

WHITEPAPER DATENSCHUTZ ALS WETTBEWERBSVORTEIL FÜR START-UPS





INHALT

- 03 Warum ist Datenschutz in meinem Start-up so wichtig?**
 - 1. Strategische Vorteile durch ein hohes Datenschutzniveau
 - 2. Datenschutzfragen verzögern den Vertrieb
 - 3. DSGVO-Konformität und Strafen
- 04 Wieso ist Kundenvertrauen wichtig für die Wettbewerbsfähigkeit?**
- 05 Datenschutz-Basics**
- 06 Was müssen besonders Start-ups beachten**
 - 1. Umgang mit Daten im Start-up
 - 2. Braucht mein Startup einen Datenschutzbeauftragten?
 - 3. Besonderheiten für SaaS-Anbieter
- 08 Wie wird Datenschutz zum Wettbewerbsvorteil?**
 - 1. Basiskompetenz im Bereich des Datenschutzes
 - 2. Mitarbeiterschulungen
 - 3. Wahl des Servserstandorts
 - 4. IT-Sicherheitskonzept
 - 5. Löschkonzept
 - 6. Kommunizieren Sie Ihre Maßnahmen im Datenschutz!
 - 7. Datenschutzbeauftragter als Innovationsbeschleunigung
- 11 Noch 5 Tipps zum Schluss**
- 12 Ihre Ansprechpartner**

WARUM IST DATENSCHUTZ IN MEINEM START-UP SO WICHTIG?

Strategische Vorteile durch ein hohes Datenschutzniveau



Kunden erwarten einen korrekten Umgang mit ihren Daten. Verbraucher werden sich immer mehr bewusst, was ein Missbrauch ihrer Daten für ihr Privat- und Berufsleben bedeuten kann. Wenn ein Start-up von Beginn an eine professionelle Lösung findet und somit Probleme vermeidet, kann Datenschutz zu einem Marketing-Argument werden. Auf der geschäftlichen Ebene erleichtert der Datenschutz die Zusammenarbeit mit Partnern, sowie den Einstieg von Investoren. In diesen Situationen ist ein exaktes und konformes Datenschutzkonzept und korrekte Dokumentation notwendig, um Verzögerungen oder Verhandlungsabbrüche zu vermeiden.

Datenschutzfragen verzögern den Vertrieb



Die Bedeutung von Datenschutz nimmt auf geschäftlicher sowie privater Seite zu. Der Umgang mit und Schutz von Daten ist mittlerweile Teil der Kaufentscheidung. Daher sollten auch die Vertriebsmitarbeiter an einer rechtskonformen Datenschutzlösung interessiert und darüber informiert sein, um im Verkaufsgespräch offene Fragen beantworten zu können. Ungeklärte Datenschutzfragen verzögern den Vertriebsprozess im Durchschnitt um vier Wochen (Quelle: Cisco 2019).

DSGVO-Konformität und Strafen



Das vermeintlich lästige Thema des Datenschutzes erstmal beiseite schieben, kann sich für junge Unternehmen schnell rächen. Strafen für Verstöße treffen sowohl neue als auch große, etablierte Unternehmen. Des Weiteren führen anfängliche Versäumnisse oft dazu, dass später aufwändige Anpassungen vorgenommen werden müssen, oft motiviert durch Abmahnungen bezüglich des Umgangs mit dem Datenschutz. Die in der Datenschutzgrundverordnung (DSGVO) festgelegten Bußgelder können sehr hoch ausfallen (bis zu 20 Millionen Euro bzw. 4% des Umsatzes) und den Fortbestand des Unternehmens gefährden.



Heißt das, Start-ups müssen sich jetzt warm anziehen?

Nein, Start-ups müssen jetzt nicht pauschal Angst haben. Die in der DSGVO vorgesehenen Sanktionsmöglichkeiten sollten keine Angst machen, sondern die Unternehmen dazu motivieren, den Datenschutz als einen Wettbewerbsvorteil zu verstehen. Es macht Sinn, Datenschutz als Qualitätsmerkmal bei Unternehmensentscheidungen stärker zu berücksichtigen. Auch weil das Ignorieren teuer werden kann.

WIESO IST KUNDENVERTRAUEN WICHTIG FÜR DIE WETTBEWERBSFÄHIGKEIT?

In vielen Branchen, vor allem aber im digitalen Bereich, ist die Auswahl an Anbietern und Produkten durch das Internet und die zunehmende Globalisierung immens groß. Um einen Kunden erfolgreich zu werben, setzt dies sein Grundvertrauen voraus, dass entstehen muss und nicht verletzt werden darf.



57% der Verbraucher würden ihre Geschäfte mit einem Unternehmen beenden, das ihre personenbezogenen Daten unsachgemäß verwendet.

(Quelle: cognizant, 2016)

Daher ist Datenschutz nicht nur eine Frage der DSGVO-Konformität, sondern hat Auswirkungen auf Reputation, Kundenvertrauen und Wettbewerbsfähigkeit. Besonders wenn ein Verstoß eine hohe Strafe nach sich zieht, folgt auch meist eine öffentliche Wirkung. Der entsprechende Imageschaden verringert das Kundenvertrauen erheblich. Während Kundenzufriedenheit erst nach dem Kauf beginnt, ist das Vertrauen bereits davor eine notwendige Voraussetzung für eine positive Kaufentscheidung.



37%
der Verbraucher

würden gerichtlich gegen ein Unternehmen vorgehen, das Daten unsachgemäß verwendet.



57%
der Verbraucher

würden ihre Geschäfte mit einem Unternehmen beenden, das ihre personenbezogenen Daten unsachgemäß verwendet.



50%
der Verbraucher

sind bereit einem Unternehmen, dem sie vertrauen, mehr zu zahlen.

Quelle: cognizant



DATENSCHUTZ-BASICS

Ein oft zitierter Ausdruck - "Daten sind das neue Öl" - sieht Daten als wertvolles Gut unserer Zeit. Dies ist das Ergebnis einer Entwicklung aus der zunehmenden Digitalisierung der letzten Jahrzehnte, die es stark erleichtert, große Mengen an Daten zu verarbeiten. Deshalb beschränken sich die Entwicklungen auch nicht auf die Digitalindustrie, sondern haben die gesamte Wirtschaft erfasst. Die Folgen sind vielschichtig: Zum einen hilft das Sammeln von Daten Unternehmen ihre Produkte und Dienstleistungen genauer und individueller auf die Wünsche der Kunden anzupassen. Zum anderen ist es nun von größter Relevanz, Datenmissbrauch zu vermeiden und Individuen davor zu schützen, dass Dritte ihre Daten frei verwenden.



Um den Schutz Privater zu stärken, trat die DSGVO, die EU-weit gilt, in Kraft. Sie trifft Regelungen für den Umgang mit den personenbezogenen Daten natürlicher Personen - und setzt damit Unternehmen online und offline klare Grenzen ihres Handelns.

Personenbezogene Daten

Laut DSGVO sind personenbezogene Daten Informationen, die Rückschlüsse auf eine natürliche Person erlauben. Sie sind besonders geschützt, weil ihre freie Verwendung negative Auswirkungen auf die betroffene natürliche Person haben kann und die freie Entfaltung ihrer Persönlichkeit gefährdet.

z.B.:

- **Vorname und Nachname**
- **E-Mail-Adresse**
- **Adresse**
- **Telefonnummer**
- **IP-Adresse eines Internetnutzers**

Datenschutz im Internet

Auch im Internet und bei der Gestaltung von Websites sind die Regelungen der DSGVO zu beachten. Sie führen zum Beispiel dazu, dass Betreiber von Websites die Einwilligung eines Seitenbesuchers erfragen müssen, bevor sie die meisten Cookies setzen. Cookies sind kleine Textbausteine, die im Browser eines Nutzers gespeichert werden und Informationen enthalten. Die Pflicht, die DSGVO auch im Internet zu beachten, tritt neben weitere gesetzliche Pflichten, z.B. ein Impressum vorzuhalten.



WAS MÜSSEN BESONDERS START-UPS BEACHTEN?

Umgang mit Daten im Start-up

Auch wenn das Geschäftsfeld eines Start-ups nicht direkt mit Daten in Verbindung steht, muss es die Vorschriften des Datenschutzes beachten. Dabei hilft ein Datenschutzbeauftragter sehr. Im Rahmen vieler Tätigkeiten in einem Start-up stellen sich Fragen, die am besten ein Experte beantwortet.

Das betrifft z.B.:

- **die Verwendung privater Laptops oder Mobilgeräte (BYOD),**
- **das Speichern von Daten in einer Cloud oder**
- **das Versenden von Newslettern.**

Bei den genannten Tätigkeiten kann es leicht zu Datenschutzverletzungen kommen. Deswegen ist es wichtig, entsprechende Maßnahmen zu ergreifen, beispielsweise Auftragsverarbeitungsverträge mit externen Dienstleistern zu schließen. Um diese Herausforderungen zu meistern oder zumindest effizient anzugehen, empfiehlt es sich einen Datenschutzbeauftragten hinzuzuziehen.

Braucht mein Start-up einen Datenschutzbeauftragten?

Wenn eines oder mehrere der folgenden Kriterien auf Ihr Unternehmen zutrifft, dann JA:

- Ihr Unternehmen hat 20 oder mehr Beschäftigte
- Sie schützen Ihr Büro mit einer Überwachungskamera.
- Der Umgang mit besonderen Kategorien von personenbezogenen Daten gehört zu ihrem Geschäftsfeld, z.B. von Gesundheitsdaten, Daten zur ethnischen Herkunft, politischen Meinung, religiösen Überzeugung oder zum Sexualleben von Personen.
- Es werden personenbezogene Daten verarbeitet, um sie geschäftsmäßig zu übermitteln. Dies ist bei vielen Personal-Unternehmen der Fall, z.B. Recruiter- oder Headhunter, trifft aber auch auf zahlreiche Marketingagenturen zu.
- Sie verarbeiten regelmäßig Daten von Personen unter 16 Jahren.



Die Benutzung von SaaS-Tools

SaaS-Tools sind für die Arbeit von Start-ups besonders wichtig, weil sie günstiger und schneller verfügbar sind als traditionelle Desktop-Software. Die Nutzung von SaaS-Tools ist ohne eine Verarbeitung personenbezogener Daten nicht vorstellbar. Somit unterliegen SaaS-Anbieter und ihre Kunden den Bestimmungen des Datenschutzes.

Die DSGVO unterscheidet zwischen sogenannten Verantwortlichen und Auftragsverarbeitern. Auftragsverarbeiter sind externe Unternehmen wie SaaS-Anbieter, an die Verantwortliche Aufgaben ausgelagert haben. Beide - Verantwortliche und Auftragsverarbeiter - müssen die Vorschriften der DSGVO befolgen und haften für Verstöße.

Das müssen Sie im Hinblick auf SaaS-Tools beachten:

- 01.** Verwenden Sie nur seriöse Tools. Wenn Sie einen externen Anbieter einschalten, trifft Sie die Pflicht, ihn auch zu überwachen.
- 02.** Passen Sie bei Anbietern von außerhalb der EU auf. Sie dürfen an diese nur Daten weitergeben, wenn ihre Sicherheit durch konkrete Vorschriften und Vorkehrungen gesichert ist. Das ist ein häufig geprüftes Thema von Aufsichtsbehörden.
- 03.** Informieren Sie ihre Kunden ausreichend über die Verwendung des Tools. Das ist vor allem dann notwendig, wenn der Anbieter des Tools außerhalb der EU sitzt.



WIE WIRD IHR DATENSCHUTZ ZUM WETTBEWERBSVORTEIL?

-
- 01** Expertise im Bereich des Datenschutzes
 - 02** Mitarbeiterschulungen
 - 03** Wahl des Serverstandorts
 - 04** IT-Sicherheitskonzept
 - 05** Löschkonzept
 - 06** Kommunizieren Sie Ihre Maßnahmen im Datenschutz!
 - 07** Datenschutzbeauftragter als Innovationsbeschleunigung



#01

Expertise im Bereich des Datenschutzes

Expertise im Datenschutz ist geschäftsentscheidend. Die überschaubaren Kosten eines Datenschutzbeauftragten rentieren sich meist schon nach wenigen Monaten. Insbesondere kann es vorteilhaft sein, bereits einen Datenschutzbeauftragten hinzuziehen, wenn noch keine akuten Probleme bestehen. Ein Datenschutzbeauftragter kann verhindern, dass es überhaupt erst zu Problemen kommt, und dazu beitragen, dass Datenschutz Teil der Unternehmenskultur wird. Externe Datenschutzbeauftragte sind günstiger als interne und verfügen häufig über einen besseren Gesamtüberblick in der Branche.

#02

Mitarbeiterschulungen

Mitarbeiterschulungen sind ein wichtiger Baustein der Datenschutz-Compliance. Geschulte Mitarbeiter minimieren außerdem das Risiko von Bußgeldern, weil die Mitarbeiter dafür sensibilisiert sind, was datenschutzkonform ist. Im Datenschutz geschulte Vertriebsmitarbeiter können nicht nur mit neuen Verkaufsargumenten punkten, sondern haben auch ein Verständnis für mögliche Vorbehalte von Kunden und können mit Lösungen reagieren. Des Weiteren verstehen Mitarbeiter, dass Datenschutz wichtig ist, und wissen das Engagement des Unternehmens zu schätzen. So haben Mitarbeiterschulungen auch einen positiven Einfluss auf die Stimmung im Unternehmen.

#03

Wahl des Serverstandorts

Wählen Sie Ihren Serverstandort so, dass Sie attraktiv für Kunden sind. Ein Serverstandort in den USA schneidet Ihnen wichtiges Geschäft in Europa ab. Auch hier hilft, Datenschutzgesetze von Anfang an zu befolgen, um sich richtig am Markt zu positionieren. Spätere Änderungen sind teuer und führen zu Frustration bei den Mitarbeitern.

#04

IT-Sicherheitskonzept

Ein IT-Sicherheitskonzept hilft, den Überblick über die Schutzmaßnahmen eines Unternehmens zu behalten und verhindert teure Datenschutzverletzungen durch Systemausfälle, den Verlust von Know-how oder Entwendung von Daten. Maßnahmen der Verschlüsselung oder die Trennung von Daten verschiedener Kunden helfen sehr konkret, Datenschutzverletzungen ganz zu vermeiden oder, falls sie dennoch eintreten, ihre Gefahr einzudämmen. Eine Übersicht über sogenannte technische und organisatorische Maßnahmen (TOMs) dokumentiert den Stand der Schutzmaßnahmen.



#05

Löschkonzept

Ein Löschkonzept hält fest, nach welchen Kriterien und zu welchem Zeitpunkt Daten in einem Unternehmen gelöscht werden. Die Erstellung kann je nach Größe und Geschäftsfeld des Unternehmens ein aufwendiger Prozess sein - der sich auszahlt! Nicht nur gehen Aufsichtsbehörden gegen die zeitlich unbegrenzte Speicherung von Daten - auch Datenfriedhöfe genannt - rigoros vor und verteilen hohe Bußgelder. Auch sehen Kunden die unbefristete Speicherung ihrer Daten sehr kritisch. Hier früh ein Konzept zu verfolgen, erspart lästige Arbeit zu einem späteren Zeitpunkt, z.B. kurz vor einer Finanzierungsrunde oder wenn die Aufsichtsbehörde schon "vor der Tür" steht. Dennoch sollte nicht wild gelöscht werden, weil Unternehmen sogar gesetzlich verpflichtet sind, bestimmte Daten für vorgeschriebene Zeitspannen aufzubewahren.

#06

Kommunizieren Sie Ihre Maßnahmen im Datenschutz!

Unternehmen rühmen sich gerne damit, dass sie emissionsfrei sind. Ihre Kunden sehen das als Zeichen dafür, dass das Unternehmen verantwortungsvoll geführt wird. Auch die Einhaltung datenschutzrechtlicher Vorschriften ist geeignet, Kunden das gesellschaftliche Verantwortungsbewusstsein von Unternehmen zu zeigen. Hier können Sie sich leicht von Ihren Wettbewerbern abheben!

#07

Datenschutzbeauftragter als Innovationsbeschleunigung

Datenschutz wird gelegentlich als Innovationsbremse gesehen. Zu Unrecht! Ein Datenschutzbeauftragter nimmt Unternehmen die Angst vor Datenschutz. Indem er Prozesse im Unternehmen von Anfang an verfolgt und gestaltend tätig wird, schafft es das Unternehmen Datenschutz rechtzeitig zu berücksichtigen und sogar zu seiner Stärke zu machen. Datenschutzkonforme Produkte und Dienstleistungen bestehen besser im Markt als ihre Konkurrenz, die kurzsichtig die Vorschriften ignoriert.



NOCH 5 TIPPS ZUM SCHLUSS

#01

Seien Sie proaktiv nicht reaktiv, präventiv nicht korrigierend!

Handeln Sie nicht erst, wenn es zu spät ist oder drängt. Beste Ergebnisse im Datenschutz erzielen Sie durch vorausschauende Planung. Ruhen Sie sich deshalb nicht darauf aus, dass Ihr Unternehmen noch "zu klein" für professionelle Datenschutzberatung ist oder dass sie - über ein veraltetes oder ungenutztes System - bereits im Datenschutz abgesichert sind. heyData gibt Ihnen mit der heyData-Plattform ein innovatives Datenschutz-Tool an die Hand, das Ihnen wirklich helfen wird.

#02

Private Handys und Computer

Besonders junge Unternehmen starten mit begrenzten Ressourcen und vermischen auch auf der technischen Ebene Privat- und Berufsleben. Wenn Sie private Mobilgeräte verwenden, können Sie leicht und unabsichtlich gegen Datenschutzregelungen verstoßen. Auch wenn die Ressourcen für eine Trennung der Geräte fehlen, sollten Sie zumindest festlegen, welche Software für Unternehmenszwecke verwendet werden darf und welche nicht.

#03

Seien Sie transparent!

Nur etwa jeder fünfte Kunde liest die Datenschutzerklärung (Quelle: Data Ethics, 2016). Sie eignet sich deshalb nicht wirklich als Kanal, das Thema Datenschutz für Kunden interessant zu machen. Gerade deshalb können Sie für zusätzliche Transparenz sorgen, indem Sie dem Kunden weitere, leicht verständliche Informationen in Werbekampagnen zur Verfügung stellen.

#04

Gehen Sie sparsam mit Daten um!

Speichern Sie nicht mehr Daten als wirklich notwendig. Sind bestimmte Daten nicht für den Abschluss eines Vertrags oder die Durchführung einer Transaktion wichtig, erheben Sie sie am besten gar nicht erst. Daten, die sie nicht haben, müssen sie auch nicht schützen. Ihr Datenschutzbeauftragter hilft Ihnen gern, die Daten zu bestimmen, die sie tatsächlich benötigen.

#05

Verwenden Sie sichere Passwörter!

Ein ausgefeiltes Datenschutzkonzept ist ein Segen, aber die Sicherheit beginnt bereits im Kleinen. Unsichere Passwörter bieten Dritten, die es darauf anlegen, einen leichten Zugang zu Ihren Systemen. Achten Sie darauf, dass Passwörter mindestens 8 Zeichen haben, Sonderzeichen beinhalten und keine Namen oder bekannte Bezeichnungen enthalten.

Haben Sie Fragen zu diesem Paper oder allgemein zum Datenschutz?

- ▷ Unsere Experten prüfen Ihr Unternehmen gern in einem unverbindlichen Beratungsgespräch auf Datenschutzlücken.



Im Vertrieb
Miloš Djurdjević
Geschäftsführer
milos@heydata.eu



Ihr Datenschutzberater
Rechtsanwalt Martin Bastius
Chief Legal Officer
support@heydata.eu