Softwarebeschaffung

Softwarebeschaffung im Sinne dieses Wiki sind der Kauf und die Miete von Standardsoftware, die Herstellung von Individualsoftware sowohl durch die Organisation selbst als auch durch Fremdanbieter aber auch die bloße Nutzung spezifischer IT-Dienstleistungen (Software as a Service - SaaS) - natürlich alles unter der Voraussetzung, dass Personenbezogene Daten verarbeitet werden.

Softwarebeschaffung ist für den Datenschutz ein zentrales Thema, da viele Datenschutzprobleme bei IT-Systemen letztlich daraus resultieren, dass die Beschaffungsentscheidungen getroffen wurden, ohne den Datenschutz mit zu berücksichtigen. Die Chancen, erfolgreich gemeinsam mit einem IT-Dienstleister zu datenschutzgerechten Lösungen zu gelangen, sind vor Auftragserteilung wesentlich höher als danach. Soweit überhaupt Bereitschaft zu Nachbesserungen nach Vertragsschluss besteht, dann häufig nur mit hohem organisatorischem und gegebenenfalls finanziellem Aufwand. Im Extremfall können irreparable Fehler bei der Softwarebeschaffung dazu führen, dass ein IT-Projekt aus Datenschutzgründen abgebrochen werden muss.

1. Hintergrund

1.1 Klassischer Ansatz

Viele Jahre dominierten bei der Softwarebeschaffung Modelle, die rechtlich Kauf- oder Werkvertragscharakter hatten: Der Hersteller liefert eine Software mit den vereinbarten Spezifikationen und der Kunde nimmt die Software ab und zahlt den Preis (Kaufpreis oder Werklohn). Aus Erwerbersicht stand also im Vordergrund, zu prüfen, ob die Software den vereinarten Spezifikationen entspricht, was sich günstigstenfalls in einer förmlichen Abnahme manifestierte.[1)] Mit der Abnahme sind bekannte und teilweise auch unbekannte IST-Abweichungen vom SOLL-Zustand im Regelfall akzeptiert.

Auch für den **Datenschutz** mussten daher erforderliche Eigenschaften der Software frühzeitig spezifiziert werden, um Gegenstand des Leistungsvertrages zu werden, der anschließend tatsächlich umzusetzen war.

Dieser Aspekt der Softwarebeschaffung ist auch nach wie vor aktuell.

1.2 Neuere Entwicklungen

Dazu entwickelt sich jedoch ein neuer[2)] Aspekt: Software as a Service (kurz SaaS) beziehungsweise weitergefasst Cloud Computing.[3)]

Durch SaaS entsteht juristisch formuliert ein Dauerschuldverhältnis. Wirtschaftlich betrachtet entsteht ein neues längerfristiges Abhängigkeitsverhältnis. Während im „klassischen Modell“ der Erwerber einer Software diese theoretisch zeitlich unbegrenzt und praktisch bis zur Obsoleszenz(technische Überholtheit) nutzen konnte, besteht diese Nutzungsmöglichkeit nun nur noch für Zeiträume, in denen der Anbieter dieses tatsächlich gestattet, was üblicherweise von vertraglichen Regelungen (und regelmäßigen Zahlungen des Erwerbers) abhängig ist. Das bedeutet, dass der Erwerber einer Software selbst bei einem vertragstreuen Anbieter jederzeit damit rechnen muss, dass der Anbieter

sein Recht zur ordentlichen Kündigung wahrnimmt und die Software bzw. allgemeiner der Dienst nach Ablauf der Kündigungsfrist nicht mehr zur Verfügung stehen. Das hat Relevanz nicht nur, wenn sich ein Anbieter aus einem Geschäftsfeld zurückzieht sondern auch und vor allem werden mit der Drohung einer Kündigung Vertragsänderungen durchgesetzt.<sup>Lock-in-Effekt|Lock-in-Effekts]]. Überdies besteht die Gefahr, dass in der Insolvenz des Anbieters die Lösung von einem Tag auf den anderen nicht mehr nutzbar ist.

Als **zusätzlicher** Aspekt ist bei der Softwarebeschaffung also zu bedenken, ob SaaS oder On Premises vorzugswürdig ist. Dafür muss in letzter Konsequenz der Lebenszyklus der zu beschaffenden Software bis zum Schluss durchdacht werden. Das alte Gewährleistungsziel der Verfügbarkeit bekommt damit zusätzliche Relevanz.

1.2.1 Kosten

Der Vergleich der Kosten ist im klassischen Fall bezogen auf das Gesamtprojekt relativ einfach, weil die Masse der Kosten einmalig bei der Beschaffung anfällt. Eine Berechnung der Kosten je Zeiteinheit ist dagegen schwierig, weil sie maßgeblich von der Einsatzdauer abhängig ist, die jedoch nur mit großer Unsicherheit geschätzt werden kann.

Bei SaaS sind die Kosten (anfänglichen) Kosten je Zeiteinheit dagegen sehr klar. Die Gesamtkosten des Projekts sind dagegen aufgrund der Unsicherheit bei der Einsatzdauer nur schwer zu schätzen. Etwaige Preisänderungen sind dagegen kaum vorhersagbar.

In beiden Fällen kaum prognostizierbar sind zum Zeitpunkt einer Beschaffungsentscheidung die Kosten für die Einführung einer Ersatzlösung. Das wird im klassischen Fall gemildert durch eine relative große Freiheit, den Zeitpunkt des Ersatzes selbst zu bestimmen. Im Falle von SaaS kann dagegen der Zwang zu einer Ersatzlösung zu ungünstigen Zeitpunkten kommen, z.B. wenn aufgrund einer Uneinigkeit zur Einbindung eines Unterauftragnehmers der Vertrag kurzfristig gekündigt wird. Die Durchsetzung elementarer Anforderungen des Datenschutzes kann also plötzlich sehr teuer werden.

1.2.2 Kündigungsfristen

Daraus ergibt sich ein weiteres in der Vergangenheit eher unbedeutendes Thema, das in kurzer Zeit brisant wurde: Kündigungsfristen.

Die gesetzliche Kündigungsfrist beträgt bei der Miete von Software, was nach deutschem Recht bei SaaS die Regel sein dürfte, gemäß § 580a Abs. 3 Nr. 2 BGB 3(!) Tage.[4)] Um das zu verdeutlichen: Am Montag kann mit Wirkung zum Donnerstag 24 Uhr gekündigt werden. Bei einer Einordnung als Dienstvertrag ist die gesetzliche Kündigungsfrist in Abhängigkeit von dem Zeitraum für den die Vergütung bemessen ist auch nicht viel länger, z.B. kann bei einer monatlichen Vergütung gemäß § 621 Nr. 3 BGB bis zum 15. eines Monats zum Monatsende gekündigt werden.

Selbst ein eher einfaches IT-System wird sich normalerweise nicht in solch kurzen Fristen zu einem anderen Anbieter übertragen lassen.

Folglich bedarf es **zwingend längerer Kündigungsfristen**, für die schon zum Zeitpunkt der Softwarebeschaffung ein Wechselszenario durchgespielt werden muss.

Die (selbst verschuldete) Unmöglichkeit eines Anbieterwechsels ist kein Entschuldigungsgrund für eine datenschutzwidrige Verarbeitung personenbezogener Daten.

1.2.3 Datenportabilität

Um die etwaigen Wechselfristen so kurz wie möglich zu halten, muss ebenfalls noch in der Beschaffungsphase die Datenportabilität geprüft werden. Im Verhältnis Betroffene Person zu Verarbeiter wird das Recht auf Datenübertragbarkeit bisweilen etwas belächelt, weil es in der Praxis allenfalls ein frommer Wunsch ist. Im professionellen Bereich ist dieses Ansinnen des europäischen Gesetzgebers aber geradezu essentiell geworden: Kann der Anbieter mir meine Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ gemäß Art. 20 DSGVO übermitteln und - was nicht in der DSGVO steht- kann ein anderer Anbieter (bzw. bei einer alternativen On-Premises-Lösung die eigene IT-Abteilung) etwas mit diesen Daten anfangen?

Für den oben angesprochenen Notfall der sofortigen Diensteinstellung (typischerweise in der Insolvenz) sollte geprüft werden, ob eine vollständige oder teilweise Speicherung der Daten, die bei dem Anbieter liegen, auf Systemen möglich und sinnvoll ist, die von dem Anbieter unabhängig sind. Um das an einem Beispiel zu verdeutlichen: Eine Datenschutzmanagement-Software (DSMS) wird die Hauptaufgabe haben, dass darüber das Verzeichnis von Verarbeitungstätigkeiten (VVT) geführt wird. Die VVT-Einträge könnten und sollten als PDF-A auch an das Archiv der Organisation übermittelt werden.

2. To Do

Zumindest folgende Punkte sollten im Regelfall bei der Softwarebeschaffung beachtet werden:

- Frühzeitig erste Überlegungen zu einem Datenschutzkonzept anstellen.
- (Betrieblichen oder behördlichen) Datenschutzbeauftragten einbinden.
- Datenschutz schon in der Ausschreibung ansprechen - und zwar möglichst konkret.
- Datenschutz im Leistungsvertrag verankern.
- Kündigungsfristen bei SaaS müssen lang genug für die Implementierung einer Ersatzlösung sein, um gegen Änderungswünsche des Vertragspartner, die für den Datenschutz problematisch sind, gewappnet zu sein.
- Im Falle von Auftragsverarbeitung ist der AV-Vertrag möglichst mit dem Hauptvertrag abzuschließen und nicht im Nachhinein.
- Vorschlag für VVT und Datenschutzerklärung vom Dienstleister unterbreiten zu lassen, ist in vielen Fällen zweckmäßig.
- Datenportabilität in möglichst hohem Umfang sicherstellen durch Tests, rechtliche Absicherung und gegebenenfalls tatsächliche anbieterunabhängige (natürlich datenschutzgerechte!) Speicherung
- Exit-Strategie planen (über Kündigungsfristen und Datenportabilität hinaus)

3. Anforderungen

Software sollte wenigstens folgende Anforderungen erfüllen[5)]:

- Zugriffskontrolle,
- Eingabekontrolle,
- Protokollauswertungen,
- Auskunftserteilung,
- Archivierung und Löschung.

Spezifisch bei SaaS oder hybriden Lösungen sollten folgende Anforderungen erfüllt sein:

- Dokumentation, welche Daten an den Anbieter übermittelt werden und wie die Übermittlung abgesichert ist,
- Zertifizierung der IT-Sicherheit des Anbieters, hilfsweise konkrete Dokumentation der Maßnahmen zur IT-Sicherheit,
- falls Drittstaatenübermittlung vorliegt,
    - Benennung der (aller) Drittstaaten, in die übermittelt wird,
    - Benennung der Rechtsgrundlagen (vgl. Art. 44 ff. DSGVO) für die Übermittlung,
    - Dokumentation der Erfüllung aller Anforderungen einer Drittstaatenübermittlung,
    - bei Übermittlung in die USA, Erklärung, ob der CLOUD Act Anwendung findet(woraufhin die Zulässigkeit der Übermittlung unter diesem Aspekt intensiv zu prüfen ist) oder aufgrund welcher nachzuweisenden Umstände der Cloud Act keine Anwendung finden soll,
- bei Anbietern mit Sitz in den USA oder mit relevanten Anteilseignern in den USA: Nachweis durch den Anbieter, dass eine Übermittlung in die USA technisch ausgeschlossen ist oder falls die Übermittlung nicht technisch ausgeschlossen ist, vollumfängliche Erfüllung der Anforderungen an Übermittlungen in die USA (siehe oben),
- im Falle von Auftragsverarbeitung: ein Muster für einen AV-Vertrag mit Benennung der Unterauftragsverarbeiter,
- bei hohem Schutzbedarf und soweit für die konkrete Anwendung sinnvoll: Ende-zu-Ende Verschlüsselung.

Die Softwareanbieter sollten wenigstens folgende Anforderungen erfüllen:

- Benennung der für den Anbieter zuständigen Aufsichtsbehörde,
- Bestellung eines Datenschutzbeauftragten, (Wenn ein Datenschutzbeauftragter nach dem BDSG nicht bestellt werden muss, ist ein Nachweis erforderlich wie der Datenschutz dann sichergestellt wird. In solchen Fällen ist die freiwillige Bestellung eines DSB vorzugswürdig.)
- Bonität.
- Dokumentation: Wie funktioniert die Software? Beschreibung der Handhabung, Flussdiagramme, FAQ´s etc.

Quellen zur Einschätzung von Anbietern und Produkten

- Tätigkeitsbericht und Stellungnahmen der Datenschutzbehörden (Siehe z.B. Datenschutzkonferenz, Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit)
- Auskünfte bei Frag den Staat

4. Weblinks

- Was muss Software zur Einhaltung der DSGVO können?
- it-sicher.kaufen ein Angebot der Fachhochschule St. Pölten (Aktualisierung unklar)

Artikel

1)

Zur Taktik und möglichen Folgen verzögerter Abnahme:haerting.de:Vorsicht Falle: Rechtsverlust durch Verweigerung der Abnahme in Softwareverträgen, Seite bei archive.org mit Verweis auf BGH, Urteil vom 5. 6. 2014 – VII ZR 276/13, Seite bei archive.org.

2)

So neu ist das Thema eigentlich nicht: Die DATEV betrieb bis 1989 ausschließlich und bis in die 1990er Jahre teilweise einen Service, der nach heutigem Verständnis SaaS war.

3)

Zu den Begrifflichkeiten siehe Software as a Service und Cloud Computing in der Wikipedia.

4)

Vgl. Redeker in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Rn. 224

5)

Vgl. noch zum BDSG Anforderungen an Software: Besser vorher an Datenschutz und IT-Sicherheit denken!.