BÜSING MÜFFELMANN & THEYE
BREMEN
FRANKFURT AM MAIN
BERLIN
MÜNCHEN

BÜSING MÜFFELMANN & THEYE MAXIMILIANSTRASSE 38, 80539 MÜNCHEN

Dr. Christian Weitzel
Rechtsanwalt

SEKRETARIAT Daniela Stoll
TELEFON 089 / 287007-0
TELEFAX 089 / 287007-29
E-MAIL weitzel@bmt.eu

STAND: 26.2.2018

Einkauf DS-GVO-konformer Software

1. DS-GVO – jetzt auch noch im Einkauf?

Viele Mitarbeiter stöhnen: DS-GVO-Vorbereitung ist schön und gut. Aber wieso jetzt noch in meiner Abteilung?

Personal und IT ist meist klar, dass sie von den Neuerungen durch die DS-GVO direkt betroffen sind. Der Einkauf dagegen staunt meist, wenn ihm erklärt wird, welche tragende Rolle er bei der Umstellung hat. Er ist es nämlich, der den Aufwand für Analyse und Erfüllung der Betroffenen-Rechte reduzieren kann.

Wie, das erläutert dieser Ratgeber.

2. Ideale Software aus Sicht der DS-GVO

Der europäische Gesetzgeber verfolgt mit der DS-GVO hehre Ziele: volle Transparenz und am besten direkter Einblick in alle Sammlungen von personenbezogenen Daten. Das findet sich – etwas versteckt im Vorspann der DS-GVO – in Erwägungsgrund 63:

> *„(…) Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der (…) direkten Zugang zu (…) personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen (…) nicht beeinträchtigen.*"

So etwas können sich nur Parlamentarier ausdenken, die noch nie in einem großen Unternehmen gearbeitet haben. Man stelle sich vor: Ein Konzern wie Siemens gewährt jedem Anfrager direkten Zugriff und Einblick in ihr SAP und hunderte weiterer Systeme weltweit – und kann dabei sicherstellen, dass der Anfrager nur seine eigenen Daten zu Gesicht bekommt und keinerlei Geheimnisse!

3. Wünschenswerte SW-Features zur Erfüllung der DS-GVO-Pflichten

Derartige IT-Systeme hat (noch) kein Unternehmen. Es gibt auch keine Pflicht, *alle* Systeme so auszugestalten – aber eine Wunschvorstellung. Nicht nur für den Gesetzgeber – wer pro Monat hunderte Auskünfte erteilen und dazu Daten ermitteln und zusammenstellen muss, wäre froh um eine so leichte Abwicklung der Auskunft nach § 15 DS-GVO.

Kurzum:
Bei der Neuanschaffung von Software, die personenbezogene Daten verarbeitet, ist ein solcher Fernzugang für das betreibende Unternehmen nützlich. Je nach Komplexität und Sicherheitsbedürfnissen mag der aufwendig zu programmieren sein. Das Kosten-Nutzen-Verhältnis kann sich vor allem bei großen Systemen durchaus lohnen.

4. Nützliche SW-Features zur Erfüllung der DS-GVO-Pflichten

Bleiben wir beim Auskunftsrecht nach § 15 DS-GVO. Fragt eine Person an, welche personenbezogenen Daten von ihr ein Unternehmen, eine Behörde oder ein Verein speichert, so muss unter anderem Auskunft erteilt werden zu

- geplanter Dauer der Speicherung oder – falls nicht möglich – Kriterien für die Festlegung dieser Dauer (Art. 15 Abs. 1 lit. d) DS-GVO),
- wenn die Daten nicht bei der betroffenen Person erhoben werden, allen verfügbaren Informationen über die Herkunft der Daten (Art. 15 Abs. 1 lit. g) DS-GVO).

Derzeit hat ein Unternehmen nur zwei Alternativen, diese Informationen zu beschaffen:

(1) Die Informationen werden in jedem Einzelfall ermittelt oder erfragt werden. Das erfordert einen hohen manuellen Aufwand. Der kann bei großen Unternehmen oder vielen Anfragen nicht innerhalb der gesetzlichen Frist getrieben werden.

(2) Die Informationen werden dem Verzeichnis der Verarbeitungstätigkeiten entnommen. Das setzt indes ein Verzeichnis voraus, das mit Sorgfalt und ausreichend Details erstellt wurde.

Die Erfahrung aus vielen DS-GVO-Vorbereitungen zeigt indes: Kaum ein Unternehmen hat die zweijährige Vorbereitungszeit genutzt, seine Verarbeitungstätigkeiten zu analysieren und gesetzkonform zu beschreiben. Zwar musste schon immer ein weitgehend ähnliches Verfahrensverzeichnis erstellt werden. Um die Einhaltung dieser Pflicht haben sich nur wenige gekümmert und die Verzeichnisse dann meist jahrelang nicht aktualisiert.

Kurzum:
Findige Mitarbeiter in den IT-Abteilungen überlegen deshalb, wie die zu beauskunftenden Daten in Zukunft direkt aus Datenbanken und Systemen ausgelesen werden können.

5. Praxisbeispiel Löschfristen

Die Haupt-Datenbank eines Web-Shops speichert verschiedene Datenkategorien mit unterschiedlicher Löschpflicht:

Kategorie	Datenfelder	Aufbewahrungs-/ Löschfrist	Quelle
Adressdaten	Name, Straße, PLZ, Ort	*Ohne Account:* Bis Ende Abwicklung Vertragsverhältnis – *Bei Rahmenvertrag (z.B. Amazon-Account):* Bis Kündigung Account	Art. 17 Nr. 1 lit. a) DS-GVO
Bestelldaten	Produkt, Zahl, Preis, Gesamtpreis, Umsatzsteuer, Bedingungen, Bestellung als eMail, Scan oder PDF	6 Jahre	§ 257 Abs. 2 Nr. 2 und Abs. 4 HGB § 147 Abs. 1 Nr. 2 und Abs. 3 AO
Auftragsdaten	Produkt, Zahl, Preis, Gesamtpreis, Umsatzsteuer, Bedingungen, Auftragsbestätigung als Scan oder PDF	6 Jahre	§ 257 Abs. 2 Nr. 3 und Abs. 4 HGB § 147 Abs. 1 Nr. 3 und Abs. 3 AO
Lieferscheindaten	Produkt, Zahl, Lieferort, Lieferbedingungen	*Wenn kein Buchungsbeleg:* Bis Versand der Rechnung *Sonst:* 10 Jahre	§ 147 Abs. 3 AO
Rechnungsdaten	Produkt, Zahl, Preis, Gesamtpreis, Umsatzsteuer, Zahlungsbedingungen, Rechnung als Scan oder PDF	10 Jahre	§ 257 Abs. 2 Nr. 4 und Abs. 4 HGB § 147 Abs. 1 Nr. 4 und Abs. 3 AO

Wie soll der Web-Shop die unterschiedlichen Löschpflichten managen?

Ideal wäre es, wenn zu jedem Feld mit personenbezogenen Daten zwei zusätzliche Felder gespeichert sind: eines mit dem Erstellungsdatum und eines mit der Speicherdauer. Weshalb nicht schlicht eines mit der Löschfrist? Ganz einfach, die gesetzlichen Fristen können sich ändern, oder ein Vertrag wird verlängert. Dann möchte und darf der Webshop die Speicherdauer verlängern. Um das Löschdatum zu kennen, muss er dann jedoch wissen, seit wann die Daten gespeichert sind.

Kurzum:
Achtet man beim Design von Datenbanken darauf, dass für personenbezogene Daten die jeweilige Löschfrist gespeichert ist, kann die Löschung automatisiert erfolgen. Außerdem kann die Auskunft zu Löschfristen direkt aus den IT-Systemen erteilt werden.

6. Privacy by Default, Privacy by Design

Diese Begriffe stehen für die deutschen Wortungetüme „Datenschutz durch datenschutzfreundliche Voreinstellungen" bzw. „Datenschutz durch Technikgestaltung"; sie finden sich im amtlichen Titel von Art. 25 DS-GVO.

Die hehren Vorstellungen des Gesetzgebers gehen weit: Datenschutz soll bereits in der Software integriert sein. Dazu soll die Software durch Voreinstellungen datenschutzfreundlich ausgestaltet sein. Die nötigen Schutzmaßnahmen für personenbezogene Daten soll die Software am besten selbst ergreifen.

Aus Art. 25 und 32 DS-GVO geht hervor, was damit gemeint ist: Wo nötig und wirtschaftlich möglich, soll die Software für

- Datenminimierung
- Reduzierung der Datenverarbeitung auf benötigte Zwecke
- Einhaltung der Speicherfrist
- Zugriffsschutz, z.B. durch
    - Reduzierung der Zugriffsrechte auf jeweils nötige Kreise und Tätigkeiten
    - Effektive Authentifizierung der Zugriffsberechtigten
    - Anonymisierung, Pseudonymisierung
    - Verschlüsselung

sorgen. Fachleute sind sich einig, dass nach dem Gesetzeszweck auch dazu gehört:

- automatische Umsetzung des Widerspruchsrechts
- automatische Umsetzung ausgeübter Widerrufe von Einwilligungen

Nach Art. 32 DS-GVO sollen Systeme und Dienste schließlich

- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Kurzum:
All diese Pflichten sollte der Einkauf kennen und beim Einkauf von Software beachten!

7. Sonderproblem: Software „aus der Cloud"

Seitdem IT-Budgets immer schlanker werden sollen, wird versucht, Investitionen in eigene Rechenzentren zu reduzieren. Dem kommen die Angebote sogenannter „Cloud-Services" entgegen.

Dabei handelt es sich oft nicht um Dienstleistungen („Services"), sondern ganz überwiegend um Software- oder Hardware-Miete, z.B. wenn Rechenleistung und Speicherplatz „in der Cloud" angemietet werden (gleich bei Amazon oder Microsoft). Auch bei spezieller konzipierten Angeboten wie *„Infrastructure as a Service (IaaS)"* und *„Platform as a Service (PaaS)"* steht die Bereitstellung von Infrastruktur im Vordergrund (z.B. bei der SAP HANA Cloud Platform). Um die gemietete Infrastruktur zu warten und betriebsbereit zu halten, ergänzen Dienstleistungen das Angebot. Rechtlich handelt es sich deshalb um gemischte Verträge.

Werden personenbezogene Daten (z.B. von Mitarbeitern, Kunden oder Lieferanten) in einer Cloud-Infrastruktur verarbeitet, sind ab 25. Mai 2018 alle Anforderungen der DS-GVO einzuhalten. Nach der DS-GVO ist Datenverarbeitung in der Cloud eine Auftragsverarbeitung. Für jeden Cloud-Anbieter braucht es nach Art. 28 DS-GVO daher ausreichende Garantien. Dazu gehören die Prüfung und Anpassung der technischen und organisatorischen Schutzmaßnahmen (TOMs) auf die neuen Anforderungen. Alte Auftragsdatenverarbeitungsvereinbarungen (ADVen) sind auf die neuen Anforderungen der DS-GVO anzupassen. Gibt es noch gar keine Vereinbarung, ist dringend eine Auftragsverarbeitungs-Vereinbarung (so der neue Sprachgebrauch unter der DS-GVO) auszuhandeln.

Das größte Problem resultiert meist daraus, dass Cloud-Anbieter nicht genau angeben, in welchen Ländern die angebotene Software oder Infrastruktur aufgestellt ist. Ist nicht sichergestellt, dass personenbezogene Daten stets in der EU verbleiben, handelt es sich um eine Datenübermittlung an Drittländer. Die wiederum ist nur noch zulässig, wenn einer der Erlaubnistatbestände nach Art. 44 bis 49 DS-GVO vorliegt, und zwar für jeden Auftragsverarbeiter und dessen Subunternehmer!

Viele Cloud-Anbieter residieren in den USA oder verlagern Daten ganz selbstverständlich in die USA. Deshalb sei darauf hingewiesen, dass die USA für die EU kein „sicherer" Drittstaat ist. Aus diesem Umstand resultieren nicht bloß datenschutzrechtliche Hürden – die mit entsprechender Vorbereitung zu nehmen sind. Nach der US-Rechtsprechung (genauer: den „Long Arm Statutes") kann schon der Vertragsschluss mit einem US-amerikanischen Cloud-Anbieter einen Gerichtsstand in den USA begründen. Aufgrund der kaum vorhersehbaren Entscheidungen amerikanischer Gerichte (Jury Trials, Schadenersatz mit Strafcharakter, Sammelklagen) besteht dadurch ein erhöhtes Risiko.

Ein weiteres Risiko bereitet das US-Prozessrecht. Im US-amerikanischen Zivilverfahren ist die Beweiserhebung im Rahmen eines Ausforschungsanspruchs (Discovery) möglich.

Der Prozessgegner kann sich seine Informationen selbst beschaffen und z.B. elektronische Datenträger (e-Discovery) durchsuchen. Speichert ein Unternehmen Daten in einer US-amerikanischen Cloud (z.B. eMails in Office 365 zur Miete), besteht das Risiko, dass diese Daten im Rahmen eines e-Discovery-Verfahrens offengelegt werden müssen. Ob jenes Risiko eine ernstzunehmende Gefahr darstellt, muss jedes Unternehmen für sich selbst beurteilen.

8. Zwölf Praxistipps für den Software-Einkauf

Wie sollte man die Vorgaben „Privacy by Default" und „Privacy by Design" beim Einkauf von Software auf die Lieferanten verlagern? Auch wenn es häufig zu lesen ist – vermeiden Sie pauschale Anforderungen wie „Lieferung einer DS-GVO-konformen Software". Das ist viel zu unbestimmt! Außerdem sollten Sie dafür sorgen, dass die Software Ihre Auskunftspflicht nach Art. 15 DS-GVO möglichst weitgehend unterstützt.

Werden Sie also konkret und verlangen Sie folgende Details:

1. Bei der Speicherung personenbezogener Daten sind zu jedem Datenfeld zwei weitere anzulegen, eines für das Erfassungsdatum und ein zweites für die Speicherdauer.
2. Es gibt eine Funktion zur periodischen Anzeige und selektiven Verlängerung der Speicherdauer bzw. der automatisierten Löschung von personenbezogenen Daten.
3. Erlaubt die Software einem externen Nutzer (z.B. Kunden, Lieferanten o.ä.) die Eingabe personenbezogener Daten, stellt sie den Nutzern automatisiert alle Informationen nach Art. 13 zur Verfügung.
4. Die Verarbeitung personenbezogener Daten in der Software wird so gestaltet, dass ausschließlich für den jeweiligen Zweck erforderliche Datenfelder und Datensätze verarbeitet werden.
5. Erfordert die Verarbeitung personenbezogener Daten eine Einwilligung, darf die Software diese erst einholen, wenn sie tatsächlich benötigt wird. Die Einwilligung muss ausdrücklich erteilt werden (Opt-in). Zuvor ist der Nutzer entsprechend der gesetzlichen Anforderungen zu informieren.
6. Personenbezogene Datensätze und Datenfelder lassen sich in der Software selektiv sperren, sodass sie nicht mehr verarbeitet werden können.
7. Zugriffsrechte auf personenbezogene Daten werden auf das Nötigste beschränkt. Dazu muss die Software entsprechende Daten- und Zugriffskategorien vorsehen und implementieren.

8. Die Software hat einen Ablauf zur Prüfung von beantragten Zugriffsrechten implementiert. Die Software hat einen Mechanismus zur regelmäßigen Prüfung, ob die vergebenen Zugriffsrechte notwendig sind.

9. Die Software hat Prüfmechanismen zur Erkennung unberechtigter Zugriffe.

10. Aus der Software können alle gespeicherten personenbezogenen Daten zu einer Person mit einer einfachen Abfrage vollständig und in verständlicher Darstellung exportiert und ausgedruckt werden.

11. Cloud-Angebote sind besonders kritisch zu analysieren und fast stets anzupassen:
    – Gibt es schon eine Auftragsverarbeitungs-Vereinbarung?
    – Sind die technischen und organisatorischen Maßnahmen beschrieben und ausreichend?
    – Handelt es sich um eine rein europäische Cloud eines EU-Anbieters?
    – Wenn US-Anbieter oder US-Cloud: Sind die Risiken abgewogen?
    – Bei jedem Transfer in Drittländer: Liegt einer der Erlaubnistatbestände nach Art. 44 bis 49 DS-GVO vor?

Falls wirtschaftlich sinnvoll lässt sich schließlich verlangen:

12. Die Software erlaubt Nutzern einen gesicherten Fernzugang entweder direkt zum System oder zu einem gesonderten, abgesicherten und teil-gespiegelten System, über den der Nutzer sämtliche in der Software gespeicherte personenbezogenen Daten einsehen kann.

Dies sind grundlegende Tipps für jede Art von Software. Bei mobilen Apps sind aufgrund des Telemedienrechts noch zusätzliche Anforderungen sinnvoll. Auf diese soll hier nicht näher eingegangen werden.