DSGVO-Compliance

Wie CRM-Software Sie bei der Einhaltung der neuen Datenschutz-Grundverordnung unterstützt

Die neue EU-Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) regelt die Verarbeitung und Aufbewahrung personenbezogener Daten von EU-Bürgern. Nach europäischem Recht sind alle Unternehmen weltweit an diese Regelung gebunden. Die DSGVO wirkt sich auf das gesamte Unternehmen aus. Diese Dokumentation erklärt, wie Act! Unternehmen bei der Einhaltung der neuen Regelung unterstützt.

Die EU-Datenschutz-Grundverordnung (DSGVO) ist am 25. Mai 2018 in Kraft getreten. Die DSGVO verpflichtet alle Unternehmen, die personenbezogene Daten von EU-Bürger verarbeiten, zur Einhaltung der Datenschutzrichtlinien und anderer festgelegter Standards. Einige der bestehenden Konzepte und Prinzipien des Datenschutzes wurden in der neuen DSGVO nur geringfügig geändert oder erweitert. Dazu zählen z. B. die Definition personenbezogener Daten, der besondere Schutz medizinischer und anderer sehr persönlicher Daten und das Auskunftsrecht betroffener Personen. Die DSGVO führt jedoch auch neue Regelungen und Anforderungen ein – zum Beispiel strengere Persönlichkeitsrechte, wie Widerspruch gegen automatisierte Verarbeitung, und erweiterte Rechenschaftspflichten.

DSGVO und CRM-Systeme

Unternehmen, die ihre Arbeitsweise nach der Datenschutz-Grundverordnung offen kommunizieren, schaffen Vertrauen bei Interessenten und Kunden und erzielen so einen wichtigen Wettbewerbsvorteil. Bei Nichteinhaltung der DSGVO riskieren Unternehmen allerdings Strafgebühren und den Verlust ihres guten Rufes. Daher ist es wichtig, dass Unternehmen einen systematischen Ansatz zur Einhaltung der DSGVO verfolgen und ihre Prozesse und Richtlinien kontinuierlich prüfen und aktualisieren.

Die meisten CRM-Lösungen sind flexible und anpassbare Systeme für das Kundenbeziehungsmanagement. Sie bieten eine Reihe von Funktionen, die Nutzer bei der effizienten Verwaltung ihrer Datenprozesse, des Datenschutzes und der Sicherheit unterstützen. Wenn Sie eine CRM-Software nutzen oder die Anschaffung planen, wissen Sie bereits, dass ein solches Programm ein äußerst wertvolles Instrument zur Einhaltung der DSGVO in Ihrem Unternehmen sein kann. In diesem Dokument werden einige der wichtigsten Richtlinien der DSGVO beschrieben. Sie erhalten Informationen darüber, wie ein CRM-System Sie bei der Einhaltung der DSGVO unterstützt.

Inhalt

10 Bereiche, in denen CRM-Systeme Sie bei der Umsetzung der DSGVO unterstützen:

1. Geographischer Geltungsbereich

Alle in der DSGVO festgelegten Vorschriften, Richtlinien, Einschränkungen und Rechte gelten für Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten. Dies betrifft Unternehmen innerhalb und außerhalb der EU. Wenn Ihr Unternehmen in den USA ansässig ist und Sie Daten natürlicher Personen mit Wohnsitz in der EU erfassen, unterliegt die Datenverarbeitung den Bestimmungen der DSGVO.

Die meisten CRM-Lösungen bieten die Möglichkeit, das Wohnsitzland eines Kontakts zu speichern. So können Sie schnell die Personen ermitteln, deren Rechte unter der DSGVO geschützt sind. Gruppieren Sie alle relevanten Datensätze zur einfachen Verwaltung.

2. Definition personenbezogener Daten

Die DSGVO definiert personenbezogene Daten als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung identifiziert werden kann. Neben den etablierten Kennungen zählen dazu auch Daten wie IP-Adressen, IDs mobiler Geräte, Verhaltensdaten und unter bestimmten Umständen auch Finanzinformationen.

Viele Daten zu natürlichen Personen (im Gegensatz zu Unternehmen und Organisationen), die Sie im CRM-System erfassen, sind gemäß DSGVO höchstwahrscheinlich „personenbezogene Daten“. Daher ist es zwingend erforderlich, dass die Erstellung, Aufbewahrung, Verwaltung und Nutzung dieser Daten der neuen Verordnung entsprechen. Die Daten müssen nicht nur sicher aufbewahrt werden, sie dürfen auch nur so lange gespeichert werden, wie es für Ihre Zwecke erforderlich ist.

3. Rechenschaftspflicht

Die DSGVO verlangt, dass Sie ein Verzeichnis über die Verwendung und Aufbewahrung (bzw. Verarbeitung) von personenbezogenen Daten führen. Für kleine und mittlere Unternehmen gilt dies nur für bestimmte Verarbeitungstätigkeiten.

CRM-Systeme besitzen viele Funktionen, mit denen Sie alle Aktionen mit personenbezogenen Daten speichern können:

- Nachverfolgen einer Datensatzquelle in einem Feld.
- Anhängen zusätzlicher Dokumente an einen Datensatz, zum Beispiel E-Mails, gescannte Dokumente, Anrufaufzeichnungen usw.
- Hinzufügen von Zeitstempel und Historiedaten für einzelne Kontakte, um Interaktionen oder einen intern angewendeten Prozess zu dokumentieren.
- Konfigurieren von Feldern zum automatischen Aufzeichnen eines Historieeintrags, um Änderungen eines Datensatzes zurückzuverfolgen.

4. Nutzung von Daten

Die Datenschutzrichtlinien in der DSGVO legen die Grundsätze für die Verarbeitung personenbezogener Daten durch Unternehmen fest. Für die Verarbeitung personenbezogener Daten gilt:

- Die Verwendung muss fair, gesetzmäßig und transparent sein.
- Die Daten dürfen nur für spezifische Zwecke erhoben werden und die Verwendung muss mit diesen Zwecken vereinbar sein.
- Es muss eine angemessene Sicherheit der Daten gewährleistet sein.

Diese grundsätzlichen Anforderungen sind eng miteinander verknüpft. CRM-Systeme können die Verwendung personenbezogener Daten nicht steuern oder begrenzen, aber Sie bei folgenden Aufgaben unterstützen:

1. Verfolgen Sie, wie Nutzer Informationen in Datensätzen erstellen, ändern und verwenden. Begrenzen Sie den Zugriff einzelner Nutzer auf bestimmte Daten, die für ihre Rolle relevant sind.
2. Speichern Sie die Wünsche von Kunden zur Verwendung ihrer Daten in der Datenbank. So können die Mitarbeiter sie bei allen Interaktionen aufrufen und verwenden. Wenn Kunden z. B. keine wöchentlichen Newsletter oder Informationen zu neuen Produkten erhalten möchten, können Sie diese als Opt-outs kennzeichnen.
3. Sicherheitseinstellungen auf Feldebene sorgen dafür, dass Nutzer nur die Daten anzeigen oder ändern können, die für ihre Rolle relevant sind.
4. Darüber hinaus kann eine genaue Kennwortrichtlinie konfiguriert werden, die die Länge, Komplexität, Änderungshäufigkeit und Wiederverwendung von Kennwörtern festlegt.

- Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die angegebenen Zwecke erforderlich ist. Formulieren Sie eine Richtlinie, die auf die Anforderungen Ihres Unternehmens abgestimmt ist und beschreibt, wie Sie zwischen veralteten und verwendbaren Daten unterscheiden. Definieren Sie außerdem Prozesse für die Ermittlung und Verwaltung dieser verwendbaren Daten.

CRM-Lösungen bieten Ihnen dazu mehrere Möglichkeiten:

1. Das Erstelldatum und das Datum der letzten Bearbeitung der Datensätze werden automatisch gespeichert. Nutzen Sie diese als Abfrageparameter, um das Alter und die Relevanz des Datensatzes zu ermitteln.
2. Erstellen Sie Gruppen für die automatische Segmentierung und kennzeichnen Sie Datensätze, die Ihren Filterkriterien entsprechen.
3. Mit der Lookup-Funktionalität können Sie komplexe Datensatzsuchen durchführen und nach dem letzten Änderungsdatum verschiedener Datensatzbereiche suchen.
4. Nutzer können in einem benutzerdefinierten Feld bestimmte Datensätze manuell markieren, die sie löschen oder archivieren möchten.

5. Rechtsgrundlage für die Verarbeitung

Unternehmen benötigen eine rechtliche Grundlage für die Verarbeitung von Daten. Es gibt sechs Grundsätze für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Diese sind:

Zustimmung
Diese muss ausdrücklich und in Bezug auf einen bestimmten Prozess erteilt werden.

Vertrag
Die Datenverarbeitung ist erforderlich, um einen Vertrag zu erfüllen oder abzuschließen.

Berechtigtes Interesse
Die Verarbeitung ist zur Wahrung Ihrer Interessen oder der Interessen einer weiteren Partei erforderlich, sofern nicht ein Grund zum Schutz der personenbezogenen Daten vorliegt, der diese Interessen überwiegt.

Gesetzliche Verpflichtungen
Ohne Vertragsverpflichtungen.

Lebenswichtige Interessen
Die Verarbeitung ist erforderlich, um lebenswichtige Interessen einer Person zu schützen.

Öffentliche Aufgabe
Dies gilt nur für Organisationen des öffentlichen Sektors.

Häufig ist die Zustimmung die rechtliche Grundlage für die Datenverarbeitung. Die betroffene Person muss ihr Einverständnis freiwillig, ausdrücklich und in Kenntnis aller Informationen erteilen. Die Zustimmung muss in Form einer klaren, affirmativen Handlung erfolgen, d. h., sie darf nicht aus Stillschweigen, vorab angekreuzten Kästchen oder Nichthandeln abgeleitet werden. Die Einwilligung muss getrennt von anderen allgemeinen Geschäftsbedingungen erteilt werden. Sie stehen in der Pflicht, betroffenen Personen eine einfache Methode anzubieten, um ihre Zustimmung widerrufen zu können. Die Zustimmung muss nachweisbar sein und Sie müssen betroffenen Personen die Möglichkeit geben, ihr Recht auf Zustimmung wahrzunehmen.

CRM-Systeme erleichtern das Verwalten von Opt-ins. Act! emarketing hat z. B. eine Option zum Abbestellen von Kampagnen. In der Act! Datenbank können Sie benutzerdefinierte Felder erstellen, um differenzierte Optionen zum Opt-in anzubieten. Suchen und Listen eignen sich ebenfalls gut zum Bearbeiten von Kontakten, die Marketing-E-Mails abbestellt haben.

6. Die Rechte natürlicher Personen

Die DSGVO erweitert die Rechte natürlicher Personen in Bezug auf die Verwendung ihrer personenbezogenen Daten.

6.1 Informationspflicht

Die Datenschutz-Grundverordnung verlangt, dass Unternehmen betroffene Personen informieren, wenn ihre Daten erfasst werden. Der Umfang dieser Informationen hängt davon ab, ob Sie die personenbezogenen Daten direkt von den betroffenen Personen erhalten haben oder nicht. Die Informationen zur Verarbeitung personenbezogener Daten müssen:

- präzise, transparent, verständlich und leicht zugänglich sein;
- in klarer und einfacher Sprache verfasst sein, vor allem wenn sie sich an Kinder richten;
- kostenlos bereitgestellt werden.

Sie können zum Beispiel ein Feld erstellen, das anzeigt, wenn betroffene Personen über die Verarbeitung ihrer Daten informiert wurden. Erstellen Sie z. B. ein Datenfeld oder Kontrollkästchen mit den Optionen „Ja“ und „Nein“. So halten Sie fest, ob und wann die Person informiert wurde. In einer Dropdown-Liste können Sie die Quelle der Zustimmung angeben z. B. Telefon, Webformular usw.

6.2 Auskunftsrecht

Laut DSGVO müssen Informationen kostenlos übermittelt werden, es sei denn, der Antrag ist offenkundig unbegründet oder exzessiv. In diesem Fall kann eine Gebühr erhoben werden. Die Auskunft muss unverzüglich, spätestens aber innerhalb eines Monats nach Eingang der Anfrage erteilt werden. Sie sind verpflichtet, die Identität des Antragstellers mit vertretbaren Mitteln zu überprüfen.

Anfragen in elektronischem Format sollten in einem gängigen Datenformat beantwortet werden. Als Best Practice wird empfohlen: „Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde“ (Erwägungsgrund 63). Diese Vorgehensweise ist u. U. nicht für alle Unternehmen umsetzbar, aber für manche Branchen gut geeignet.

In CRM-Systemen können in der Regel verschiedene Berichte wie z. B. Kontaktberichte generiert werden. Hier können Sie für einzelne Kontakte eine vollständige Auflistung der gespeicherten Daten erstellen.

Die Daten in den Kontaktfeldern können mit vielen CRM-Tools auch in verschiedene Dateiformate (einschließlich CSV-Dateien) exportiert und so auf einfache Weise an betroffene Person gesendet werden.

6.3 Recht auf Berichtigung

Die betroffene Person hat das Recht, die Berichtigung ihrer Daten zu verlangen, falls diese falsch oder unvollständig sind. Die Berichtigung muss innerhalb eines Monats erfolgen. Es besteht die Möglichkeit zur Verlängerung der Frist, falls die Anfrage komplex ist. Werden keine Maßnahmen ergriffen, so muss dies der betroffenen Person unter Hinweis auf ihr Beschwerderecht mitgeteilt werden. Drittanbieter, an die Daten weitergegeben wurden, sind ebenfalls zur Berichtigung der Daten verpflichtet.

In den meisten CRM-Tools können Sie einen Datensatz zum Antrag auf Berichtigung anlegen, entweder mit einer Notiz oder der Historie. Dabei wird in der Regel auch das Erstelldatum gespeichert. Folgeaktionen zu einem Antrag werden dann als zusätzlicher Historieeintrag oder als Aktivität für einen bestimmten Nutzer festgehalten.

Mit einem CRM-Programm können Sie aufzeichnen, ob und wann Informationen an Drittparteien weitergegeben werden. Dies erleichtert die Kontaktaufnahme, falls ein Antrag auf Berichtigung oder Löschen der Daten gestellt wird.

Wir empfehlen, einen Prozess aufzusetzen, den Mitarbeiter beim Erhalt eines Antrags auf Berichtigung einhalten müssen.

6.4 Recht auf Löschung

Das Recht auf Löschung wird auch Recht auf Vergessenwerden genannt. Die betroffene Person hat das Recht zu verlangen, dass ihre personenbezogenen Daten gelöscht oder entfernt werden, wenn kein wichtiger Grund mehr für die Verarbeitung vorliegt. Unter bestimmten Voraussetzungen müssen personenbezogene Daten gelöscht und dürfen nicht weiter verarbeitet werden. Drittanbieter, an die Daten weitergegeben wurden, sind ebenfalls zur Einhaltung von Richtlinien verpflichtet.

In den meisten CRM-Systemen ist das Löschen von Kontaktdatensätzen problemlos möglich. Dabei werden alle Einträge und dem Datensatz zugeordnete Daten gelöscht (es sei denn, diese sind mit anderen Kontakten verknüpft). Der Löschvorgang wird in einem Bereich aufgezeichnet, der alle Aktionen von Nutzern des Systems speichert, z. B. wer die Daten gelöscht hat, einschließlich Datum, Uhrzeit und Name des Kontakts.

In einer CRM-Lösung kann festgehalten werden, wenn Informationen an Drittanbieter weitergegeben wurden. So können Sie diese schnell kontaktieren, falls die Daten gelöscht werden müssen.

6.5 Recht auf Einschränkung der Verarbeitung

Natürliche Personen haben das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Wenn die Verarbeitung eingeschränkt wurde, darf ein Unternehmen die personenbezogenen Daten aufbewahren, aber nicht weiter verarbeiten.

In einem benutzerdefinierten Feld können Sie notieren, wenn Kunden die Verarbeitung ihrer Daten einschränken.

6.6 Recht auf Datenübertragbarkeit

Betroffene Personen haben das Recht, ihre personenbezogenen Daten für eigene Zwecke über verschieden Dienste zu erhalten und wiederzuverwenden. Der Auftragsverarbeiter sollte in der Lage sein, die Daten sicher und ohne Behinderung zwischen IT-Services zu verschieben, zu kopieren oder zu übertragen. Der Auftragsverarbeiter muss innerhalb eines Monats auf eine solche Anfrage antworten. Personenbezogene Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden. Eventuell müssen Sie die Daten an ein anderes Unternehmen übertragen, soweit dies technisch möglich ist. Sie dürfen dabei die Rechte anderer nicht verletzten, z. B. durch Offenlegen der Daten von Drittanbietern.

Sie können in Ihrer CRM-Lösung bequem Daten aus den Kontaktfeldern in verschiedene Dateiformate (einschließlich CSV) exportieren.

6.7 Widerspruchsrecht

Wenn ein Auftragsverarbeiter personenbezogene Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrung der unternehmenseigenen Interessen verarbeitet, kann die betroffene Person aus Gründen, die sich aus ihrer besonderen Situation ergeben, dagegen Widerspruch einlegen. Das Unternehmen darf die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, es kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung von Rechtsansprüchen.

Die betroffene Person muss zum Zeitpunkt der ersten Kommunikation und in der Datenschutzerklärung über ihr Widerspruchsrecht informiert werden. Sie muss ausdrücklich und in einer verständlichen und von anderen Informationen getrennten Form auf ihre Rechte hingewiesen werden. Erfolgt die Datenverarbeitung online, muss eine Möglichkeit bestehen, online Widerspruch einzulegen. Dieser Punkt ist wichtig. Wir empfehlen daher, die vollständige Leitlinie der zuständigen Datenschutzbehörde zu lesen.

In Ihrem CRM-System sollten Empfänger in der Fußzeile die Möglichkeit haben, E-Mails einer Kampagne abzubestellen. In Act! emarketing können Sie zum Beispiel die Empfänger nachverfolgen, die Ihre Kampagnen abbestellt haben.

6.8 Automatisierte Entscheidungen einschließlich Profiling

Die DSGVO gewährt natürlichen Personen bestimmte Rechte, wenn Sie einer automatisierten Entscheidung und Profiling unterworfen werden. Dies gilt insbesondere, wenn die automatisierte Entscheidung und das Profiling der Person gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen.

CRM-Administratoren müssen Unternehmens- und Rechtsberater darüber informieren, dass bei der Verwendung von CRM-Systemen die Möglichkeit zu automatisierten Entscheidungen und Profiling besteht. Datenschutzerklärungen müssen einen entsprechenden Hinweis enthalten. Wir empfehlen, entsprechende Verfahren einzuführen. Unterbinden Sie z. B. automatisierte Entscheidungen und Profiling für natürliche Personen. Ermöglichen Sie Nutzern, Kunden ihre Daten zu übermitteln, die für automatisierte Entscheidungen und Profiling verwendet werden, und kennzeichnen Sie Kontakte, die unter der DSGVO als schutzbedürftige Gruppe gelten.

7. Verantwortlichkeit und Rechenschaftspflicht

Gemäß der DSGVO müssen Unternehmen umfassende, jedoch angemessene Maßnahmen zur Einhaltung der Richtlinien treffen. Zum Nachweis der Einhaltung müssen Unternehmen:

- geeignete technische und organisatorische Maßnahmen treffen, die die Einhaltung der Richtlinien sicherstellen und nachweisen. Dazu zählen interne Datenschutzvorkehrungen wie Mitarbeiterschulungen, interne Audits der Datenverarbeitung und die Prüfung interner HR-Richtlinien.
- relevante Verarbeitungstätigkeiten dokumentieren;
- gegebenenfalls einen Datenschutzbeauftragten benennen;
- eine Datenschutz-Folgeabschätzung vornehmen, falls erforderlich;
- Maßnahmen zur Einhaltung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen treffen. Zu diesen Maßnahmen zählen:
    - Daten minimieren;
    - Daten pseudonymisieren;
    - Transparenz herstellen;
    - betroffenen Person ermöglichen, die Verarbeitung zu überwachen; und
    - Sicherheitsfunktionen schaffen und verbessern.

Eine weitere Möglichkeit ist die Einhaltung genehmigter Verhaltensregeln bzw. die Teilnahme an einem Zertifizierungsverfahren.

Die Nutzung eines CRM-Tools wie Act! fällt in den Anwendungsbereich weiterer Teile dieser DSGVO-Richtlinie. Alle Unternehmen müssen Compliance-Prozesse implementieren, z. B. Nachweise über die konforme Datenverarbeitung speichern und Folgenabschätzungen durchführen. Außerdem müssen geeignete Maßnahmen für den Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen getroffen werden. Wenden Sie sich an einen Berater, der Sie bei der Umsetzung und Einhaltung geeigneter Maßnahmen unterstützt.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Auftragsverarbeiter müssen technische und organisatorische Maßnahmen treffen, die den Datenschutz bei allen Verarbeitungsvorgängen berücksichtigen.

„Eingebauter Datenschutz“ ist ein Ansatz, der den Schutz der Privatsphäre und den Datenschutz frühzeitig unterstützt. Unternehmen sollten sicherstellen, dass der Schutz der Privatsphäre und der Datenschutz bereits in den frühen Phasen eines Projekts und in seinem gesamten Lebenszyklus berücksichtigt werden. Beispiele:

- Aufbau neuer IT Systeme zum Speichern von personenbezogenen Daten und den Zugriff darauf;
- Entwicklung von Gesetzen, Richtlinien oder Strategien, die sich auf den Datenschutz auswirken;
- Initiative zum Austausch von Daten oder
- Verwenden der Daten für neue Zwecke.

Insbesondere bei der Verwendung neuer Technologien sollte eine Datenschutz-Folgenabschätzung durchgeführt werden. Die Datenschutzbehörde hat einen Leitfaden, der die Verwendung von Folgenabschätzungen erklärt. Eine solche Folgenabschätzung reduziert das Risiko für natürliche Personen, dass ihre Rechte durch den Missbrauch personenbezogener Daten verletzt werden. Sie hilft Ihnen dabei, effiziente und wirkungsvolle Prozesse für den Umgang mit personenbezogenen Daten zu entwickeln.

In diesem Fall ist es hilfreich, eine CRM-Lösung als Dokumentenspeicher zu nutzen. Wenn Sie z. B. mit dem Manager für benutzerdefinierte Tabellen in Act! Premium Plus Projekte erstellt haben, kann die schriftliche Folgenabschätzung für einzelne Projekte gemeinsam mit anderen Dokumenten gespeichert werden (z. B. mit einem Geschäftsvorgang oder einem Dokument zur Projektinitiierung).

8. Ernennen eines Datenschutzbeauftragten

Unter bestimmten Umständen ist es erforderlich, einen Datenschutzbeauftragten zu ernennen. Er oder sie muss über ausreichende Kenntnisse und Ressourcen zur Einhaltung der DSGVO verfügen. Dies gilt auch, wenn ein Unternehmen nicht zur Ernennung eines Datenschutzbeauftragten verpflichtet ist. Die Mindestanforderungen an diese Tätigkeit sind hier klar definiert.

9. Verarbeitung personenbezogener Daten von Kindern

Wenn Ihr Unternehmen Produkte oder Dienstleistungen für Kinder anbietet, müssen Sie die Einwilligung der Eltern oder Erziehungsberechtigten einholen, bevor Sie deren Daten erfassen und verarbeiten. Gemäß der DSGVO darf in Deutschland die Altersgrenze für die Zustimmung von Kindern nicht unter dem 16. Lebensjahr liegen.

In einer CRM-Software können Sie das Alter für neue Kontakte speichern und dann eine Suche nach Datensätzen von Kindern durchführen. So können Sie entsprechende Schritte für die DSGVO-konforme Verarbeitung der Daten einleiten.

10. Sicherheit personenbezogener Daten

Für die Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden. Führen Sie eine Risikoanalyse durch, implementieren Sie entsprechende Unternehmensrichtlinien und ergreifen Sie geeignete technische und physische Maßnahmen. Anonymisierung und Verschlüsselung der Daten sind ebenfalls geeignete Methoden. Systeme und Services müssen die Vertraulichkeit, Sicherheit und Integrität personenbezogener Daten gewährleisten. Erstellen Sie Sicherungskopien, um Ihre Daten vor Verlust zu schützen. Die getroffenen Maßnahmen müssen getestet und gegebenenfalls verbessert werden.

Datentransfer in Länder außerhalb der EU

Personenbezogene Daten dürfen nur unter bestimmten Bedingungen übertragen werden.

Es gibt dazu mehrere Entwürfe der Datenschutzbehörden, die den Beschlüssen der Europäischen Kommission folgen.

Die Übermittlung ist nur unter bestimmten, besonderen Umständen zulässig – und zwar dann, wenn:

- die betroffene Person über die Übermittlung informiert wurde und ausdrücklich ihre Zustimmung erteilt hat;
- die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Unternehmen oder zur Durchführung vorvertraglicher Schritte auf Antrag der betroffenen Person erforderlich ist;
- die Übermittlung für die Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person zwischen dem Verantwortlichen und einer anderen Person geschlossen wurde;
- die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses erforderlich ist;
- die Übermittlung für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;
- die Übermittlung zur Wahrung lebenswichtiger Interessen der betroffenen Person oder anderen Personen, die aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, erforderlich ist;
- aus einem Register erfolgt, das gemäß EU-Recht zur Information der Öffentlichkeit bestimmt ist (und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht).

Unter bestimmten, genau festgelegten Umständen ist die einmalige Übermittlung von Daten weniger natürlicher Personen gestattet.

Meldung von Verletzungen des Schutzes personenbezogener Daten

Datenverarbeitende Unternehmen sind verpflichtet, Datenschutzverletzungen zu melden, wenn sie voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Dies ist beispielsweise der Fall, wenn die Datenschutzverletzung Diskriminierung, Rufschädigung, finanzielle Verluste, Verlust der Vertraulichkeit oder andere erhebliche wirtschaftliche oder soziale Nachteile nach sich zieht. Betroffene Personen müssen benachrichtigt werden, wenn dieses Risiko hoch ist.

Die Meldung an die Aufsichtsbehörden muss innerhalb von 72 Stunden erfolgen. Gegebenenfalls sind betroffene Personen unverzüglich zu informieren. Unterlassungen können erhebliche Strafzahlungen zur Folge haben (bis zu zehn Millionen Euro oder zwei Prozent des globalen Umsatzes).

Daher empfehlen wir Unternehmen, Mitarbeiterschulungen durchzuführen und Verfahren zum Erkennen, Untersuchen und Melden von Datenschutzverstößen festzulegen.

Über Act!

Act! macht es Ihnen einfach dauerhafte Beziehungen aufzubauen – greifen Sie schnell und einfach auf personalisierte Kundeninformationen zu. Da jedes Unternehmen einzigartig ist, haben Sie die Freiheit Act! an die Bedürfnisse Ihres Unternehmens und Ihrer Branche anzupassen. Act! ist Ihr flexibler, stets perfekt verbundener Arbeitsplatz.

Endlich eine CRM-Lösung, die perfekt auf Sie zugeschnitten ist.

Erfahren Sie mehr über Act! auf
www.act.com/de

Oder rufen Sie uns an
Deutschland: 0800 1812014
Schweiz: 043 508 2364

Folgen Sie Act!

Swiftpage International Limited | Ground Floor, Q15 Quorum Business Park | Benton Lane, Newcastle upon Tyne | NE12 8BU | act.com/de