sicht verschiedener Benutzer verschieden aus, je nachdem, welche Berechtigung sie vorweisen können. Dies wirft allerdings mehrere Probleme in der Umsetzung auf.

Erstens:
Das Kopieren dieser Informationen aus dem Dokument und das Einfügen in ein anderes Dokument soll natürlich nur möglich sein, wenn die „Kapselung" der Daten mit in das neue Dokument übernommen wird. Ansonsten könnte die Kapselung leicht umgangen werden. Auch ist an das Sperren der Druckfunktion und von Screenshots zu denken.

Zweitens:
Die Granularität der Berechtigungen muss sich nach der benötigten Granularität der personenbezogenen Daten selbst richten. So könnte es sinnvoll sein, Tag und Monat einerseits sowie Jahr andererseits eines Geburtsdatum als getrennte personenbezogene Daten zu behandeln und „freischalten" zu können.

Drittens:
Wird das Dokument an externe, datenschutzrechtlich legitimierte Dritte weitergegeben (z. B. als E-Mail-Anhang), so wird die Einsehbarkeit der enthaltenen personenbezogenen Daten für den Dritten davon abhängen, dass dieser über die entsprechende Software bzw. Infrastruktur (Laufzeitumgebung) verfügt. Wenn nämlich die „virtuelle" Sichtweise des Datenschutzrechts, wer zulässigerweise bestimmte personenbezogene Daten verarbeiten darf, mit der technischen bzw. faktischen Zugriffsmöglichkeit auf bestimmte Daten synchronisiert wird, muss jedem Teilnehmer an diesem Synchronisationsmechanismus im Grundsatz dieselbe, personenbezogene Daten „kapselnde" Laufzeitumgebung zur Verfügung stehen. Das kann die Notwendigkeit eines eigenständigen, überall kostenlos verfügbaren, möglicherweise web-gestützten „Viewers" begründen, der zunächst aktuelle Zugriffsberechtigungen abfragt, bevor die personenbezogenen Daten angezeigt werden. Verliert der Besitzer des Dokuments seine Zugriffsberechtigung, kann er die personenbezogenen Daten des Dokuments nicht mehr sichtbar machen. Die datenschutzfreundliche Software wird so zu einer Zugriffssteuerungsplattform, die ständig und von überall her erreichbar sein muss.

Viertens:
Personenbezogene Daten erschöpfen sich bekanntlich nicht in Name und Adresse. Es geht vielmehr um „identifizierbare“ Personen. Wenn etwa ein einziger Beschäftigter eines Unternehmens 172 Kilogramm wiegt, würde die Angabe des Gewichts, gleich an welcher Stelle einer Korrespondenz, unmittelbar zu dessen Identifizierbarkeit führen, auch wenn der Name an anderer Stelle im Dokument „geschwärzt“ erscheint. Auch Umschreibungen oder „unscharfe“ Beschreibungen können also sowohl personenbezogene Daten sein als auch die Identifizierung einer betroffenen Person ermöglichen. Hier werden die Grenzen der automatischen Erkennung von personenbezogenen Daten in einem Dokument sichtbar.

Übermittlung in ein Drittland

Generell bedarf die Übermittlung personenbezogener Daten an Dritte außerhalb des Verantwortlichen und ggf. seines Auftragsverarbeiters, etwa per E-Mail, einer datenschutzrechtlichen Legitimationsgrundlage. Die zur Verfügung stehende Bandbreite an Legitimationsgründen ist bekanntlich breit, insbesondere im Bereich der Interessenabwägung. Bevor Software in der Lage ist, das Interesse des Verantwortlichen und das Interesse des Betroffenen automatisiert zu ermitteln und rechtssicher gegeneinander abzuwägen, wird noch einige Zeit ins Land gehen.

Eine Besonderheit besteht allerdings stets dann, wenn Daten in ein Drittland übermittelt werden. In diesem Fall reicht es nicht aus, nur über eine (inhaltliche) Legitimationsgrundlage für die Übermittlung an einen (bestimmten) Dritten zu verfügen. Es muss eine weitere (formale) Legitimationsgrundlage für die Drittlandsübermittlung hinzukommen, nämlich entweder ein Angemessenheitsbeschluss der EU-Kommission oder das Bestehen von (seitens der Aufsichtsbehörden freigegebener) „binding corporate rules“ innerhalb eines Konzerns oder die Vereinbarung von EU-Standardklauselwerken zwischen dem Verantwortlichen und dem Dritten oder die Erforderlichkeit im Zusammenhang mit bestimmten Verträgen oder aber das Vorliegen einer qualifizierten Einwilligung des Betroffenen nach besonderer Aufklärung.

Ausgehender Datenverkehr könnte daher softwaregestützt anhand der Zieladresse daraufhin überwacht werden, ob eine Datenübertragung in ein Drittland stattfinden soll, um dann regelbasiert festzustellen, ob eine formale Legitimationsgrundlage besteht. Auf diese Weise können datenschutzwidrige Drittlandsübermittlungen vermieden werden.

Löschfristen und „Legal Hold“

Die Entwicklung und Umsetzung von Löschkonzepten gehört zu den schwierigsten Aufgaben der technischen Implementierung eines Datenschutz-Compliance-Management-Systems. Dies liegt an der Vielzahl von gesetzlich angeordneten oder anderweitig notwendigen Aufbewahrungsfristen, an den interpretationsbedürftigen Ausnahmen von der datenschutzrechtlichen Löschpflicht und an der Notwendigkeit der Klassifizierung jedes einzelnen Datums hinsichtlich der einschlägigen Löschfrist. Technisch kommt das Problem der vollständigen Löschung (auch auf Backup-Medien oder in Archivierungssystemen, die eigentlich ihrem Zweck nach nicht auf Löschung, sondern auf „ewige Speicherung“ angelegt sind) hinzu.

Software kann zunächst schon bei Erhalt eines konkreten personenbezogenen Datums die Einteilung desselben in eine vordefinierte Löschklasse unterstützen. Sobald dann später das Ereignis, das die Löschfrist auslöst, eintritt (bzw. automatisch erfasst oder bestimmt wird), beginnt die softwaregestützte „Lösch-Sanduhr“ für dieses Datum zu laufen. Bei Ablauf des Countdowns, der z. B. eine Aufbewahrungsfrist repräsentiert, wird das personenbezogene Datum automatisiert und sicher gelöscht. Während des Countdowns ist durch entsprechende Kapselung der Daten sicherzustellen, dass nur noch ein Zugriff im Rahmen des (verbleibenden) Aufbewahrungszwecks erfolgen kann. Bei steuerlichen Aufbewahrungsfristen kann dies im Extremfall nur noch ein (externer) Betriebsprüfer sein.

Verkompliziert wird die Umsetzung der starren Löschfristen (sobald die richtige Kategorie gewählt wurde) durch die Notwendigkeit, solche laufenden „Lösch-Countdowns“ aufhalten zu können. Denn jede rechtliche Frist ist Verlängerungen zugänglich. Steuerliche Aufbewahrungsfristen beispielsweise müssen bei Beginn einer Betriebsprüfung – sog. Ablaufhemmung – vor Fristablauf „gestoppt“ werden. Das gilt natürlich nur für die Fristen bezüglich derjenigen Daten, die von der Betriebsprüfung umfasst sind. Eine datenschutzfreundliche Software enthält also nicht nur umfangreiche Werkzeuge für ein datenschutzkonformes Löschkonzept, sondern erlaubt auch das Aufhalten bzw. Wiederanlaufen bestimmter Fristen auf Knopfdruck für die Gruppe der jeweils betroffenen personenbezogenen Daten.

Bearbeitung von Auskunftsrechten

Das Auskunftsrecht des Betroffenen ist neben dem Löschrecht das in der Praxis wichtigste Betroffenenrecht. Der Verantwortliche muss in der Lage sein, dem Betroffenen innerhalb eines Regelzeitraums von vier Wochen die jeweils verarbeiteten personenbezogenen Daten sowie verschiedene Metadaten auf einem sicheren Übertragungsweg zur Verfügung zu stellen.

Software kann hier zunächst den Workflow der Bearbeitung des Auskunftsrechts vorzeichnen bzw. in Teilaspekten unterstützen. Der Workflow reicht von der Anlage eines Vorgangs („Ticket“) und der Prüfung der Identität des Betroffenen über das Zusammenziehen der notwendigen Daten und Metadaten aus angeschlossenen Systemen bis hin zur Bereitstellung einer Web-Plattform des Verantwortlichen, auf welcher der Betroffene nach entsprechender Authentifizierung „seine“ Daten einsehen und herunterladen kann.

Der wichtigste Baustein ist dabei die Identifikation sämtlicher personenbezogener Daten, die „irgendwo in den Systemen“ über den Betroffenen, der Auskunft begehrt, verarbeitet wurden oder werden. Dazu sind deren Herkunft, einschlägige Löschfristen, (bisherige) Empfänger, Drittlandsübermittlungen etc. als Metadaten zu ermitteln, was voraussetzt, dass diese Daten erfasst wurden, identifizierbar und für ein zentrales System verfügbar sind, welches diese Daten dann zusammenstellt. Hier werden die oben angesprochenen „Track Records“ wieder relevant. Ein datenschutzfreundliches CRM-System etwa könnte all diese Daten für die Kontaktdaten von Repräsentanten von Unternehmenskunden auf Knopfdruck zur Verfügung stellen. Plakativ gesagt sollte die vollständige und richtige Bearbeitung eines Auskunftsrechts nur noch Sekunden dauern, wenn datenschutzfreundliche Software eingesetzt wird.

Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit ist ebenfalls ein Betroffenenrecht und setzt erhebliche Vorarbeiten in Gestalt eines entsprechenden Software-Designs voraus. Der Betroffene hat dieses Recht im Grundsatz immer dann, wenn er dem Verantwortlichen personenbezogene Daten „bereitgestellt“ hat. Wann genau das der Fall ist, wird von der DSGVO nicht näher erläutert. Selbstverständlich neigen die Datenschutzbehörden dazu, diesen Begriff weit im Sinne sämtlicher vom Verantwortlichen „erhobener“ Daten des Betroffenen zu verstehen, solange der Betroffene irgendwie an der Erhebung mitwirkt.

Diese Daten müssen dem Betroffenen in einem „strukturierten, gängigen und maschinenlesbaren Format“ zur Verfügung gestellt werden. Auch hier ist daher zunächst eine web-gestützte Plattform zur „Auslieferung“ der Daten an den Betroffenen notwendig, da der postalische Versand von physischen Datenträgern auf Kosten des Verantwortlichen vermieden werden sollte. Die Besonderheit liegt hier im Wort „strukturiert“, d. h. die Daten müssen so aufbereitet werden, dass sie in eine (aus Sicht des Betroffenen) ähnliche „Funktionsumgebung“ eines anderen Anbieters importiert werden können. Der Gesetzgeber hatte hier den Fall vor Augen, dass ein Betroffener von „Facebook 1“ zu „Facebook 2“ migrieren möchte, d. h. seine Daten bei „Facebook 1“ exportiert und bei „Facebook 2“ importiert und dann dort in einer ähnlichen Umgebung auf den entsprechenden (historischen) Daten aufsetzen

kann. Man kann sich vorstellen, was passiert, wenn ein Fahrer der Automarke X die von ihm bislang generierten und im Fahrzeug gespeicherten und/oder an die Server des Automobilherstellers übermittelten „Fahrkenndaten“ exportieren möchte, um diese bei einem Fahrzeugwechsel einem anderen Automobilhersteller als „historische Fahrersignatur“ zu importieren. Bis das möglich wird, was der Gesetzgeber so weitgehend über seine ursprüngliche Absicht hinaus vorgegeben hat, muss noch viel Software konzipiert werden.

Einwilligung/Koppelungsverbot

Wenn auch wenig präzise formuliert, geht der Gesetzgeber im Rahmen des sog. „Koppelungsverbots“ davon aus, dass beim Abschluss von Verträgen (auch EULAs und „Nutzungsbedingungen“) nur die Daten erhoben werden dürfen, die für die Erfüllung des Vertrages erforderlich sind. Das ist einfach erklärt: Geht ein Kunde in einen Schuhladen und möchte Schuhe kaufen, wäre die Frage des Verkäufers nach seiner Hemdengröße nicht für den Zweck des Schuhkaufs erforderlich. Würde der Schuhladenbesitzer den Abschluss eines Schuhkaufvertrages verweigern, weil ihm die Hemdengröße nicht mitgeteilt wurde (bzw. der Kunde keine Einwilligung zur Erhebung der Hemdengröße erteilt hat), hätte er den Schuhkaufvertrag mit der Hemdengrößenthematik unzulässigerweise „gekoppelt“. Gibt der Kunde seine Hemdengröße unter dem Druck, sonst keine Schuhe kaufen zu können, schließlich heraus, ist die damit verbundene datenschutzrechtliche Einwilligung nicht „freiwillig“ erteilt worden. Sie ist unwirksam. Der Schuhladenbesitzer darf die Hemdengröße als personenbezogenes Datum nicht verarbeiten. Er „sitzt auf toxischen Daten“, könnte man sagen. Die Lösung für dieses Problem ist einfach: Der Kunde kann Schuhe kaufen und frei entscheiden, ob er seine Hemdgröße preisgibt oder nicht. Tut er dies nicht, kann er die Schuhe ebenso kaufen.

Es wird leicht ersichtlich, dass diese Thematik großen Einfluss auf die Struktur insbesondere von solcher Software hat, mit der personenbezogene Daten im Zusammenhang mit Vertragsbeziehungen zwischen Anbieter und Kunden originär erhoben werden. Bislang wurde derartige Software – einschließlich vieler Apps – häufig so gestaltet, dass der Benutzer einer Plattform am Anfang ein Paket von Einwilligungen erteilt hat. Sonst ging es schlicht nicht weiter. Und nicht alle diese Daten, in deren Verarbeitung insgesamt eingewilligt werden musste, waren „vertragsnotwendig“ (schon gar nicht, wenn der Vertrag bzw. die Nutzungsbedingungen an AGB-rechtlichen Maßstäben gemessen werden). Die Möglichkeit, die eine Einwilligung zu erteilen, die andere aber nicht, war nicht vorgesehen. Wenn man dieses Bündel an Einwilligungen nun aus datenschutzrechtlichen Gründen in Einzeleinwilligungen aufteilen muss, die separat erteilt oder verweigert werden können, dann muss die Software

in ihrem weiteren Ablauf mit jeder Kombination aus Einwilligungen und Nicht-Einwilligungen umgehen können. Wird beispielsweise die Einwilligung in die Verarbeitung des jeweiligen (GPS-) Standorts nicht erteilt, müssen sämtliche Funktionen, die dieses Datum benötigen, „elegant abgeschaltet" werden. Der Rest der Funktionalität der Software muss natürlich weiterhin sinnvoll funktionieren.

Schlusswort

Die Beispiele zeigen in groben Umrissen, was „datenschutzfreundliche" Software – je nach Aufgabenstellung – ausmachen kann. Es liegt auf der Hand, dass Software, die derartige Möglichkeiten bietet, nicht nur bei der Beschaffung datenschutzrechtlich vorzugswürdig ist, sondern auch, dass deren Einsatz Kosten senken und die Verlässlichkeit interner Prozesse im Rahmen des Datenschutz-Compliance-Management-Systems erhöhen kann.

Das führt zum Schluss wieder dazu zurück, dass Software nur einen Baustein des Datenschutz-Compliance-Management-Systems des Verantwortlichen darstellt; es geht also nicht nur um die „Einbettbarkeit", sondern stets auch um die konkrete Einbettung der Software in die Gesamtheit der technischen und organisatorischen Maßnahmen (TOMs) des Verantwortlichen. Dabei können die TOMs bei jedem Verantwortlichen, der die gleiche Software nutzt, durchaus anders aussehen. Dies ist auch der Grund dafür, warum die Zertifizierung einer Software als „DSGVO-konform" oder „datenschutzfreundlich" wenig über die tatsächliche Einhaltung der DSGVO durch den Verantwortlichen aussagen würde. Denn DSGVO-konform kann nur das Datenschutz-Compliance-Management-System des Verantwortlichen als Ganzes sein und jede Software kann in diesem Kontext falsch eingesetzt werden. Andersherum ausgedrückt: Es bringt nicht viel, eine Taschenrechner-App als „DSGVO-konform" zu zertifizieren, nur weil diese dazu geeignet ist, im Rahmen der Entscheidungsfindung zum Datenschutz durch Technikgestaltung die verschiedenen Faktoren der Implementationskosten richtig aufzuaddieren. Auch diese App ist Software und ein sehr kleiner Baustein, den man richtig oder falsch in das Gesamtsystem integrieren kann. Der Aussagewert eines Zertifikats im Sinne von „im richtigen Kontext richtig eingesetzt kann man damit die DSGVO-Anforderungen erfüllen" – das müsste man auch jeder Textverarbeitungssoftware attestieren – wäre daher begrenzt.

Die DGSVO sieht dementsprechend auch kein spezifisches Zertifikat für die Datenschutzfreundlichkeit einer Software vor. Nur der Verantwortliche kann sich selbst (bzw. seine Umsetzung der DSGVO-Vorgaben) dahingehend zertifizieren lassen, dass er die DSGVO-Vorgaben einhält. Dabei ist allerdings zu betonen, dass ihn dies nicht von seiner Verantwortlichkeit entbindet und im Streitfall auch keinen „Beweis", sondern nur ein Indiz darstellt. Das erfolgreich durchlaufene Zertifizierungsverfahren hinsichtlich des Datenschutz-Compliance-Management-Systems des Verantwortlichen insgesamt kann dann, so Art. 25 Abs. 3 DSGVO, auch den Nachweis erleichtern, dass den Vorgaben des Datenschutzes durch Technikgestaltung Genüge getan wurde. Mit anderen Worten: Wenn der Datenschutz als Ganzes „stimmt", schließt dies die Verwendung ausreichend datenschutzfreundlicher Technik – immerhin eine der vielen datenschutzrechtlichen Vorgaben – ein.

Die Werbebotschaft des Softwareherstellers hinsichtlich der Datenschutzfreundlichkeit seiner Software muss demnach lauten, dass diese den Verantwortlichen bei der Erfüllung seiner DSGVO-Pflichten begleitet und unterstützt, indem dort bestimmte Funktionalitäten bereits umgesetzt worden sind. Funktionalitäten, die sich jeder Verantwortliche im Rahmen der Implementierung seines Datenschutz-Compliance-Management-Systems „eigentlich" wünschen müsste, weil sie ihm die Erfüllung seiner Pflichten wesentlich vereinfachen. Je mehr die Datenschutzfreundlichkeit der Software an diesem Anspruch wächst, desto mehr ist der Verantwortliche daneben aus datenschutzrechtlicher Sicht sogar verpflichtet, diese Software auch bei der Beschaffung vorzuziehen.

Experten-Kontakt

Dr. Axel-Michael Wagner
Rechtsanwalt

E-Mail: a.wagner@psp.eu

Über PSP

Peters, Schönberger & Partner (PSP) zählt mit einer über 35-jährigen, erfolgreichen Unternehmenshistorie zu den renommiertesten mittelständischen Kanzleien in Deutschland. Als Steuerberater, Wirtschaftsprüfer und Rechtsanwälte unterstützen wir Sie bei wichtigen Entscheidungen und begleiten Sie bei deren Umsetzung. Zu unseren Mandanten zählen mittelständische Unternehmen, Familienunternehmen, vermögende Privatpersonen und Private Equity-Gesellschaften, die den Wunsch nach einer interdisziplinären und individuellen Beratung haben. Sie finden in uns einen professionellen, verlässlichen und durchsetzungsstarken Partner, der mit Leidenschaft Ihre rechtlichen und steuerlichen Interessen vertritt und auch die klassischen Aufgaben der Wirtschaftsprüfung übernimmt. Das PSP-Family Office unterstützt Sie zudem bei der Vermögensstrukturierung und verfügt über ausgewiesene Expertise in Nachfolge-, Stiftungs- und Immobilienfragen.

PETERS, SCHÖNBERGER & PARTNER
RECHTSANWÄLTE
WIRTSCHAFTSPRÜFER
STEUERBERATER
www.psp.eu