Der große Datenschutz-Report 2025

FÜR DIGITALE PROZESS AGENTUREN

EINLEITUNG

Der Datenschutz ist 2025 weiterhin ein zentrales Thema für viele Unternehmen – und insbesondere für digitale Prozessagenturen, die SaaS-Lösungen implementieren und dazu beraten.

Alle Agenturen haben im Laufe der Zeit mit dem Thema auf die ein oder andere Weise zu tun.
Durch die Einführung und Verwaltung von SaaS-Lösungen stehen auch Agenturen im Fokus den Datenschutz sicherzustellen.
Es ist entscheidend, sicherzustellen, dass alle Prozesse datenschutzkonform und transparent sind.

Die Datenschutz-Grundverordnung (DSGVO) und andere Gesetze können hohe Anforderungen an die Verarbeitung personenbezogener Daten und den damit verbundenen Dokumentationspflichten, stellen.

Um als Agentur nicht nur rechtliche Risiken zu minimieren, sondern auch das Vertrauen deiner Kunden zu gewinnen und zu behalten, ist es wichtig, Datenschutz in jede Implementierung zu integrieren.

Dieser Report bietet dir eine umfassende Anleitung, wie du den Datenschutz in der Beratung und Implementierung von SaaS-Standardlösungen effektiv managen kannst.

Du wirst lernen, welche Herausforderungen dabei auftreten können, wie du die Datenschutzanforderungen richtig umsetzt und wie du den Datenschutz als Verkaufsargument nutzt, um das Vertrauen deiner Kunden zu stärken.

Und letztlich wie du vermeidest, dass deine Kunden durch Bußgelder und Sanktionen der Aufsichtsbehörden geschädigt werden.

SUMMARY

Datenschutz ist ein zentraler Punkt, wenn es um SaaS-Implementierung und -Beratung geht. Besonders für digitale Prozessagenturen, die mittelständische Unternehmen bei der Auswahl, Implementierung und Wartung von SaaS-Lösungen unterstützen, wird es immer wichtiger, Datenschutz zu priorisieren.

Der Report gibt dir praxisorientierte Ansätze, wie du Datenschutz-anforderungen in jeder Phase der SaaS-Einführung umsetzt und dokumentierst.

• **Die größten Herausforderungen:** Ich zeige dir, wo es oft hakt, wenn digitale Prozessagenturen SaaS-Lösungen für ihre Kunden einführen. Das fängt bei der Anpassung an die individuellen Datenschutzanforderungen an und hört bei der Regelung der Datenverarbeitung im Wartungsprozess noch lange nicht auf.

• **Aktuelle Änderungen der DSGVO:** Ich zeige, wie sich die DSGVO weiterentwickelt und welche neuen Anforderungen du bei der Implementierung von SaaS-Lösungen beachten musst.

• **Datenschutz und Automatisierung:** Automatisierung und SaaS gehen Hand in Hand. Doch wie sorgst du dafür, dass deine automatisierten Systeme immer DSGVO-konform bleiben? Ich gebe dir praxisorientierte Lösungen für den Datenschutz in automatisierten Prozessen.

• **Vertrauen aufbauen:** Datenschutz ist nicht nur eine rechtliche Verpflichtung, sondern auch ein wichtiger Verkaufsfaktor. Ich zeige dir, wie du den Datenschutz als Mehrwert und USP in deiner Agentur nutzt.

Dieser Report liefert dir die nötigen Werkzeuge, um Datenschutz nicht nur als Herausforderung zu sehen, sondern als strategischen Vorteil in deiner Arbeit als digitale Prozessagentur.

WER ICH BIN

Ich bin Jasmin Lieffering, Spezialistin im Bereich Datenschutz für digitale Geschäftsmodelle .

Seit 2016 bin ich im Datenschutz als externe Datenschutzbeauftragte, Beraterin und Projektbegleitung für Agenturen, SaaS-Hersteller, IoT-Anbieter und KI-Unternehmen auch international tätig.

Als TÜV-zertifizierte Datenschutzbeauftragte liegt der Schwerpunkt darauf, digitale Prozessagenturen mit praxisnahen Lösungen auszustatten, die Datenschutz nicht nur als Pflicht, sondern als strategischen Vorteil begreifen. Datenschutzkonforme Implementierungen und transparente Prozesse schaffen Vertrauen und stärken die Position am Markt.

Die Onlinekurse bieten strukturierte, anwendungsorientierte Inhalte, die es ermöglichen, Datenschutz effizient in den Unternehmensalltag zu integrieren. Statt trockener Theorie stehen praxisnahe Strategien im Fokus, die direkt in der Beratung und Umsetzung von SaaS-Lösungen angewendet werden können.

Ein klarer, umsetzbarer Ansatz macht es leicht, die gesetzlichen Anforderungen zu erfüllen und gleichzeitig Datenschutz als überzeugendes Verkaufsargument zu nutzen. So wird nicht nur Rechtssicherheit geschaffen, sondern auch ein nachhaltiger Wettbewerbsvorteil aufgebaut.

Ich freue mich, dir mit diesem Report wertvolle Insights zu liefern, damit du deine Agentur 2025 noch erfolgreicher im Bereich SaaS-Implementierung positionieren kannst.

Falls du noch Fragen hast, schreibe mir gerne eine Email an: info@litc.de

1. DIE GRÖSSTEN DATENSCHUTZ-HERAUSFORDERUNGEN

Digitale Prozessagenturen, die SaaS-Lösungen implementieren und dazu beraten, sehen sich mit einer Vielzahl von Datenschutzherausforderungen konfrontiert. Diese Herausforderungen betreffen sowohl die technische als auch die organisatorische Ebene. Die zentralen Herausforderungen sind:

1.1 Unzureichende Anpassung an individuelle Datenschutzbedürfnisse der Kunden

SaaS-Standardlösungen bieten eine allgemeine Infrastruktur, die nicht immer den spezifischen Datenschutzanforderungen des jeweiligen Kunden gerecht werden. Ein Beispiel: Ein mittelständisches Unternehmen könnte in seiner Branche sehr strengen Vorschriften unterliegen (z. B. im Gesundheitswesen oder im Finanzsektor), während eine allgemeine SaaS-Lösung möglicherweise nicht alle regulatorischen Anforderungen erfüllt.

Lösung: Agenturen müssen sicherstellen, dass sie die individuellen Datenschutzbedürfnisse jedes Kunden erkennen und berücksichtigen.

Das bedeutet, dass die SaaS-Lösung angepasst werden muss, z. B. durch zusätzliche Sicherheitsfunktionen oder Anpassungen in der Datenverarbeitung.
Daher ist es keine schlechte Idee vor der Implementierung ein Datenschutz-Audit oder zumindest einen kurzen Datenschutz-Check-up des Kunden durchzuführen.

So ein Prozess stellt sicher, dass relevanten Datenschutz-Vorgaben erkannt und berücksichtigt werden.

Beispiel: CRM-System
Ein SaaS-Anbieter stellt eine Lösung für das CRM zur Verfügung. Wenn Kunden (Nutzer) deiner Agentur in der EU ansässig sind, musst du sicherstellen, dass das SaaS den Anforderungen der DSGVO entspricht.

1.2 Mangelnde Dokumentation der Datenschutzprozesse

Die DSGVO verlangt eine lückenlose Dokumentation aller Prozesse, bei denen personenbezogene Daten verarbeitet werden.
Für digitale Prozessagenturen, die SaaS-Lösungen implementieren, stellt sich die Frage, wie diese Prozesse von Anfang an dokumentiert und nachvollziehbar gemacht werden können.

Lösung: Jede SaaS-Implementierung sollte mit einer detaillierten Dokumentation der Datenverarbeitungsprozesse beginnen. Dies umfasst nicht nur die Beschreibung der Datenflüsse, sondern auch der getroffenen Sicherheitsmaßnahmen (wie Verschlüsselung) und der Art der erfassten Daten.

Eine vollständige Dokumentation sollte auch die technischen und organisatorischen Maßnahmen (TOMs) umfassen, die während der Implementierung und des laufenden Betriebs von SaaS-Lösungen ergriffen werden.

Beispiel: Bei der Implementierung einer SaaS-Lösung für eine Finanzberatung muss deine Agentur alle Schritte der Datenverarbeitung dokumentieren, von der Erhebung personenbezogener Daten über deren Speicherung bis hin zur Löschung gemäß des Löschkonzeptes. Diese Dokumentation ist sowohl für interne Prüfungen als auch für etwaige externe Datenschutz-Audits erforderlich.

1.3 Unklare Regelungen bei der Datenverarbeitung während Wartung und Support

Häufig wird auch während der laufenden Wartung und Support-Leistung der Datenschutz vergessen. Gerade wenn personenbezogene Daten im laufenden Betrieb verarbeitet werden (z. B. durch Updates, Fehlerbehebung oder Anpassungen), muss der Datenschutz ebenfalls gewährleistet sein.

Auf der anderen Seite darf auch nicht vergessen werden, das diese Leistungen für den Kunden dokumentiert werden müssen.

Lösung: Agenturen sollten klare vertragliche Regelungen treffen, die die Verarbeitung von Daten im Wartungs- und Supportprozess regeln. Dies betrifft insbesondere den Zugang zu Kundendaten durch Support-Mitarbeiter und Subunternehmer aber auch Protokollpflichten der Einsätze. Die DSGVO verlangt, dass diese Prozesse transparent und nachvollziehbar sind, und dass alle beteiligten Parteien (z. B. externe IT-Dienstleister) ebenfalls DSGVO-konform arbeiten.

Beispiel: Ein Kunde stellt fest, dass die gespeicherten Kundendaten aufgrund eines Softwarefehlers korrigiert werden müssen. In diesem Fall muss der Supportmitarbeiter auf die betroffenen Daten zugreifen können. Um DSGVO-konform zu handeln, muss im Vorfeld festgelegt worden sein, dass Supportmitarbeiter nur auf die für die Fehlerbehebung notwendigen Daten zugreifen dürfen und dies nur unter strengen Sicherheitsvorkehrungen (z. B. Zwei-Faktor-Authentifizierung, Protokollierung des Zugriffs), sowie dass der Vorgang genau protokolliert wann welche Änderungen von wem durchgeführt wurden.

1.4 Vertrags- und Vereinbarungsmanagement

Die richtigen Verträge und Vereinbarungen sind entscheidend, um sicherzustellen, dass die SaaS-Lösungen DSGVO-konform eingesetzt werden können.

Besonders wichtig sind hier die sogenannten Auftragsverarbeitungsverträge (AVV), die zwischen der Agentur, dem SaaS-Anbieter und dem Endkunden abgeschlossen werden müssen.

Lösung: Der Vertrag muss genau festlegen, wer für welche Datenverarbeitung verantwortlich ist, welche Sicherheitsmaßnahmen ergriffen werden und wie der Datenschutz während der gesamten Lebensdauer der SaaS-Lösung gewährleistet wird. Ein spezifischer Punkt ist die Auswahl der Subunternehmer des SaaS-Anbieters – auch hier müssen klare datenschutzrechtliche Vereinbarungen getroffen werden.

Beispiel: Ein SaaS-Anbieter hat Subunternehmer für bestimmte Teile seiner Cloud-Infrastruktur (z. B. für die Speicherung von Daten in einem Rechenzentrum). Deine Agentur muss sicherstellen, dass der SaaS-Anbieter eine Vereinbarung zur Auftragsverarbeitung hat, die die Subunternehmer einbezieht, und dass diese Vereinbarung den Datenschutzanforderungen der DSGVO entspricht.

1.5 Schulung der Mitarbeiter und der Kunden

Ein weiterer oft übersehener Punkt ist die kontinuierliche Schulung sowohl der Mitarbeiter der Agenturen als auch der Mitarbeiter der Kunden.Nur durch regelmäßige Schulungen und die Sensibilisierung für Datenschutzaspekte kann sichergestellt werden, dass alle Beteiligten ihre Verpflichtungen kennen und einhalten.

Lösung: Regelmäßige Schulungen sollten für alle Mitarbeiter angeboten werden, die mit SaaS-Implementierungen und Support zu tun haben. Dazu gehören auch Schulungen für die Kunden, die die SaaS-Lösung nutzen.

Die Schulungen sollten nicht nur auf rechtliche Anforderungen eingehen, sondern auch praxisorientierte Tipps und Tools bereitstellen, wie datenschutzrechtliche Anforderungen im Arbeitsalltag umgesetzt werden können.

Beispiel: Ein Kunde, der eine SaaS-Lösung zur Verwaltung von Kundendaten implementiert hat, sollte alle relevanten Mitarbeiter schulen, damit diese verstehen, wie die Lösung sicher genutzt wird und welche Datenschutzmaßnahmen und Prozesse beachtet werden müssen, etwa bei der Handhabung von Kundendaten in der Software. Dies kann auch durch deine Agentur angeboten werden.

2. AKTUELLE DSGVO-ÄNDERUNGEN

Die Rechtssprechung zur Datenschutz-Grundverordnung (DSGVO) wird noch weitere strengere Anpassungen in der täglichen Arbeit für SaaS-Agenturen bereithalten. Einige der wichtigsten Änderungen betreffen die SaaS-Implementierungen:

2.1 Erweiterte Transparenzanforderungen bei der Datenverarbeitung

Ab 2025 könnte die DSGVO-Rechtssprechung mehr Transparenz bei der Datenverarbeitung von SaaS-Anwendungen verlangen. Besonders wichtig wird es, die Kunden detailliert über die Art und Weise zu informieren, wie ihre Daten in der Lösung verarbeitet werden – und das nicht nur einmal zu Beginn der Nutzung, sondern laufend.

Lösung: Deine Agentur sollte sicherstellen, dass alle betroffenen Personen über den gesamten Lebenszyklus ihrer Daten informiert werden. Dies könnte durch die Implementierung von klaren und verständlichen Datenschutzrichtlinien innerhalb der SaaS-Lösung sowie durch regelmäßige Updates zur Datenverarbeitung erfolgen.

Beispiel: Wenn eine SaaS-Lösung personenbezogene Daten durch ein automatisiertes System verarbeitet, müssen die Endbenutzer klar verstehen, wie ihre Daten durch das System verarbeitet werden – z. B. in einer leicht verständlichen Datenschutzerklärung oder durch interaktive Hinweise in der Software.

2.2 Stärkere Kontrolle bei Subunternehmern und Dritten

Mit der Zunahme von Cloud-basierten SaaS-Lösungen müssen Agenturen darauf achten, dass Subunternehmer, die die Daten verarbeiten, ebenfalls den Datenschutzanforderungen der DSGVO entsprechen. Auch die Rolle des Subunternehmers im Rahmen der Datenverarbeitung muss explizit im Vertrag festgehalten werden. Hier sind auch aktuelle Entwicklungen bezüglich von personenbezogenen Daten in Drittstaaten wie die USA zu beachten.

Lösung: Agenturen sollten genau dokumentieren, welche Subunternehmer involviert sind, und sicherstellen, dass sie entsprechende vertragliche Vereinbarungen treffen, die den Datenschutz und die Sicherheit der Daten gewährleisten.

Beispiel: Wenn ein SaaS-Anbieter auf einen externen Cloud-Provider zurückgreift, muss der Vertrag mit dem Cloud-Provider auch die Datenschutzanforderungen und die Zugriffskontrollen ansprechen, um eine DSGVO-konforme Verarbeitung zu garantieren. Bei Subunternehmer in Drittländern wie die USA muss überprüft werden ob die Datenverarbeitung und Speicherung der Daten in den USA oder in Europa stattfindet

2.3 Verantwortung bei Wartung und Support

Die DSGVO macht keine Ausnahme bei Leistungen wie Wartung und Support. Auch hier müssen Agenturen sicherstellen, dass keine unbefugten Datenzugriffe stattfinden und dass alle Datenverarbeitungsprozesse weiterhin den Datenschutzrichtlinien entsprechen.

Lösung: Agenturen sollten nicht nur beim initialen Setup der SaaS-Lösung auf Datenschutz achten, sondern auch regelmäßige Prüfungen der Systeme durchführen, um sicherzustellen, dass auch bei der Wartung alle Datenverarbeitungsprozesse transparent und sicher sind.

Beispiel: Wenn ein SaaS-Anbieter Software-Updates durchführt, die Daten betreffen, muss deine Agentur sicherstellen, dass keine personenbezogenen Daten ohne ausdrückliche Zustimmung des Kunden verarbeitet oder offengelegt werden.

3. DATENSCHUTZ UND AUTOMATISIERUNG

Die Implementierung von SaaS-Lösungen erfordert zunehmend den Einsatz von Automatisierung. Die Herausforderungen und Chancen im Bereich Datenschutz steigen, da Unternehmen auf automatisierte Systeme angewiesen sind, um ihre Daten effizient zu verarbeiten und zu verwalten. Doch wie lässt sich sicherstellen, dass diese Automatisierungsprozesse weiterhin DSGVO-konform bleiben?

3.1 Automatisierte Datenaufbewahrung und -löschung

Ein zentraler Grundsatz der DSGVO ist die Datenminimierung – die Vermeidung der Speicherung unnötiger personenbezogener Daten. Zudem müssen personenbezogene Daten nach dem Erreichen des Verarbeitungszwecks gelöscht werden. Automatisierte Systeme können dabei helfen, diese Anforderungen zu erfüllen, indem sie die Datenverwaltung und Löschung effizient und ohne menschliche Fehler durchführen.

Lösung: Implementiere automatisierte Mechanismen, die Daten gemäß der festgelegten Aufbewahrungsrichtlinie regelmäßig löschen, sobald sie nicht mehr benötigt werden. Dies kann z.B. durch das Setzen eines automatischen Löschzeitpunkts oder durch die automatische Archivierung von Daten erfolgen. Automatisierungstools können dabei helfen, diese Prozesse systematisch und fehlerfrei umzusetzen.

Beispiel: In einem CRM kann die automatische Löschung von Kundendaten eingerichtet werden. Wenn ein Kunde seine Geschäftsbeziehung beendet oder seine Einwilligung zur Verarbeitung widerruft, werden die Daten gelöscht. Dies könnte durch ein integriertes System geschehen, das automatisch die Daten eines abgemeldeten Kunden nach einer festgelegten Frist entfernt, um der DSGVO-Anforderung der Datenminimierung gerecht zu werden.

3.2 Pseudonymisierung und Anonymisierung

Pseudonymisierung und Anonymisierung sind zwei wichtige Konzepte, die den Datenschutz im Rahmen von Automatisierung und Datenverarbeitung sichern.

Lösung: Nutze die Möglichkeit, personenbezogene Daten bei der Automatisierung durch Pseudonymisierung zu schützen.

In Fällen, in denen Daten langfristig verarbeitet, aber nicht mehr eindeutig einer Person zugeordnet werden müssen, kann die Anonymisierung eine zusätzliche Schutzmaßnahme darstellen. Dies ist besonders wichtig in Bereichen wie der Datenanalyse oder bei der Erstellung von Reports, in denen personenbezogene Daten nicht unmittelbar erforderlich sind.

Beispiel: Wenn ein SaaS-Anbieter eine Datenbank mit Kundentransaktionsdaten führt, können sensible Informationen wie Namen und Adressen pseudonymisiert werden, sodass die Identität des Kunden im System nicht mehr direkt ersichtlich ist. Nur autorisierte Mitarbeiter mit speziellen Berechtigungen haben Zugriff auf die vollständige Identität der Person. Bei der Analyse von Verkaufsdaten können diese dann anonymisiert werden, um sicherzustellen, dass keine personenbezogenen Daten verarbeitet werden.

3.3 Regelmäßige Audits und Datenschutz-Monitoring

Automatisierte Systeme zur Datenverarbeitung sollten regelmäßig auf ihre DSGVO-Konformität geprüft werden. Dies bedeutet, dass ein kontinuierlicher Monitoring-Prozess etabliert werden muss, um sicherzustellen, dass keine Sicherheitslücken oder Datenschutzverstöße auftreten.

Lösung: Implementiere Datenschutz-Monitoring-Tools, die kontinuierlich die Einhaltung der Datenschutzrichtlinien überwachen. Zudem sollten regelmäßige Audits oder kleinere Check-ups durchgeführt werden, um sicherzustellen, dass die Datenverarbeitung den rechtlichen Anforderungen entspricht und keine Risiken bestehen. Dies kann entweder durch interne Prüfungen oder durch externe Datenschützer erfolgen, die die Prozesse überprüfen und gegebenenfalls Anpassungen vornehmen.

Beispiel: Ein SaaS-Anbieter für Personalmanagement-Software könnte regelmäßig automatisierte Prüfungen durchführen, um sicherzustellen, dass die personenbezogenen Daten von Mitarbeitern, wie z. B. Gehaltsdaten, ausschließlich zu den vereinbarten Zwecken verarbeitet und nicht unbefugt weitergegeben oder gespeichert werden. Im Rahmen eines Audits könnten auch alle Verarbeitungsschritte überprüft und dokumentiert werden, um vollständige Transparenz über die Datenverarbeitung zu gewährleisten. Die Ergebnisse des Audits können mit den Kunden der Agentur geteilt werden.

4. KUNDENVERTRAUEN AUFBAUEN:
DATENSCHUTZ ALS VERKAUFSARGUMENT

In der heutigen Geschäftswelt legen Unternehmen zunehmend Wert auf Datenschutz, besonders bei der Auswahl von SaaS-Lösungen.
Das ist bei den Sanktionen, Bußgeldern und seit neustem auch Schadensersatzforderungen verständlich. Um das Vertrauen von Kunden zu gewinnen und als Experte im Bereich Digitale Prozesse zu positionieren, ist Datenschutz nicht nur als rechtliche Notwendigkeit zu verstehen, sondern kann auch als Wettbewerbsvorteil genutzt werden.

4.1 Datenschutz als Mehrwert und USP

Wenn digitale Prozessagenturen Software-as-a-Service-Lösungen für Kunden implementieren, kann der Datenschutz als ein entscheidenderer Mehrwert in den Vordergrund gestellt werden. Das bedeutet, dass die Sicherheits- und Datenschutzmaßnahmen nicht nur als Pflicht, sondern auch als eine der Stärken der Lösung präsentiert werden können.

Lösung: Verwandle den Datenschutz in einen USP. Informiere deine Kunden darüber, wie du die Implementierung der SaaS-Lösungen sicher und DSGVO-konform gestaltest und welche zusätzlichen Maßnahmen du für deren Sicherheit triffst.
Positioniere dich als die Agentur, die den höchsten Wert auf Datenschutz legt und diesen aktiv kommuniziert.

Beispiel: Ein SaaS-Anbieter für die Buchhaltung von kleinen und mittelständischen Unternehmen könnte als besonderes Verkaufsargument hervorheben, dass alle Daten in einer hochverschlüsselten Cloud gespeichert und regelmäßig durch externe Sicherheitsfirmen geprüft werden. Dies könntest du auch in deiner Verkaufspräsentation oder in Marketingmaterialien ausdrücklich betonen.

4.2 Transparente Kommunikation

Kunden möchten wissen, wie ihre Daten verarbeitet werden – und sie möchten sicher sein, dass ihre Daten sicher sind. Transparenz ist daher ein entscheidender Faktor, um Vertrauen aufzubauen. Dies bedeutet, dass du offen kommunizierst, wie die Daten verarbeitet werden und welche Sicherheitsmaßnahmen getroffen wurden.
Das gleiche gilt auch für die Kunden und Mitarbeiter der Kunden. Dein Kunde ist sogar dazu verpflichtet seine Kunden und Mitarbeiter über die Verarbeitungsprozesse in seinem Unternehmen zu informieren.

Lösung: Stelle sicher, dass du klare, verständliche und detaillierte Datenschutzhinweise bereitstellst, die genau erklären, wie die Daten verarbeitet und gesichert werden. Du kannst auch Datenschutzhinweise bereitstellen, die deine Kunden an ihre Mitarbeiter und Kunden rausgeben können. Dies gilt sowohl für die von dir implementierten SaaS-Lösungen als auch für die laufende Wartung und den Support. Zusätzlich kannst du regelmäßig Updates zur Sicherheit und zu eventuellen Änderungen der Datenschutzpraktiken anbieten.

Beispiel: Bei der Implementierung einer HR-Software für einen mittelständischen Kunden könntest du regelmäßig über die Sicherheitseinstellungen und den Datenschutzstatus der Lösung informieren. Beispielsweise durch monatliche Updates oder regelmäßige Datenschutzberichte, die dem Kunden einen Überblick über alle durchgeführten Sicherheitsmaßnahmen und etwaige Veränderungen im System geben.
Du könntest auch Datenschutzhinweise erstellen oder erstellen lassen und diese an deine Kunden rausgeben, so dass sie ihrer Informationspflicht gegenüber ihren Mitarbeitern nachkommen können.

4.3 Zertifikate, Audits und Datenschutzbeauftragte

Ein weiteres starkes Verkaufsargument ist der Nachweis der DSGVO-Konformität. Kunden suchen oft nach Anbietern, die offiziell zertifiziert sind, um sicherzustellen, dass alle gesetzlichen Anforderungen erfüllt werden.

Lösung: Strebe Zertifikate und Audits an, die die Datenschutzpraktiken deiner Agentur belegen. Dies umfasst insbesondere die ISO 27001 für Informationssicherheit oder das TÜV-Siegel für Datenschutz. Biete diese Nachweise in deiner Kommunikation an, um das Vertrauen deiner Kunden zu stärken.
Auch die Bestellung eines Datenschutzbeauftragten erhöht das Vertrauen deiner Kunden in dich. Denn damit wird ein Ansprechpartner für Datenschutz bereit gestellt.

Beispiel: Bei der Implementierung einer SaaS-Lösung für ein größeres Unternehmen könnte es für das Unternehmen entscheidend sein, dass der SaaS-Anbieter und die implementierende Agentur ISO 27001 zertifiziert sind. Diese Zertifikate zeigen, dass du nicht nur gesetzliche Vorgaben einhältst, sondern auch proaktiv hohe Sicherheitsstandards umsetzt.
Für manche Unternehmen sind Datenschutzbeauftragte, die regelmäßig die Agenturen beraten eine Anforderung um überhaupt in die nähere Auswahl zu kommen.

5. PRAKTISCHE SCHRITTE:
DEINE AGENTUR FÜR DEN DATENSCHUTZ FIT MACHEN

Der Erfolg einer Agentur im Bereich der digitalen Prozess-Implementierung hängt auch davon ab, wie gut du die oben genannten Aspekte in deinen Arbeitsalltag integrierst und dauerhaft sicherstellst, dass alle Prozesse den Datenschutzanforderungen entsprechen. Hier sind praktische Schritte, die du umsetzen kannst:

5.1 Schulung und Sensibilisierung
Die Grundlage für ein datenschutzkonformes Arbeiten in deiner Agentur ist die Schulung deiner Mitarbeiter. Datenschutz ist eine gemeinsame Verantwortung, und alle Mitarbeiter müssen mit den relevanten Vorschriften und Prozessen vertraut sein.

Lösung: Organisiere regelmäßige Schulungen für alle Mitarbeiter, die mit SaaS-Implementierungen und der Wartung von Softwarelösungen zu tun haben. Dies umfasst sowohl datenschutzrechtliche Grundlagen als auch praktische Anwendungstipps zur sicheren Verarbeitung von personenbezogenen Daten.

.**Beispiel:** Du könntest regelmäßig Workshops anbieten, in denen die Mitarbeiter lernen, wie sie Daten in der Cloud sicher verwalten, welche Schritte erforderlich sind, um Datenschutzverletzungen zu vermeiden, und welche Tools ihnen helfen, Daten DSGVO-konform zu verarbeiten, welche Kundenanforderungen sie umsetzen dürfen und wann sie aufpassen müssen.

5.2 Verträge und Vereinbarungen prüfen

Die Vertragsprüfung ist essenziell, um sicherzustellen, dass alle Datenschutzanforderungen rechtlich abgesichert sind. Achte darauf, dass alle Verträge mit deinen Kunden und SaaS-Anbietern den aktuellen Datenschutzbestimmungen entsprechen.

Lösung: Überprüfe alle bestehenden Verträge und stelle sicher, dass sie die notwendigen Datenschutzklauseln enthalten. Achte besonders auf die Auftragsverarbeitungsverträge mit deinen SaaS-Anbietern und Kunden sowie auf die Verschwiegenheitserklärungen in Arbeitsverträgen mit deinen Mitarbeitern.

Beispiel: Bei der Vertragsgestaltung mit einem SaaS-Anbieter für eine neue CRM-Lösung kannst du sicherstellen, dass der Vertrag explizit regelt, wie der Anbieter personenbezogene Daten verarbeitet und schützt. Du kannst diese auch durch einen Datenschützer prüfen lassen.

MEINE LÖSUNGEN FÜR DICH

„Datenschutz ist kein NICE-TO-HAVE sondern ein MUST-DO. Wer es klug angeht, schafft keine Papiertiger sondern bessere Prozesse und echten Mehrwert für die Kunden.“

Als Spezialistin für digitale Geschäftsmodelle und TÜV-zertifizierte Datenschutzbeauftragte habe ich seit 2016 SaaS-Anbieter, Digital Agenturen und IT-Dienstleister auf unterschiedliche Weise begleitet. Dabei hat sich herausgestellt, dass die nachhaltigste Methode, das Do-it-Yourself ist,

Do-it-yourself - die nachhaltigste Form der Begleitung

Hier setzt es voraus, dass du selber Zeit investierst und dich in die Thematik tief einarbeitest.

Datenschutz für dich als Agentur:
Der **Datenschutz-Club** geht auf deinen eigenen Datenschutz ein. Du bekommst alles was du für den Datenschutz in deinem Business brauchst. Von Marketing& Sales über Businessmodelle, interne Prozesse zu Technik und Auftragsverarbeitung, Zusammenarbeit mit freien und angestellten Mitarbeitern und vielen weiteren Themen. Infos findest du hier: https://litc.tentary.com/p/d0lKXh

Datenschutz für Digitale Prozess Agenturen
In diesem Onlinekurs bekommst du alles zum Datenschutz rund um das Geschäftsmodell deiner Agentur. Du erfährst worauf di achten musst in der Abreit mit deinen Kunden und wie du die Lösungen dafür bereitstellst. Wie du Datenschutz als USP einsetzen kannst. Das Produkt befindet sich noch im Aufbau du kannst dich hier in eine Wartelist eintragen und ich informiere dich über den Verkaufsstart: https://litc.tentary.com/p/kMpBpX

Bei Fragen schreib mir gerne eine email an info@litc.de