DataGuard

Whitepaper

Mehr Kunden und schnellere Abschlüsse durch Datenschutzexzellenz – wir erklären, wie das geht.

DATENSCHUTZ ALS WETTBEWERBSVORTEIL – EIN GUIDE FÜR SAAS-ANBIETER

INHALT

HINTERGRUND UND ZIEL DES WHITEPAPERS

„Wo ist denn Ihr Serverstandort?"

„Wie setzen wir Löschanfragen von Betroffenen in Ihrer Lösung um?"

„Wie sieht es mit der Verfügbarkeit der Daten aus?"

„Der Auftragsverarbeitungsvertrag ist lückenhaft."

„Unser Datenschutzbeauftragter braucht mehr Informationen zu […], sonst können wir nicht unterschreiben."

Sind Ihren Vertriebsmitarbeitern diese oder ähnliche Rückfragen auch nur allzu vertraut? Datenschutzbedenken ziehen oftmals Verzögerungen im Vertriebsprozess nach sich oder bedeuten sogar direkt das Ende einer potenziellen Zusammenarbeit. Das Inkrafttreten der DS-GVO hat das Bewusstsein rund um Datensicherheit und Compliance bei Unternehmen zusätzlich noch einmal geschärft.

In der Datenschutz Benchmark-Studie von Cisco (2019) heißt es:

> *„Organisationen profitieren von Datenschutzinvestitionen, die über bloße Compliance hinausgehen. Die Cisco Studie zeigt, dass eine strenge Einhaltung von Compliance-Vorschriften den Vertriebszyklus verkürzt und das Vertrauen von Kunden erhöht."*

Aber was genau müssen SaaS-Anbieter tun, um Ihre Maßnahmen zum Schutz personenbezogener Daten transparent nach außen zu tragen und für den eigenen Wettbewerbsvorteil zu nutzen? Und wie können die richtigen Argumente und Dokumentationen im Vertriebsprozess eingesetzt werden?

Weil wir bei DataGuard nicht nur Datenschutzprofis aus Leidenschaft, sondern selbst Anbieter einer SaaS-Lösung sind, schauen wir gleich aus zwei Perspektiven auf diese Fragestellung. Mit unseren Handlungsempfehlungen möchten wir Ihnen helfen, aus dem Störfaktor Datenschutz ein schlagendes Verkaufsargument zu machen.

DAS BESONDERE VERHÄLTNIS VON SAAS-UNTERNEHMEN ZUM DATENSCHUTZ

Durch das Hosting, Wartungsarbeiten an der SaaS-Lösung oder sonstigen Support übernehmen Sie als Herrsteller einer SaaS-Lösung meist eine Teilleistung von Datenverarbeitungsprozessen, die Sie auf Weisung des entsprechenden Kunden bzw. der Beauftragung durchführen. Demnach sind Sie in den meisten Fällen als Auftragsverarbeiter im Sinne von Art. 28 DS-GVO zu klassifizieren.

Um Anforderungen der DS-GVO zu erfüllen, müssen Sie als SaaS-Anbieter im Auftragsverhältnis mindestens folgende Punkte erfüllen:

- **Gewährleistung geeigneter technischer und organisatorische Maßnahmen zum Schutz personenbezogener Daten des Kunden.**
- **Keine Einschaltung von weiteren Subauftragnehmern ohne vorherige schriftliche Genehmigung des Kunden bzw. Verantwortlichen. Dies ist auch der Fall, wenn ein Dritter zur Bereitstellung von Serverkapazitäten eingeschaltet wird. Im Falle einer allgemeinen schriftlichen Genehmigung, muss der Kunde bzw. Verantwortliche über jede beabsichtigte Hinzuziehung oder Änderung anderer Auftragsverarbeiter informiert werden, damit er die Möglichkeit eines Widerspruchs hat.**
- **Die Schließung eines Auftragsverarbeitungsvertrages mit allen nötigen Elementen aus Art. 28 DS-GVO**

Helfen Sie Ihren Kunden, indem Sie bereits alles zur Schließung eines rechtssicheren Auftragsverarbeitungsvertrages vorbereiten. Am besten so gut, dass der Datenschutzbeauftrage Ihres Kunden keine Rückfragen mehr stellen muss (mehr dazu später).

Neben dem Auftragsverarbeitungsvertrag gibt es drei wesentliche übergeordnete Themen, die Ihnen zu einem Wettbewerbsvorteil verhelfen können:

- **Compliance –** natürlich müssen Sie die Anforderungen der DS-GVO selbst erfüllen. Damit minimieren Sie das Risiko für Datenpannen und Bußgelder. So erfahren Unternehmen, die sich als datenschutzkonform einstufen, weniger Datenpannen als solche, die noch kein gutes Level an DS-GVO-Konformität erreicht haben (Cisco 2019).

- **Transparenz –** die eigenen Datenschutzkonzepte auch nach außen zu zeigen, schafft Vertrauen und einen damit einhergehenden Wettbewerbsvorteil. „Cybersicherheit rückt das Kundenvertrauen in den Mittelpunkt des Wettbewerbs", heißt es im Harvard Business Review. Und weiter: „Es müssen klare und nachvollziehbare Prozesse eingeführt werden, um die Bedeutung des Datenschutzes sowohl innerhalb als auch außerhalb jeder Organisation zu verdeutlichen." Wer seine starken Datenschutzkonzepte gut dokumentiert und kommuniziert, hebt sich ab.

- **Unterstützung –** Wenn Sie Ihre Kunden aktiv bei deren Datenschutzbemühungen entlasten können, positionieren Sie sich als SaaS-Unternehmen ab Tag eins als vertrauenswürdiger Partner. So können Neukunden beispielsweise durch entsprechende Vorlagen, Beispieldokumentationen und vorgeschriebene Absätze bei ihren eigenen Dokumentationspflichten unterstützt werden. Wahrscheinlich kämpfen diese nämlich selbst mit den Datenschutzanforderungen.

In diesem Whitepaper gehen wir auf die Punkte 2 und 3 ein und erklären Ihnen, wie Sie Datenschutz als Verkaufsargument nutzen und sich einen Wettbewerbsvorteil verschaffen können.

Disclaimer: Dieses Whitepaper erhebt keinen Anspruch auf Vollständigkeit.

GRUNDLEGENDES – DIE DS-GVO KURZ ERKLÄRT

(Wenn Sie sich schon auskennen, können Sie diese Seite einfach überspringen.)

- Jeder, der in der EU personenbezogene Daten verarbeitet, ist von der Datenschutz-Grundverordnung (DS-GVO) betroffen und muss eine entsprechende Datenschutzerklärung vorhalten.
- Ziel sind eine maximale Transparenz hinsichtlich der Verarbeitung personenbezogener Daten und ein weitreichender Schutz der Verbraucher.
- Als personenbezogen gelten Daten dann, wenn natürliche Personen mit ihrer Hilfe direkt oder indirekt identifiziert werden können. (Name, Wohnort, Geburtsdatum, Sozialversicherungsnummern, Kontodaten etc.)
- Besonders sensibel sind Daten, die beispielsweise Gesundheitsinformationen, sexuelle Orientierung, Religionszugehörigkeit, politische Meinung, ethnische Herkunft und Rassemerkmale betreffen. Diese bezeichnet die DS-GVO als besondere Kategorien von personenbezogenen Daten und stellt sie unter einen noch weitreichenderen Schutz.
- Unter Datenverarbeitung versteht der Gesetzgeber unter anderem das Erheben, Speichern, Verbreiten und Löschen von Daten.
- In Bezug auf diese Verarbeitungstätigkeiten gilt auch mit der DS-GVO das sogenannte Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass die Datenverarbeitung nur dann zulässig ist, wenn ein gesetzlicher Erlaubnistatbestand dies ausdrücklich zulässt, es also beispielsweise andere Gesetze gibt, die eine Datenverarbeitung explizit fordern.
- SaaS-Unternehmen übernehmen für ihre Kunden oft die Rolle eines Auftragsverarbeiters.
- Ein Datenverantwortlicher bestimmt Zwecke und Mittel der Verarbeitung von personenbezogenen Daten. Ein Datenverarbeiter hingegen führt die Verarbeitung der Daten im Rahmen eines Vertrags durch.
- Sowohl Verantwortliche als auch (Auftrags-)Verarbeiter haften für Verstöße gegen die Datenschutzrichtlinien.

9 SCHLAGENDE DATENSCHUTZ-ARGUMENTE FÜR IHREN WETTBEWERBSVORTEIL

Wussten Sie, dass ungeklärte Datenschutzfragen Vertriebsprozesse im Schnitt um knapp vier Wochen, teilweise sogar ein ganzes Jahr, verzögern? (Quelle: Cisco 2019)

Doch wer gut vorbereitet ist, kann die Bedenken potenzieller Neukunden direkt ausräumen und die Basis für eine gute Geschäftsbeziehung schaffen. Wir erklären Ihnen, welche neun Argumente dabei helfen:

01 Die Implementierung und Kommunikation der Grundsätze „Privacy by Design" und „Privacy by Default"

02 Die Wahl und Dokumentation zum Serverstandort

03 Transparenz hinsichtlich der Verarbeitung personenbezogener Daten, insbesondere von Kundendaten, in Ihrem Unternehmen

04 Technische und organisatorische Maßnahmen (TOM) und ein IT-Sicherheitskonzept

05 Ein starker Auftragsverarbeitungsvertrag (AVV)

06 Die Erarbeitung eines Löschkonzepts, das Kunden unterstützt und Zeit und Geld spart

07 Die Bereitstellung einer Beispieldokumentation für die Risikoeinschätzung und Datenschutz-Folgenabschätzung Ihrer Kunden

08 Eine Aufzeichnung von Datenverarbeitungsflüssen

09 Die Schulung Ihrer eigenen Mitarbeiter

#01
DATA PRIVACY BY DESIGN AND DEFAULT

Sie als SaaS-Anbieter müssen sicherstellen, dass Datenschutzprinzipien schon in den Entwicklungsprozess eingeflossen sind (Data Privacy by Design) und dass die Einstellungen Ihrer Lösung durch Voreinstellungen so datenschutzfreundlich wie möglich gestaltet sind (Data Privacy by Default). Vermeiden Sie z. B., Analysedaten über Nutzerverhalten zu sammeln, die für den Anwendungsfall nicht nötig sind.

Letztendlich zielt das Konzept Data Privacy by Design and Default auf „Datenschutz durch Technikgestaltung" ab. Im Gegensatz zu vielen anderen Punkten hält die DS-GVO sich aber zur konkreten Umsetzung bedeckt. Umso wichtiger also, hier eine fachkundige Beratung einzuholen – von Anfang an. Wir empfehlen daher, mit Ihrem Datenschutzbeauftragen (DSB) zusammenzuarbeiten, der sich bestenfalls besonders gut mit SaaS-verwandten Themen auskennt.

Ihre Software von Anfang an auf Datenschutz auszurichten, erspart Ihnen unangenehme Nachfragen und minimiert die Gefahr von Datenpannen (unerlaubte Weitergabe personenbezogener Daten an Dritte) enorm.

Sie legen bei Ihrem Softwaredesign den Grundstein für den Geschäftserfolg, und das in vielfacher Hinsicht. Natürlich sind Performance, Design und Skalierbarkeit unglaublich wichtig – aber auch der Datenschutz sollte ganz weit oben auf der Prioritätenliste stehen. Teilen Sie Ihren (Neu-)Kunden mit, welche Datenschutzprinzipien in Ihre Softwareentwicklung eingeflossen sind und welche datenschutzfreundlichen Voreinstellungen mitgeliefert werden.

#02
DER RICHTIGE SERVERSTANDORT FÜR SAAS-ANBIETER IM EWR

Wollen Sie mit Ihrer SaaS-Lösung personenbezogene Daten in der EU verarbeiten, sollte ein Serverstandort in der EU oder dem Europäischen Wirtschaftsraum (EWR) angestrebt werden. Steht der Server außerhalb der EU, ist eine Datenverarbeitung über die entsprechende SaaS-Lösung z. B. zulässig, wenn ein Angemessenheitsbeschluss der EU für das entsprechende Land vorliegt oder eine andere sogenannte „geeignete Garantie" zum datenschutzkonformen Datentransfer in ein Drittland vorliegt.

Gerade durch das jüngste Urteil des Europäischen Gerichtshofs (EuGH) zum Privacy Shield ist eine wesentliche dieser geeigneten Garantien zum datenschutzkonformen Versand personenbezogener Daten in die USA nicht mehr gültig. Generell ist durch das Urteil ein Datentransfer in die USA aktuell nicht gänzlich risikofrei durchführbar. Der EuGH hat sich in der Sache „Schrems II" insbesondere zur Frage der Angemessenheit des Datenschutzniveaus in den USA geäußert. Dabei wurde der entsprechende Angemessenheitsbeschluss der EU-Kommission, das sogenannte EU-US Privacy Shield, überprüft und im Ergebnis für nichtig erklärt. (Hier geht es zu unserem ausführlichen Whitepaper mit praxisnahem 11-Punkte-Plan zu diesem Thema.)

Angemessene Garantien für einen Drittlandtransfer können nun die sogenannten „EU-Standarddatenschutzklauseln" darstellen, die Ihre Kunden mit Ihnen als SaaS-Anbieter abschließen können. Hier geht LinkedIn mit gutem Beispiel voran und zeigt, wie effizienter Service aussieht: Die Standardvertragsklauseln finden sich direkt auf der Website, können heruntergeladen und so reibungslos abgeschlossen werden.

Der Serverstandort spielt im Entscheidungsprozess Ihrer Kunden wahrscheinlich eine große Rolle. Wenn Sie den Datentransfer in Drittländer nicht ausschließen können, erleichtern Ihnen schnell verfügbare Standardvertragsklauseln (wie die von LinkedIn) die Vertragsverhandlungen.

#03
TRANSPARENZ ÜBER DEN EIGENEN DATENSCHUTZ

Ein Kernelement der DS-GVO ist die transparente Aufklärung von Nutzern darüber, welche ihrer Daten in welchem Umfang, zu welchem Zweck, wie lange und wo genau erhoben und gespeichert werden. Diese Anforderung geht aus den Informationspflichten aus Kapitel 3 der DS-GVO hervor und umfasst die Datenschutzerklärung und sonstige Informationspflichten.

Die Datenschutzerklärung muss einfach zu verstehen und vollständig sein. Unter anderem muss auf folgende Punkte hingewiesen werden:

- **Die Verwendung von Cookies**
- **Die Übermittlung von Daten an weitere Empfänger**
- **Die Übermittlung in Drittländer und entsprechende geeignete Garantien**
- **Die Verwendung von Plug-ins, die in irgendeiner Form personenbezogene Daten verarbeiten**

Und genau da liegt eine große Chance für Sie, sich bei Neukunden als Datenschutzprofi zu positionieren. Da auch Ihre Kunden die Verwendung Ihrer Software (als Drittanbieter) mit in ihre eigene Datenschutzerklärung aufnehmen müssen, entsteht ein gewisser Dokumentationsaufwand. Und den können Sie minimieren.

Liefern Sie dazu einen aussagekräftigen Absatz mit einer Beschreibung zur Funktionsweise Ihrer Software, der Rechtsgrundlage für die Auftragsverarbeitung, Ihrer Speicherfristen etc. mit. Diesen kann Ihr Kunde dann einfach in seine Dokumentation übernehmen.

#04
TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM) UND EIN IT-SICHERHEITSKONZEPT

Stellen Sie sicher, dass angemessene TOM zum Schutz personenbezogener Daten in Ihrem Produkt implementiert sind (siehe Punkt #1) und erstellen Sie die dazu passende Dokumentation, inkl.:

- **Verschlüsselungsmaßnahmen**
- **Aufschlüsselungen, wer Zugang zu welchen Daten hat**
- **Informationen zur Serverredundanz und Serversicherheit, um Verfügbarkeiten zu garantieren**
- **Ein Vermerk zur Mandantenfähigkeit Ihrer Lösung**
- **Anmerkungen zu Multi-Faktor-Authentifizierung (zum Beispiel für Admins), falls vorhanden**
- **Dem Zweck der erhobenen Daten, um nachzuweisen, dass nur die für die Bereitstellung des Service notwendige Daten erhoben werden.**
- **Informationen zu Patch-Management und regelmäßigen Updates**
- **Hinweise zum Vorgehen bei der Fernwartung**

Die TOM sind das vielleicht wichtigste Dokument im Vertriebsprozess. Sie drücken aus, wie sicher Sie mit den Daten Ihrer Kunden umgehen und sind ein wesentlicher Bestandteil von Auftragsverarbeitungsverträgen. Bereiten Sie diese anhand der oben genannten Punkte daher so auf, dass der DSB des (Neu-)Kunden keinen Grund finden kann, Ihre Lösung abzulehnen. Im Idealfall belegen Sie durch Ihre TOM, dass Sie mindestens genauso hohe Sicherheitsstandards erfüllen wie der Kunde in seinen eigenen, lokalen Prozessen.

#05
EIN STARKER AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

Wahrscheinlich haben Sie schon längst einen AVV erstellt. Aber wie gut kommt dieser bei den DSB Ihrer Kunden an? Gibt es Rückfragen oder Schwierigkeiten? Dann könnte das daran liegen, dass Ihr AVV nicht alles abdeckt, was ein anspruchsvoller DSB sich wünscht.

Stellen Sie zunächst sicher, dass wirklich alle Punkte aus Art. 28 der DS-GVO mit abgedeckt werden.

Viele SaaS-Anbieter können unserer Erfahrung nach besonders an folgenden drei Punkten feilen:

- **Eine wirklich gut definierte Leistungsbeschreibung, aus der genau hervorgeht, welche Teilleistung Sie als AV erbringen**
- **Datenkategorien, die nicht nur oberflächlich, sondern detailliert erklärt sind**
- **Eine Auflistung Ihrer Subauftragsverarbeiter und Nachweise über die Prüfung derer Datensicherheit**

Notiz zu den Subauftragsverarbeitern: In aller Regel setzen Sie als SaaS-Anbieter selbst Lösungen von Drittanbietern ein, z. B. zu Hosting-Zwecken, zur Fernwartung oder für Teilleistungen von individuellen Anpassungen am entsprechenden Tool. Sobald Sie einen weiteren Subauftragnehmer einschalten, haben Sie Sorge dafür zu tragen, dass wesentliche Grundlagen der DS-GVO zu Auftragsverarbeitungsverhältnissen vom Subauftragnehmer eingehalten werden. Sie als SaaS-Anbieter müssen in jedem Fall einen Auftragsverarbeitungsertrag mit solchen Subauftragnehmern schließen und agieren dabei in der Rolle des Verantwortlichen.

Eine eingehende Prüfung jedes Subunternehmers ist Teil des Auswahlprozesses, denn jetzt gilt für Sie: Durch die von Ihnen herangezogenen Drittanbieter sollten Ihnen keine zusätzlichen Sicherheitslücken entstehen.

Ein lückenloser AVV begeistert zwar keine Kunden, sorgt aber für einen reibungslosen Vertriebsprozess. Fehlen grundlegende Informationen nach Art. 28, DS-GVO, gehen unnötigerweise Tage oder Wochen verloren. Wer seinen Kunden einen umfassenden AVV inkl. der Nachweise über die Prüfung seiner Subunternehmer vorlegen kann, beweist Gründlichkeit und Gewissenhaftigkeit und schafft so Vertrauen.

EXKURS:

DAS VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN (VVT)

Anmerkung: Hierbei handelt es sich ausnahmsweise nicht um einen direkten Wettbewerbsvorteil, sondern um einen wichtigen Baustein der DS-GVO-Konformität für SaaS-Unternehmen generell. Wir haben diesen Hinweis zum VVT mit aufgenommen, da dieses oft vergessen wird.

Die meisten SaaS-Anbieter sind in der Regel für fast alle ihrer Kunden als Auftragsverarbeiter zu klassifizieren. Daher ist besonders für SaaS-Anbieter eine besondere Dokumentationspflicht neben dem normalen Verzeichnis von Verarbeitungstätigkeiten zu beachten: das Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter. Dieses Verzeichnis muss z. B. folgende Angaben enthalten:

- **Den Namen und die Kontaktdaten des Auftragsverarbeiters**
- **Eine Auflistung jedes Verantwortlichen (im Anwendungsfall SaaS-Anbieter = Kunde), für den der Auftragsverarbeiter tätig ist**
- **Eine Auflistung von Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden**
- **Falls vorhanden, die Übermittlung von personenbezogenen Daten in ein Drittland außerhalb der EU bzw. des EWR inkl. geeigneter Garantien zur Datenübermittlung**
- **Eine allgemeine Beschreibung der implementierten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten des entsprechenden Verantwortlichen bzw. Kunden**

Die meisten SaaS-Anbieter werden für alle Kunden die gleichen Verarbeitungstätigkeiten durchführen, dabei die gleichen Arten personenbezogener Daten verarbeiten und die gleichen Sicherheitsmaßnahmen für die Tätigkeiten implementiert haben. Darüber hinaus wird der Datentransfer in Drittländer nicht von Kunde zu Kunde abweichen. Daher empfehlen wir zur Effizienz, neben einer allgemeinen Beschreibung der entsprechenden Tätigkeiten, eine Liste zu erstellen, die alle Kunden enthält, für die eine explizite Verarbeitungstätigkeit als Auftragsverarbeiter erfolgt. Dadurch sparen Sie Dokumentationsaufwände und gewährleisten trotzdem eine vollständige Dokumentation wie in der DS-GVO gefordert.

#06
RISIKOEINSCHÄTZUNG UND DATENSCHUTZ-FOLGENABSCHÄTZUNG

Insbesondere beim Einsatz neuer Technologien – die Einführung einer neuen SaaS-Lösung bei Kunden kann in der Regel als neue Technologie klassifiziert werden – können im Verarbeitungsprozess Risiken für Rechte und Freiheiten der Kunden Ihrer Kunden und deren Mitarbeiter entstehen, die eine Datenschutz-Folgenabschätzung erfordern können.

Ihre Kunden sind dazu verpflichtet, zu prüfen, ob durch die Nutzung der neuen SaaS-Lösung ein neues Risiko entsteht und ob dadurch die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung entsteht.

Zwei Beispiele zur Veranschaulichung:

Ein Fall, bei dem die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung wahrscheinlich vorliegt:
Die Einführung einer digitalen Kundendatei über ein Online-CRM bei einem Zahnarzt, der dort Gesundheitsdaten seiner Kunden speichert.

Ein Fall, bei dem diese Notwendig wahrscheinlich nicht vorliegt:
Die Einführung eines CRM bei einem Maschinenbauunternehmen, das dort ausschließlich Geschäftsdaten seiner Kunden speichert (also z. B. keine persönlichen Adressen).

Liegt eine entsprechende Notwendigkeit vor, können Sie Ihren Kunden wieder recht einfach bei der erforderlichen Dokumentation unter die Arme greifen. Am besten fertigen Sie eine Beispieldokumentation an, aus der die wesentlichen Punkte Ihrer Software für eine Datenschutz-Folgenabschätzung hervorgehen (welche Daten werden verarbeitet, in welche Drittländer werden diese übertragen und welche risikominimierenden Maßnahmen werden von Ihnen ergriffen).

Auch hier ersparen Sie Ihren (Neu-)Kunden einen gewissen Zeitaufwand und liefern ein weiteres Verkaufsargument, das Ihre Konkurrenz höchstwahrscheinlich nicht auf dem Schirm hat.

#07
EIN DURCHDACHTES LÖSCHKONZEPT

Das Thema Löschung findet sich gleich mehrmals in der DS-GVO:

Art. 28 DS-GVO

Die Daten Ihrer Kunden müssen nach Abschluss der Erbringung der Leistung – also bei Beendigung des Vertrages – gelöscht werden (Art. 28 Abs. 3 lit. g). (Anmerkung: Es gibt Ausnahmen für diese Regel. Zum Beispiel müssen Rechnungen steuerrechtlich zehn Jahre lang aufbewahrt werden. Auch sie enthalten Daten Ihrer Kunden. In diesem Fall gilt keine Pflicht zur Löschung.)

Um diese Anforderung zu erfüllen, raten wir dazu, eine Datenklassifizierung vorzunehmen. Zeichnen Sie dafür auf, für welche Kategorien personenbezogener Daten welche Löschfristen bestehen (z. B. steuerrelevante Daten bis zu zehn Jahre, Bewerberdaten bis zu sechs Monate, personenbezogene Daten auf Einwilligung: bis zum Widerruf usw.).

Dokumentieren Sie dann, wo diese Daten liegen. Das machen Sie am besten mit einer Aufzeichnung von Datenverarbeitungsflüssen (siehe nächstes Kapitel). Wenn Sie die Daten an Subunternehmen übermittelt haben, müssen diese ebenfalls über die Löschung informiert werden.

Die Löschung personenbezogener Daten Ihrer Kunden kommt meist erst zum Ende der Geschäftsbeziehung zum Tragen, ist aber wichtig, um nicht durch fahrlässige Fehler Imageschäden oder gar Bußgelder zu riskieren.

Art. 17 DS-GVO

Das Recht auf Vergessenwerden (Art. 17 DS-GVO) sieht vor, dass personenbezogene Daten unverzüglich gelöscht werden, sobald die Daten zum ursprünglichen Verarbeitungszweck nicht mehr notwendig sind oder die betroffene Person ihre Einwilligung widerrufen hat.

Als Auftragsverarbeiter müssen Sie grundsätzlich bei der Durchführung von Löschanfragen durch Betroffene, die bei Ihren Kunden eingehen, unterstützen. Ihre Software muss dafür eine vollständige Löschung zulassen. Am besten bauen Sie hier direkt eine entsprechende Funktionalität ein, die Ihr Kunde über die Bedienoberfläche nutzen kann. Das erspart Ihnen viel Zeitaufwand und macht auch Ihren Kunden den Arbeitsalltag leichter. Gibt es eine solche Funktionalität nicht, muss jede Löschanfrage manuell bearbeitet werden.

Auch hier gilt wieder: Die Daten müssen aus Ihrem System verschwinden, aber auch aus den Systemen aller Subunternehmer. Und dazu braucht es wiederum die Aufzeichnung von Datenverarbeitungsflüssen.

Kunden freuen sich über eine einfache Funktion zum vollständigen Löschen personenbezogener Daten Ihrer Kunden und fragen – je nach Lösung – gleich zu Beginn des Vertriebsprozesses danach. Ein typischer Fall von „Low Hanging Fruit" ist hier die Entwicklung eines entsprechenden Features.

#08
EINE AUFZEICHNUNG VON DATENVERARBEITUNGSFLÜSSEN

Um Daten zu schützen oder zu löschen, müssen Sie zunächst wissen, wo diese Daten überhaupt liegen.

Wir empfehlen, eine Prozesslandkarte aufzubauen. Sie enthält alle Prozesse, die mit automatischen Verarbeitungsanlagen zu tun haben. Diese Prozesslandkarte kann ein einfaches Excel-Dokument sein oder ein umfangreiches PDF. Wichtig ist nur, dass sie alle Cloudaktivitäten abbildet und zeigt, welche Daten wann von welchem System oder Server wohin fließen. Am besten verknüpfen Sie diese Prozesslandkarte mit den Datenkategorien aus Punkt #7.

Vorsicht bei unstrukturierten Daten: Unter unstrukturierten Daten versteht man Daten, die nicht eindeutig zugeordnet werden können. An ihnen lässt sich nicht erkennen, ob es sich um personenbezogene Daten oder sogar sensible Daten handelt, da ihre Beziehung zum ursprünglichen Datenset nicht mehr nachvollziehbar ist. Diese Daten sind datenschutzrechtlich besonders bedenklich und sollten vermieden werden – auch da kann eine Aufzeichnung der Datenverarbeitungsflüsse helfen.

Der Wettbewerbsvorteil durch diese Maßnahme ist ein indirekter – die Aufzeichnung von Datenverarbeitungsflüssen ermöglicht erst andere wichtige Schritte, wie die Erstellung eines überzeugenden Löschkonzeptes. Sie kann außerdem in die TOM mit aufgenommen werden.

#09
MITARBEITERSCHULUNGEN

Sie können technisch den besten Datenschutz der Welt implementiert haben, Ihre Verträge können lückenlos sein und jeder Subunternehmer kann eingehend geprüft worden sein – wenn ein neu angelernter Supportmitarbeiter einen Kunden nach seinem Passwort fragt, sensible Daten ausgedruckt im Büro umherschwirren oder einfach so neue Plug-ins installiert werden, waren trotzdem alle Mühen umsonst.

Das sieht auch der Gesetzgeber so und hat in der DS-GVO eine verpflichtende Mitarbeiterschulung zum Thema Datenschutz aufgenommen. Der DSB muss Mitarbeiter nach Art. 39 Abs. 1 lit. b dahingehend schulen, dass sie die Daten der Kunden datenschutzrechtlich korrekt verarbeiten. Das kann zum Beispiel als Teil des Einarbeitungsprozesses geschehen oder in E-Learnings.

Ihre Mitarbeiter sind die wichtigste Schnittstelle zu Ihren Kunden. Wenn ein Vertriebsmitarbeiter in Vertragsverhandlungen vertrauliche Daten eines anderen Kunden ausplaudert, kann Sie das den Vertragsabschluss kosten (wenn nicht sogar rechtliche Konsequenzen nach sich ziehen). Generische Trainings sind aus unserer Sicht nur bedingt hilfreich. Am besten erstellen Sie Schulungsmaterialien speziell für die verschiedenen Rollen im Unternehmen.

Datenschutz steht und fällt mit Ihren Mitarbeitern. Um Ihre Bemühungen rund um den Datenschutz nach außen zu tragen und Kunden von Ihrer Verlässlichkeit zu überzeugen, müssen Ihre Mitarbeiter Bescheid wissen.

DATENSCHUTZ, DER BEGEISTERT – ZUSAMMENFASSUNG

Datenschutz ist viel mehr als nur eine gesetzliche Verpflichtung. Gut umgesetzt, dokumentiert und kommuniziert kann ein Datenschutzkonzept Ihnen dabei helfen:

- **Ihre eigene Compliance zu gewährleisten**
- **Mit Transparenz das Vertrauen von Kunden zu gewinnen**
- **Durch proaktive Unterstützung Ihrer Kunden hinsichtlich Ihrer Datenschutzbemühungen von Anfang an zu glänzen**

Salesforce fand heraus, dass 84 % der befragten Nutzer den Unternehmen gegenüber loyaler sind, die starke Sicherheitsmaßnahmen nachweisen können. Mit unseren neun Punkten für Ihren Wettbewerbsvorteil beweisen Sie Umsicht beim Datenschutz und leisten sogar wertvolle Vorarbeit für Ihre Kunden – in einem Umfang, der Ihre Konkurrenz wahrscheinlich abhängt.

Weil wir verstehen, wie überwältigend diese Aufgabe für SaaS-Unternehmen sein kann, stehen wir Ihnen natürlich jederzeit persönlich für Fragen zur Verfügung. Wir freuen uns auf einen Austausch!

ÜBER DEN AUTOR

Tobias Theelen

Berater für Datenschutzrecht
bei DataGuard

DataGuard