Teamleader

DSGVO: WIE SIE IHR UNTERNEHMEN RICHTIG VORBEREITEN

DIGITALISIERUNG UND PRODUKTIVITÄT

EINFÜHRUNG

Teamleader

DANKESCHÖN!

Vielen Dank, dass Sie sich dieses E-Book heruntergeladen haben. Teilen Sie es gerne mit Ihren Kontakten und Kollegen.

UBER TEAMLEADER

FOLLOW US

WAS MÜSSEN SIE ÜBER DIE DSGVO WISSEN?

Bald ist es so weit: Nicht mehr lange, und die von der Europäischen Union durchgesetzte DSGVO oder auch Datenschutz-Grundverordnung tritt in Kraft. Sie enthält Vorschriften zum Schutz natürlicher Personen, Regelungen für die Verarbeitung dieser personenbezogenen Daten sowie zum freien Verkehr solcher Daten. In diesem E-Book klären wir, was die Datenschutz-Grundverordnung ist, was die Anforderungen bei der Verwaltung personenbezogener Daten konkret sind, und wie Sie sich und Ihr Unternehmen darauf vorbereiten.

DIE ÜBERHOLTEN EUROPÄISCHEN RECHTSVORSCHRIFTEN

Aktuell gilt für Unternehmen in der EU die europäische Datenschutzrichtlinie. Diese europäische Richtlinie zu Privatsphäre und Datenschutz stammt noch aus dem Jahre 1995. Den EU-Ländern wird bei der Umsetzung von Richtlinien ein gewisser Spielraum eingeräumt, so dass sie bestimmten nationalen Besonderheiten Rechnung tragen können. Jedes Land kann sich daher dafür entscheiden, strengere Vorschriften einzuführen. Aus diesem Grund unterscheiden sich die Datenschutzbestimmungen in der EU von Land zu Land, was die Situation für Unternehmen mit internationaler Präsenz erschwert und verkompliziert.

Es liegt auf der Hand, dass die Welt seit 1995 massive digitale Umwälzungen erlebt hat. Durch die zunehmende Nutzung von Cloud-Diensten und sozialen Medien ist auch der Datenschutz stärker in den Mittelpunkt gerückt. Es nur konsequent, dass auch die Gesetzgebung zum Thema Datenerfassung und -verarbeitung unbedingt angepasst werden muss, und dass das im besten Interesse aller ist: sowohl aus Unternehmens- als auch aus Kundenperspektive.

Der Trend zum Cloud Computing und die Erfordernis der DSGVO

Dass der Trend in Richtung Cloud Computing geht, lässt sich nicht übersehen: Heutzutage spielt sich fast alles in der Cloud ab. Europäische Unternehmen werden umfassend dabei unterstützt, ihren Digitalisierungsprozess voranzutreiben, wobei Cloud Computing zweifellos besondere Bedeutung zukommt. Durch Initiativen wie zum Beispiel den Europäischen Digitalen Binnenmarkt und die Europäische Cloud-Initiative werden europäische Unternehmer auf dem Weg in die Cloud unterstützt und begleitet:

„Cloud-Computing entwickelt sich rasant. Schätzungen zufolge könnten diese Entwicklungen dazu führen, dass der Cloud-Markt in Europa von 9,5 Milliarden € im Jahre 2013 bis 2020 auf 44,8 Milliarden anwachsen kann, sich der Marktumfang in dieser Zeit also verfünffacht.“ (Die Europäische Kommission zum Thema Cloud-Computing)

Mit der Zunahme des Cloud Computing wächst auch der Anspruch an Sicherheit und das **Sicherheitsbedürfnis.**

Die DSGVO vereinheitlicht den Datenschutz innerhalb der EU

Wenn die DSGVO am 25. Mai 2018 in Kraft tritt, sind alle europäischen Länder an dieselben Datenschutzvorschriften gebunden. **Wenn Ihr Unternehmen den Anforderungen der DSGVO entspricht, dann befinden Sie sich im Wesentlichen[1] auch im Einklang mit den Datenschutzgesetzen aller europäischen Länder.**

Die neue DSGVO ist eine Verordnung, wohingegen die vorherigen Vorschriften auf Richtlinien beruht haben. Der Hauptunterschied?

- **Verordnung:** ein verbindlicher Rechtsakt, den alle EU-Länder in vollem Umfang umsetzen müssen.
- **Richtlinie:** ein Rechtsakt, in dem ein von allen EU-Ländern zu erreichendes Ziel festgelegt wird. Es ist Sache der einzelnen Länder, eigene Rechtsvorschriften zur Verwirklichung dieses Ziels zu erlassen. Eine Richtlinie ist in den EU-Ländern nicht unmittelbar anwendbar und sollte erst noch in nationales Recht umgesetzt werden, bevor Regierungen, Unternehmen und Einzelpersonen sie anwenden können.

Welches Risiko gehen Unternehmen ein, die sich nicht an die Verordnung halten?

Die Verordnung legt fest, dass Unternehmen, die die Anforderungen der DSGVO nicht erfüllen, eine durch die lokale Aufsichtsbehörde verhängte Geldbuße riskieren, die bis zu 4 Prozent ihres Jahresumsatzes betragen kann. **Jedes Unternehmen sollte angemessene Maßnahmen ergreifen, die Anforderungen der Datenschutzverordnung bis zum 25. Mai 2018 zu erfüllen,** z.B. indem es eine Datenschutzerklärung bereitstellt und ein Konzept zum Umgang mit Datenschutzverletzungen erstellt (vgl. Artikel 83,4 und 83,5 der DSGVO).

Für Kunden, die einem Unternehmen ihre Daten überlassen, ist wichtig, wie und wo diese Daten gespeichert und weiterverarbeitet werden. So haben Untersuchungen der britischen Datenschutzbehörde ICO (Information Commissioner's Office) ergeben, dass nur 20 % der britischen Bevölkerung Unternehmen und Organisationen vertrauen, die ihre personenbezogenen Daten speichern. Entsprechend gehört es zu den größten Risiken von Unternehmen, (potenzielle) Kunden zu verlieren, denn eine Nichterfüllung der DSGVO kann sich massiv auf **das Vertrauen Ihrer Kunden auswirken und den Ruf Ihres Unternehmens schädigen.**

[1] Da es sich bei der DSGVO um eine besondere Verordnung handelt, die es den EU-Ländern ermöglicht, strengere Regeln einzuführen, sollte jedes Unternehmen überprüfen, ob es nationale Unterschiede gibt. So legt die DSGVO beispielsweise das Alter von Kindern auf 16 Jahre oder jünger fest. Manche Länder, wie z.B. Frankreich und Belgien, werden diese Altersgrenze auf 13 Jahre absenken. Das österreichische Datenschutzgesetz setzt diese Altersgrenze mit dem vollendeten 14. Lebensjahr fest, Deutschland hat das Alter bislang nicht herabgesetzt.

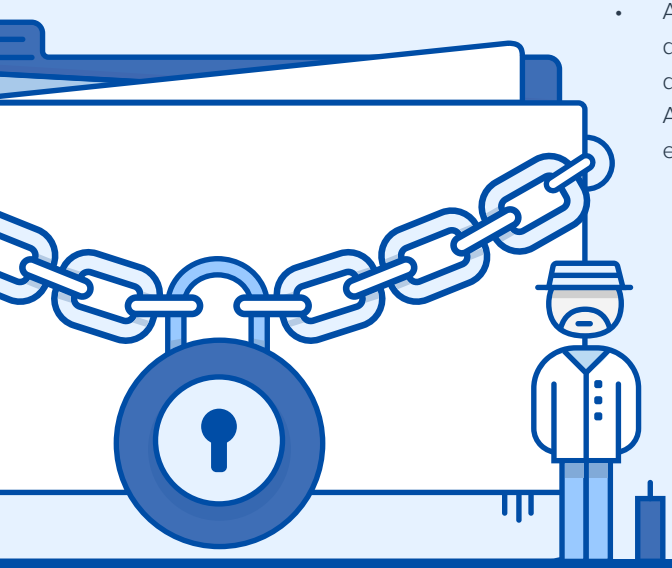
Zwar bedeutet die Einhaltung der Verordnung einen beträchtlichen Arbeitsaufwand - vor allem für kleine und mittlere Unternehmen, die ihre Unternehmensabläufe auf Konformität überprüfen müssen, die Regelung bringt Unternehmen aber auch einige Vorteile:

- Größere Transparenz darüber, wie und wofür Daten erhoben werden, kann **das Vertrauen der Kunden vergrößern.**
- Dadurch, dass die DSGVO verbindliches Recht ist, wird Ihr Unternehmen den Anforderungen der **Datenschutzvorschriften in ganz Europa entsprechen**. Dadurch wird es einfacher, in andere europäische Länder zu expandieren.
- Der Rechtsrahmen der DSGVO wird dazu führen, dass **personenbezogene Daten auf nachhaltigere Weise gesammelt und verarbeitet** werden, da er Unternehmen dazu anhält, personenbezogene Daten an einem einzigen Ort zusammenzuführen. Dadurch lassen sie sich leichter auffinden und bearbeiten. Jedoch: Die Kundenverwaltung ohne entsprechende Software wird schwerer.

Das eigentliche Ziel der DSGVO ist, **jedem Menschen die Kontrolle über seine personenbezogenen Daten zurückzugeben.** Indem Ihr Unternehmen die erforderlichen Strategien und Maßnahmen ergreift, sichert es sich gleichzeitig für die Zukunft ab.

Die Grundprinzipien der DSGVO

Für viele Unternehmen gehört das Sammeln, Verarbeiten und Austauschen personenbezogener Daten zu ihrem Tagesgeschäft. Die DSGVO hat einen zweifachen Anwendungsbereich:



1. **Sachlicher Anwendungsbereich:** Die DSGVO findet Anwendung, sobald personenbezogene Daten verarbeitet werden
2. **Räumlicher Anwendungsbereich:** Die DSGVO findet Anwendung:

- Wenn Sie in der EU niedergelassen sind und im Rahmen Ihrer Tätigkeiten personenbezogene Daten verarbeiten, unabhängig davon, ob die Verarbeitung dieser Daten in der EU stattfindet oder nicht, und unabhängig davon, ob Sie als Verantwortlicher oder Auftragsverarbeiter agieren (siehe unten).
- Auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der EU befinden (also nicht nur beschränkt auf EU-Bürger), durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter, sofern die Datenverarbeitung im Zusammenhang mit einer der folgenden Aktivitäten steht:
  - wenn betroffenen Personen in der EU Waren oder Dienstleistungen angeboten werden (unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist)
  - wenn das Verhalten betroffener Personen in der EU beobachtet wird, soweit ihr Verhalten in der EU stattfindet

Es ist auch wichtig, festzustellen, welche **Rolle** Ihr Unternehmen im **Sinne der DSGVO** einnimmt. Hier lassen sich drei Rollen unterscheiden:

- **Verantwortlicher**: entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten
- **Auftragsverarbeiter**: verarbeitet personenbezogene Daten im Auftrag und auf Weisung des Verantwortlichen und führt ein detailliertes Verzeichnis dieser Daten
- **Betroffene Person**: eine identifizierte oder identifizierbare natürliche Person, auf die sich personenbezogene Daten beziehen
- **Unterauftragsverarbeiter**: jeder Auftragsnehmer, der im Auftrag des Auftragsverarbeiters tätig ist
- **Gemeinsam für die Verarbeitung Verantwortlicher:** legt gemeinsam mit einem anderen Verantwortlichen die Zwecke der und die Mittel zur Verarbeitung fest

Unternehmen können sowohl Datenverantwortliche als auch Auftragsverarbeiter sein: Jeder Auftragsverarbeiter ist automatisch auch ein Verantwortlicher, aber nicht jeder Verantwortliche ist Auftragsverarbeiter. So sind Lohnbüros oder Marktforschungsunternehmen Beispiele für Auftragsdatenverarbeiter. Ein Lohnbüro ist Datenverantwortlicher für die Daten seiner eigenen Mitarbeiter, aber Auftragsverarbeiter, wenn es die Lohn- und Gehaltsdaten der Mitarbeiter seiner Kundenunternehmen verarbeitet.

WAS SIND PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Beispiele für personenbezogene Daten sind:

- ein Vor- und Nachname
- Telefonnummer
- eine Privatadresse
- Geschlecht und Nationalität
- Bankverbindung
- medizinische Informationen
- alle Daten, die sich auf persönliche Interessen und Neigungen beziehen
- eine E-Mail-Adresse wie vorname.nachname@unternehmen.com
- Website-Verhalten
- Ausweisnummer
- Standortinformationen (z.B. GPS)
- eine IP-Adresse (Internet-Protokoll-Adresse)
- eine Cookie-ID
- die Werbe-ID auf Ihrem Telefon (also eine einmalige ID für jedes Mobilgerät, das Ad-Netzwerke nutzen, um gezielte Werbung anzuzeigen)

Beachten Sie bitte, dass es eine besondere Kategorie personenbezogener Daten gibt: **sensible personenbezogene Daten**. Hierzu zählen beispielsweise Gesundheitsdaten, Daten zur rassischen oder ethnischen Herkunft, zu politischen Meinungen, zu religiösen oder weltanschaulichen Überzeugungen, zur Gewerkschaftszugehörigkeit oder genetische und biometrische Daten (z.B. Fingerabdruck). Finanzdaten zählen nicht zu den sensiblen Daten. Wenn ein Unternehmen sensible Daten verarbeitet, müssen besondere technische Sicherheitsmaßnahmen vorgenommen werden, um diese Daten besonders zu schützen.

Es muss bedacht werden, dass **auch Unternehmensdaten personenbezogene Daten sein können**. So ist emily@teamleader.eu ein Beispiel für personenbezogene Daten, weil die E-Mail-Adresse mit einer identifizierbaren natürlichen Person ‚Emily' in Verbindung gebracht werden kann. E-Mail-Adressen wie info@teamleader.eu werden hingegen nicht als personenbezogene Daten angesehen und fallen daher nicht in den Anwendungsbereich der DSGVO.

Selbst wenn Sie pseudonymisierte personenbezogene Daten verwenden (d.h. Daten, bei denen alle identifizierbaren Merkmale durch ein Pseudonym ersetzt werden), zum Beispiel durch Hashing oder Verschlüsselung, bleibt eine Identifizierung möglich. **Man spricht so lange von personenbezogenen Daten, bis es keine identifizierbaren Merkmale mehr gibt und eine Rekonstruktion personenbezogener Daten nicht mehr möglich ist.**

BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN MÜSSEN FOLGENDE GRUNDSÄTZE BERÜCK-SICHTIGT WERDEN:

- **Fairness und Transparenz:** Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und auf nachvollziehbare Weise verarbeitet werden. Das bedeutet, dass Sie Ihre Kunden darüber informieren sollten, welche personenbezogenen Daten Sie erheben und wie Sie diese verwenden werden.

  Beispiel: Eine Fluggesellschaft darf Sie nach Ihrem Geburtsdatum fragen, weil sie diese Information für den Zoll benötigt, aber sie darf diese Informationen nicht für Marketingzwecke verwenden.

- **Zweckbindung:** Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Nachdem Sie Ihre Kunden darüber informiert haben, wie Sie mit personenbezogenen Daten umgehen, dürfen Sie sie nur für diese Zwecke verwenden.

  Beispiel: Ein Spirituosenhändler hat legitime Gründe dafür, Sie nach Ihrem Geburtsdatum zu fragen, da er sein Produkt nicht an Personen unterhalb eines bestimmten Alters vertreiben darf.

- **data minimisation:** Organisations can only collect data that's adequate, relevant and limited to what's necessary for the purpose, so you can only ask information that's necessary for the process.

  Beispiel: Als Paketdienstleister haben Sie keinen Grund dafür, Geburtsdaten zu erheben.

- **Sachliche Richtigkeit:** Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein.

  Beispiel: Wenn jemand umzieht oder seine E-Mail-Adresse ändert, hat er das Recht, ein Unternehmen dazu aufzufordern, seine Daten diesbezüglich zu ändern.

- **Datenlöschung:** Daten dürfen nur so lange aufbewahrt werden, wie es zur Erfüllung des ursprünglichen Zwecks erforderlich ist: zum Beispiel so lange wie jemand ein Kunde ist. Es muss klar definiert sein, wie lange die Daten benötigt werden.

  Beispiel: Dank der DSGVO werden die Betroffenen eine bessere Kontrolle über ihre personenbezogenen Daten haben. Das Recht auf Datenübertragbarkeit ist ein gutes Beispiel: Betroffene Personen haben das Recht, die Übermittlung ihrer Daten von einem Verantwortlichen an einen anderen zu verlangen. Das wird es künftig vereinfachen, die Bank oder den Stromanbieter zu wechseln. Für den Fall, dass Kunden nicht mehr von einem Unternehmen kontaktiert werden möchten, haben sie das Recht, die Löschung ihrer Daten zu verlangen: Das ist das Recht auf Vergessenwerden.

- **Sicherheit:** Organisationen sind verpflichtet, zum Schutz personenbezogener Daten technische und organisatorische Sicherheitsmaßnahmen vorzunehmen. Um festzulegen, welche Maßnahmen Ihr Unternehmen treffen muss, müssen Sie Art, Umfang, Umstände und Zwecke Ihrer Datenverarbeitung sowie die Rechte und Freiheiten der natürlichen Personen, deren Daten Sie verarbeiten, berücksichtigen. Entsprechend müssen Unternehmen, die sensiblere Daten wie z.B. Gesundheitsdaten verarbeiten, weitergehende Sicherheitsmaßnahmen treffen.

  Beispiel: Für den Fall einer Sicherheitsverletzung müssen Unternehmen einen Krisenmanagementplan vorbereitet haben, in dem die Schritte festgelegt sind, die vorzunehmen sind, um die Sicherheit ihrer Kunden und ihres Unternehmens zu gewährleisten.

- **Rechenschaftspflicht:** Es sollten Maßnahmen implementiert werden, die sicherstellen, dass der Umgang mit personenbezogenen Daten den Grundsätzen der DSGVO entspricht. So müssen beispielsweise Abläufe (z.B. der Krisenmanagementplan) und Dokumentation (z.B. Einwilligung in die Datenverarbeitung) aktualisiert werden, um die Einhaltung der DSGVO nachzuweisen.

  Beispiel: Kunden sollen in der Lage sein, offizielle Rechtsdokumente einzusehen, in denen aufgelistet ist, welche Daten gespeichert werden und wofür diese verwendet werden.

Wie sollten Sie mit E-Mails umgehen?

Die DSGVO unterscheidet zwei unterschiedliche Arten von E-Mails:

- **Ohne kommerziellen Aspekt:** E-Mails mit Urlaubsgrüßen oder guten Wünschen, Informationen zur DSGVO, etc.

- **Mit kommerziellem Aspekt oder Direktmarketing:** enthalten Preisinformationen, Preisnachlässe, Aktionsangebote, etc.

Für E-Mails ohne kommerziellen Aspekt müssen Sie lediglich jede Mail mit einer Opt-out-Möglichkeit versehen (also die Möglichkeit, diese Sorte von E-Mails abzubestellen).

Für E-Mails mit kommerziellem Aspekt werden Sie das Einverständnis oder die Einwilligung der betroffenen Person einholen müssen. So können Sie kommerzielle E-Mails beispielsweise nicht einfach an alle Ihre Kontakte versenden, sondern müssen vorher die **Einwilligung der Betroffenen einholen (Opt-in)**. Nur wenn die Betroffenen Ihr Einverständnis erklärt haben, dürfen Sie sich mit Direktmarketing an diese wenden. Auch hier müssen Sie ihnen die Möglichkeit geben, sich wieder abzumelden (Opt-out).

Es gibt zwei Fälle, bei denen keine Einverständniserklärung benötigt wird:

1. Wenn Sie sich mit Direktmarketingmaßnahmen an Bestandskunden wenden und der Inhalt der E-Mail vergleichbare Produkte oder Dienstleistungen Ihres Unternehmens bewirbt. Denken Sie aber immer daran, dass Sie den Empfängern jederzeit ein Opt-out ermöglichen müssen.

2. Wenn Sie Direktmarketingmails an juristische Personen (info@deloitte.com) versenden und es sich um Produkte oder Dienstleistungen für juristische Personen handelt. Auch hier müssen Sie immer ein Opt-out ermöglichen.

Vier Vorschläge, wie Sie hierzu vorgehen können:

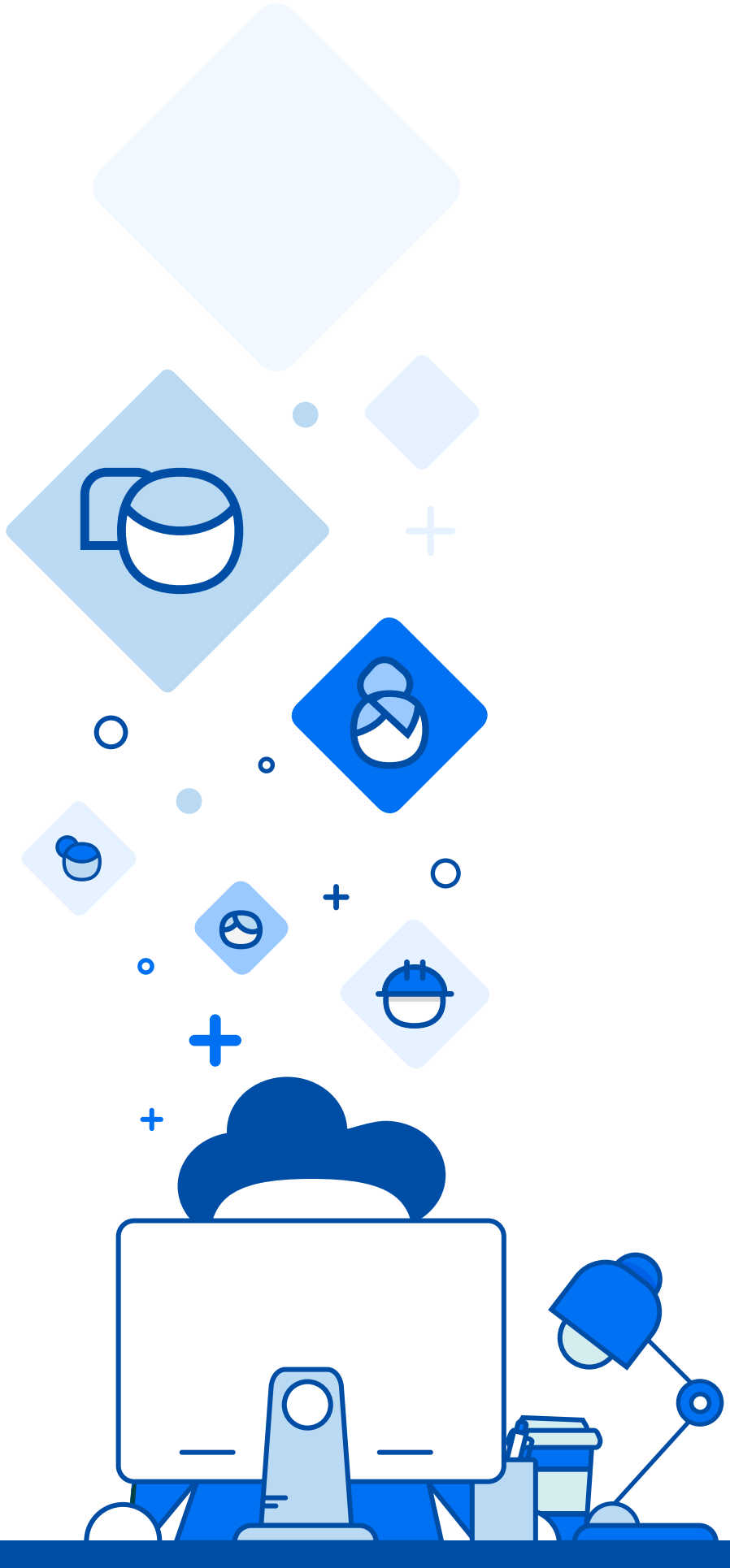
Wie können Sie unkompliziert Einverständ-niserklärungen für E-Mails mit kommerziellen Aspekten einholen?

- Fügen Sie bis zum 25. Mai jeder kommerziellen E-Mail folgende kurze Zeile hinzu: „Bestätigen Sie Ihre Anmeldung zu diesem Newsletter“. Indem die Empfänger auf diesen Hyperlink klicken, geben sie Ihre Einwilligung.

- Bitten Sie explizit um Einwilligung, da Sie sonst künftig keine kommerziellen E-Mails mehr verschicken können. Wenn die Resonanz dürftig ist, versuchen Sie es mit unterschiedlichen Überschriften, um die Aufmerksamkeit der Empfänger zu wecken.

- Bitten Sie auf Ihrer Website um die explizite Einverständniserklärung, kommerzielle E-Mails zugesendet zu bekommen, beispielsweise durch ein Pop-up-Fenster oder einen speziellen Button auf Ihrer Homepage.

- Machen Sie sich das Gefühl der Dringlichkeit zu Nutze, indem Sie eine „letzte Aufforderung“ versenden. „Ab nächster Woche werden Sie diese E-Mails nicht mehr empfangen... Geben Sie jetzt Ihre Einwilligung!“



WIE SICH IHR UNTERNEHMEN VORBEREITEN MUSS

UM SICH AUF DIE DSGVO VORZUBEREITEN, MÜSSEN SIE AUF FOLGENDEN GEBIETEN NACHWEISEN, DASS SIE DIE DATENSCHUTZBESTIMMUNGEN EINHALTEN:

- Richtlinien und Abläufe: Sowohl intern als auch extern werden sich einige Richtlinien ändern müssen, da die gegenwärtigen Vorschriften der DSGVO beispielsweise vorsehen, dass Kunden in die Speicherung ihrer Daten einwilligen müssen. Denken Sie an Richtlinien für die Bereiche Social Media, Archivierung, Mitarbeiterdaten, Data Governance, Datenlöschung, Backup, usw. Jedes Unternehmen sollte zumindest seine Datenschutzerklärung anpassen.
    - Extern: Kunden, Prospects, Geschäftspartner, Dienstleister, etc.
    - Intern: Personal, Auftragnehmer, Management, etc.
- Fortbildungs- und Sensibilisierungsmaßnahmen: Jeder Unternehmensangehörige sollte über Grundkenntnisse im Bereich der DSGVO verfügen, um sich datenschutzkonform zu verhalten. Indem Sie Ihr Team entsprechend schulen, stellen Sie sicher, dass sich jeder an die richtigen Abläufe hält.
- Dokumentation aller Vorgänge: Alle Unternehmen, die Umgang mit Daten haben, sollten sämtliche Datenverarbeitungsaktivitäten dokumentieren. Sie werden auch nachweisen müssen, wofür Sie diese Daten verarbeiten.
- Datenschutz-Folgeabschätzung (oder Audits): Sehr wahrscheinlich werden die Unternehmen daraufhin überprüft werden, ob sie ihre Abläufe an die neuen Vorschriften der DSGVO angepasst haben. Mehr noch, jedes Mal, wenn Unternehmen einen neuen Ablauf einführen oder eine neue Kooperation eingehen, müssen sie überprüfen, ob sich das auf die aktuellen Datenschutzvorgänge auswirkt. Ist das der Fall, müssen Sie die notwendigen Maßnahmen ergreifen, damit die Datenschutzvorschriften eingehalten werden, z.B. mit jedem neuen Partner eine Vereinbarung zur Auftragsdatenverarbeitung abschließen.
- Wenn sich Ihre Unternehmen und Abläufe mit der Zeit verändern, wirkt sich das auch darauf aus, ob Sie den Datenschutzvorschriften nachkommen. Eine weitere Möglichkeit ist, durch regelmäßig durchgeführte Audits zu überprüfen, ob Ihre Datenschutzmaßnahmen noch den Vorschriften genügen.
- Datenschutzbehörde (Data Protection Authority, DPA): Wenn Sie weitere Hilfe benötigen oder noch Fragen haben, können Sie sich an diese nationale Behörde wenden.

[2]Als Mindestanforderung muss eine Datenschutzerklärung sich auf die DSGVO beziehen und Informationen zu den folgenden Punkten beinhalten: welche personenbezogenen Daten erhoben werden, wie diese erhoben werden, dem Verarbeitungszweck, der Datenspeicherfrist, den Rechten der betroffenen Personen, Ihrem Beschwerdeverfahren, der Datenübertragung an Dritte, etc.

CHECKLISTE ZUR EINHALTUNG DER DSGVO: 10 MASSNAHMEN, DIE SIE ERGREIFEN MÜSSEN:

Haftungsausschluss: Es wird ausdrücklich darauf hingewiesen, dass Teamleader nicht garantieren kann, dass ein Unternehmen, das die hier aufgeführten Maßnahmen ergreift, die Datenschutzvorschriften zu 100 % einhält. Teamleader bietet lediglich Tipps und Hinweise zur DSGVO an. Entsprechend werden diese Informationen ausschließlich zu Informationszwecken angeboten und dienen nicht der Rechtsberatung oder der Beurteilung, wie die DSGVO sich auf Sie und Ihr Unternehmen/Ihre Organisation auswirkt.

Check

- **1.** Führen Sie **interne Audits** zu Ihrer Datenverarbeitung durch, um in Erfahrung zu bringen, was bereits in Ordnung ist und wo Sie noch Anpassungen an die neuen Vorschriften vornehmen müssen. Darüber hinaus sollten Sie **sämtliche Ihrer Rechtsdokumente juristisch überprüfen lassen und sie aktualisieren.**

- **2.** Holen Sie die explizite **Einwilligung** zur Datenverarbeitung ein: Überprüfen Sie, wie Sie das Einverständnis aktuell einholen. Wenn die bestehenden Einverständniserklärungen nicht mehr dem DSGVO-Standard entsprechen, erneuern Sie die Einwilligungen. (In Kapitel 1 dieses E-Books wurde erklärt, wie Sie Einverständniserklärungen einholen können)

- **3.** Erläutern Sie Ihren Kunden mittels einer Datenschutzerklärung[2], **wie und warum Sie Daten erheben und wie lange Sie diese Daten voraussichtlich speichern werden.** Um sich darauf vorzubereiten, können Sie ein Datenaudit durchführen, um eine Bestandsaufnahme darüber zu machen, über welche Daten Sie verfügen, wo diese herkommen und mit wem Sie sie austauschen. Zusätzlich sollten Sie Ihre Mitarbeiter informieren sowie Dokumente und Abläufe für den internen Gebrauch aktualisieren (z.B. Richtlinien für den Laptop-, Social-Media- und Internet-Gebrauch, Mitarbeiterverträge, Dienstvorschriften).

- **4.** Schulen Sie Ihre Mitarbeiter und **sensibilisieren** Sie sie in Informationsveranstaltungen, damit diese die Auswirkungen der DSGVO verstehen.

- **5. Beweisen** Sie, dass Sie die Vorschriften einhalten: Bestimmen Sie dafür die Rechtsgrundlage Ihrer Datenverarbeitungsaktivitäten in der DSGVO, dokumentieren Sie Ihre Abläufe und passen Sie Ihre Datenschutzerklärung an. Modifizieren Sie beispielsweise Ihre allgemeinen Geschäftsbedingungen und/oder die Vereinbarung, die Sie mit Ihren Kunden getroffen haben. Treffen Sie darüber hinaus mit Ihren Auftragsverarbeitern eine Vereinbarung zur Auftragsdatenverarbeitung (ADV) und, wenn notwendig, auch mit Ihren Unterauftragsverarbeitern.

- **6.** Sorgen Sie dafür, dass Sie über ein System verfügen, das die personenbezogenen Daten **löscht**, sobald die gesetzliche Aufbewahrungsfrist verstrichen ist oder die betroffene Person ihre Einwilligung zurücknimmt.

- **7.** Sorgen Sie dafür, dass für den Fall einer Datenschutzverletzung ein klar formulierter **Krisenmanagementplan** vorhanden ist, um diese zu erkennen, zu melden und zu untersuchen. Wichtiger Hinweis: Abhängig von der Art des Vorfalls oder der Verletzung muss die Meldung innerhalb eines bestimmten Zeitraums erfolgen. Um mehr darüber zu erfahren, innerhalb welcher Frist Sie eine Krise melden müssen, wenden Sie sich an Ihre nationale Datenschutzbehörde.

- **8.** Erstellen oder aktualisieren Sie **Zugriffsabläufe**: zum Beispiel, dass nur berechtigte Benutzer Zugriff auf Ihren Server haben. Umgekehrt müssen die Betroffenen auf Anfrage Zugriff auf ihre Daten bekommen.

- **9.** Schützen Sie die Daten von **Kindern unter 16 Jahren**, da diese der Zustimmung eines Elternteil oder Erziehungsberechtigten benötigen. Jedes EU-Land darf diese Altersgrenze auf 13 Jahre herabsetzen. Frankreich und Belgien haben sie beispielsweise auf 13, Österreich auf 14 abgesenkt.

- **10.** Berufen Sie einen **Datenschutzbeauftragten (DSB)**, der Ihre Abläufe auf Einhaltung des Datenschutzes hin überprüft. Dies ist nicht für jedes Unternehmen verpflichtend, wird aber empfohlen. Der DSB kann ein externer Berater sein oder auch ein Mitarbeiter, der diese zusätzliche Rolle neben seinen täglichen Aufgaben übernimmt.

WAS BEDEUTET DIE DSGVO FÜR TEAMLEADER?

Als Unternehmen mit mehreren Standorten und Kunden in ganz Europa muss Teamleader sich an viele verschiedene europäische Gesetze halten. In der Vergangenheit waren die europäischen Datenschutzgesetze unübersichtlich und uneinheitlich, was sich aber durch die neue DSGVO verbessern wird. Mit einer Vielzahl von Maßnahmen können wir ein Höchstmaß an Schutz für all unsere Stakeholder garantieren.

Teamleader fungiert sowohl als Auftragsverarbeiter als auch als Verantwortlicher:

- Auftragsverarbeiter: Wir entwickeln eine Cloud-Lösung, die wir anderen Unternehmen, unseren Kunden, zur Verfügung stellen, damit diese darin ihre Kundendaten speichern können. In diesem Verhältnis fungiert Teamleader als Auftragsverarbeiter, unsere Kunden sind die Verantwortlichen. Dies wird in einer **Vereinbarung zur Auftragsdatenverarbeitung** geregelt. Diese ADV wird von Teamleader bereitgestellt und ist nicht verhandelbar.

- Verantwortlicher: Wir verarbeiten Daten unserer Mitarbeiter, Kunden, Leads, Partner,...

Unsere Verantwortung für die Einhaltung der DSGVO-Anforderungen

Als Plattform trifft Teamleader gewisse Vorkehrungen, damit unsere Nutzer die DSGVO bis zum 25. Mai einhalten können. Wenn unsere Nutzer jedoch personenbezogene Daten (z.B. ihrer Kunden) in Teamleader eingeben, werden sie als Datenverantwortliche angesehen und sind entsprechend allein dafür verantwortlich, die Datenschutzvorschriften einzuhalten. In diesem Fall handelt Teamleader ausschließlich als Bereitsteller seiner Plattform und entsprechend als Auftragsverarbeiter dieser personenbezogenen Daten.Unsere Kunden, als Verantwortliche, sind für die Einhaltung der DSGVO Regelungen im Bezug auf die Daten der Endkunden natürlich verantwortlich.

Teamleader wird am 25. Mai auf die neue DSGVO vorbereitet sein. Die Dokumente auf folgender Liste sind nur einige Beispiele für die Maßnahmen, die wir treffen, um die Datenschutzvorschriften einzuhalten:

- **Interner Reaktionsplan**, um Datenschutzverletzungen zu entdecken und zu melden und um festzustellen, welche Schritte im Falle einer Datenschutzverletzung unternommen werden müssen.

- TOM bzw. **Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten**: eine Liste aller Maßnahmen zum Schutz personenbezogener Daten, die Teil der Vereinbarung zur Auftragsdatenverarbeitung ist.

- Die **Datenschutzerklärung** bezieht sich auf die DSGVO und enthält Informationen zu den folgenden Punkten: welche personenbezogenen Daten erhoben werden, wie diese erhoben werden, dem Verarbeitungszweck, der Datenspeicherfrist, den Rechten der betroffenen Personen, dem Beschwerdeverfahren, der Datenübertragung an Dritte, etc.

- Die **Vereinbarung zur Auftragsdatenverarbeitung** enthält die Vereinbarungen zwischen Teamleader und seinen Kunden in Bezug auf die Verarbeitung der Kundendaten (also der Daten, die von unseren Kunden in Teamleader eingeben werden) durch Teamleader in Übereinstimmung mit den Anweisungen des Kunden/Verantwortlichen. Für den Fall, dass Teamleader Unterauftragsverarbeiter beauftragt, stellen wir sicher, dass diese durch dieselben DSGVO-Verpflichtungen gebunden sind wie Teamleader.

Die Webanwendungs-, Kommunikations- und Datenbankserver sowie sämtliche Kundendaten von Teamleader werden auf europäischen Servern in Irland gespeichert und von Amazon Web Services, Inc. (AWS) betrieben und werden zu keinem Zeitpunkt auf US-amerikanischen Servern verarbeitet oder gespeichert. Entsprechend fällt Teamleader unter die DSGVO. Um die Normen und Verpflichtungen der DSGVO einzuhalten, hat Teamleader das ‚AWS Data Processing Addendum' unterschrieben. Amazon ist darüber hinaus nach ISO 27001, einer internationalen Norm für IT-Sicherheitsmanagement, zertifiziert und wird gemäß international anerkannter Best Practices geführt.

Im AWS-Rechenzentrum werden die Daten auf verschlüsselten Festplatten gespeichert. Die Rechenzentren werden darüber hinaus kontinuierlich innoviert, um sie vor von Menschen verursachten und natürlichen Risiken zu schützen. Zur Bestätigung ihrer Sicherheit und Compliance werden sie externen Audits unterzogen. Den höchsten Regulierungsanforderungen unterliegende Organisationen auf der ganzen Welt, wie z.B. die NASA, vertrauen täglich auf AWS.

Was ist Verschlüsselung und warum ist sie für den Datenschutz so wichtig?

Verschlüsselung ist die effektivste und beliebteste Methode für den Datenschutz. Dabei werden Daten in einen geheimen Code umgewandelt. Um eine verschlüsselte Datei zu lesen, braucht man Zugriff auf einen geheimen Schlüssel, mit der sie sich wieder entschlüsseln lässt. Unverschlüsselte Daten bezeichnet man als Klartext, verschlüsselte Daten als Geheimtext.

Personenbezogene Daten sind SSL-verschlüsselt und können so nur von einer kleinen Gruppe autorisierter Teamleader-Mitarbeiter eingesehen werden. Neben der technischen Sicherheitsüberprüfung findet schließlich auch noch eine weitere Kontrolle durch einen externen Rechtsberater statt.

2017 haben wir auch noch zwei obligatorische **unternehmensweite Schulungen** für unsere Mitarbeiter durchgeführt, in denen wir sie ausführlich darüber informiert haben, was die DSGVO bedeutet und welche Maßnahmen wir ergreifen, um gut auf den 25. Mai 2018 vorbereitet zu sein.

Indem sichergestellt wurde, dass alle Daten auf äußerst sichere Weise gespeichert und verarbeitet werden, hat Teamleader viele proaktive Maßnahmen ergriffen, um die Sicherheit unserer Kunden und all unserer Stakeholder zu gewährleisten.

Teamleader

„Datensicherheit, Datenschutz und die Einhaltung gesetzlicher Vorschriften sowohl für Nutzer als auch deren Kunden ist schon immer ein wichtiges Anliegen von Teamleader gewesen. Daran wird sich auch nichts ändern, wenn die DSGVO in Kraft tritt. Bestehende und künftige Teamleader-Kunden können sich darauf verlassen, dass wir alle gesetzlichen Anforderungen erfüllen.“

Tom Schouteden, CTO bei Teamleader

Sie möchten wissen, welche Maßnahmen für Datensicherheit und Datenschutz Teamleader ergreift? Dann lesen Sie doch unseren Blog zu diesem Sicherheitsthema.

MEHR ERFAHREN

Sie arbeiten täglich mit Kundendaten? Dann sollten Sie auf eine Lösung umsteigen, die die neuen Anforderungen an den Datenschutz komplett erfüllt. Mit dem CRM von Teamleader lösen Sie dieses Problem.

14 TAGE KOSTENLOS TESTEN