DSGVO-Compliance

Wie die CRM-Software Act! 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.

Die DSGVO und Act!

Unternehmen, die ihre Arbeitsweise nach der Datenschutz-Grundverordnung offen kommunizieren, schaffen Vertrauen bei Interessenten und Kunden und erzielen so einen 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.

Als hoch flexible, anpassbare Lösung bietet die CRM-Software Act! eine Reihe von Funktionen, die Nutzer bei der effizienten Verwaltung ihrer Datenprozesse, des Datenschutzes und der Sicherheit unterstützt. Act! ist ein wertvolles Instrument zur Einhaltung der DSGVO und kann im Unternehmen im Rahmen eines umfassenden Compliance-Ansatzes eingesetzt werden. Dieses Dokument beschreibt einige der wichtigsten Richtlinien der DSGVO und zeigt, wie die CRM-Lösung Act! Sie bei der Einhaltung unterstützt.

Inhalt

Neun Bereiche, in denen das CRM-System Act! Sie bei der Umsetzung der DSGVO unterstützt:

1. Definition personenbezogener Daten

Personenbezogene Daten sind Daten, die allein oder in Kombination mit anderen Daten zur Identifizierung einer natürlichen Person verwendet werden können. Die neue DSGVO erweitert den Begriff „„personenbezogene Daten“ um zahlreiche Angaben, mit denen eine Person identifiziert werden kann. Dazu gehören eindeutige Identifikationsnamen und -nummern, IP-Adressen, Daten zum Online-Verhalten und Standortdaten.

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.

2. Verantwortliche und Auftragsverarbeiter

Ein Unternehmen, das festlegt, wie und für welche Zwecke personenbezogene Daten verarbeitet werden, wird als „„Verantwortlicher“ bezeichnet. Ein Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Verantwortliche sind unter der DSGVO an gesetzliche Verpflichtungen gebunden. Das gleiche gilt für Auftragsverarbeiter, die z. B. ein Verzeichnis der Verarbeitungstätigkeiten führen müssen.

3. Geographischer Geltungsbereich

Die DSGVO gilt für alle Unternehmen mit Firmensitz in der EU sowie für Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten. Sie gilt auch für Unternehmen außerhalb der EU.

Wenn Sie den Wohnsitz natürlicher Personen in Act! speichern, können Sie schnell die Datensätze aufrufen, die von der DSGVO betroffen sind. Diese Datensätze lassen sich auch gruppieren, um sie schnell und einfach zu durchsuchen.

Wie kann ich Gruppen in Act erstellen und verwalten?: Antwort-ID 38857

4. Grundsätze des Datenschutzes

Ähnlich wie im Datenschutzgesetz, das vor der DSGVO galt, wird die Verwendung personenbezogener Daten von sechs Datenschutz-Grundsätzen geregelt. 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.
- Die Verwendung muss angemessen, relevant und auf das für die angegebenen Zwecke erforderliche Maß beschränkt sein.

Diese grundsätzlichen Anforderungen sind eng miteinander verknüpft. Act! kann die Verwendung personenbezogener Daten zwar nicht steuern oder begrenzen, unterstützt Sie jedoch bei folgenden Aufgaben:

1 Verfolgen Sie, wie Nutzer Informationen in Datensätzen erstellen, ändern und verwenden.

Die Historienliste in Act! verwenden: Antwort-ID 39123

2 Begrenzen Sie den Zugriff einzelner Nutzer auf Datensätze oder bestimmte Felder, die für ihre Rolle relevant sind.

Sicherheitsrollen in Act!: Antwort-ID 38958

3 Speichern Sie deutlich sichtbar die Wünsche betroffener Personen bezüglich der Verwendung ihrer Daten in der Datenbank. So können Nutzer diese Wünsche beim Verarbeiten der Daten berücksichtigen. Dies betrifft auch Opt-ins oder Opt-outs zu bestimmten Benachrichtigungen und Interessen, damit die Mitteilungen an den Kunden stets relevant sind. Empfänger haben z. B. die Möglichkeit, Kampagnen abzubestellen, die Sie über Act! emarketing[1] versenden. Dieser Artikel erklärt Schritt für Schritt, wie Sie eine Liste aller Opt-outs anzeigen:

Wie erstelle ich in Act! emarketing eine Suche nach nicht zustellbaren Nachrichten oder Opt-outs für Act! v17.2 und höher: Antwort-ID 39122

- Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die angegebenen Zwecke erforderlich ist.

Ihr Unternehmen muss eigene Kriterien für veraltete oder redundante Daten festlegen und Prozesse für die Identifikation und Verwaltung dieser Datensätze definieren. Act! bietet Ihnen dazu mehrere Möglichkeiten:

1 Das Erstelldatum und das Datum der letzten Bearbeitung der Datensätze werden automatisch gespeichert. Sie können diese Daten dann durchsuchen oder filtern, um Alter und Relevanz eines Datensatzes zu prüfen.

2 Erstellen Sie Gruppen für die automatische Segmentierung und kennzeichnen Sie Datensätze, die bestimmten Kriterien entsprechen.

3 Mit der Such-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.

Der folgende Artikel beschreibt, wie Sie in Act! Datensätze nach bestimmten Feldwerten durchsuchen:

Wie kann ich meine Datenbank durchsuchen?: Antwort-ID 38843

Sie können nicht nur einzelne Felder durchsuchen, sondern auch eine Suche mithilfe der Funktionen „AND/OR“ (UND/ODER) erstellen:

Wie verwende ich die erweiterte Suche?: Antwort-ID 38841

Darüber hinaus besteht die Möglichkeit, Gruppen einzurichten. Sie können die Kontakte einer Gruppe statisch und dynamisch zuordnen.

Datenbankfelder in Act! erstellen und verwalten: Antwort-ID 39125

- Personenbezogene Daten werden nicht länger als erforderlich in einer Form gespeichert, die die Identifizierung der betroffenen Personen ermöglicht.

Das Erstell- oder Bearbeitungsdatum von Datensätzen zeigt, wann die letzte Interaktion stattgefunden hat. Anhand dieser Daten können Sie Berichte oder Suchen erstellen und entscheiden, ob der Datensatz weiterhin gespeichert werden muss. Nutzer können beispielsweise nach dem Datum der letzten Interaktion mit einem Kontakt oder dem letzten Änderungsdatum suchen.

Verfolgen Sie Feldänderungen, indem Sie den Historieverlauf für bestimmte Datenbankfelder im Abschnitt zum Definieren von Feldern von Act! aktivieren. So können Sie alle Änderungen nachverfolgen, die der Nutzer an den Daten vorgenommen hat:

Datenbankfelder in Act! erstellen und verwalten: Antwort-ID 39125

- Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Dazu gehört auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schäden. Hierzu müssen geeignete technische und organisatorische Maßnahmen getroffen werden.

Act! bietet zahlreiche Funktionen, die die Sicherheit und den Zugriff auf Datensätze steuern. Sie können z. B. den Benutzerzugriff auf bestimmte Daten begrenzen, indem Sie die Sicherheitsstufe anpassen oder Zugriffsberechtigungen für Felder einrichten. Der eingeschränkte Zugriff durch Nutzer bedeutet, dass diese nur auf Daten zugreifen können, die für sie relevant sind. Damit wird das Risiko „der unbefugten Offenlegung von oder des unbefugten Zugangs zu personenbezogenen Daten“ reduziert.

Sicherheitsrollen in Act!: Antwort-ID 38958

Hinweis: Um Einträge zu Notizen, Historien, Verkaufschancen oder Kontakten auf „Öffentlich“ oder „Privat“ festzulegen, ist ein Offline-Client erforderlich. Informationen zur Erstellung eines Offline-Clients finden Sie im folgenden Artikel:

Wie kann ich meinen Act! Premium Cloud Offline-Client einrichten?: Antwort-ID 37973 (in englischer Sprache)

Act! bietet zahlreiche Funktionen zur Verwaltung der Datensätze und des Datenzugriffs:

1. Sicherheitseinstellungen auf Feldebene sorgen dafür, dass Nutzer nur die Felddaten anzeigen oder ändern können, die für ihre Rolle relevant sind.

Sicherheitseinstellungen auf Feldebene in Act! verwalten: Antwort-ID 39124

2. Der Datensatzzugriff kann für bestimmte Datensätze wie Kontakte, Unternehmen, Gruppen und Verkaufschancen festgelegt werden. Dann ist der gesamte Datensatzinhalt nur für bestimmte Nutzer oder konfigurierte Nutzergruppen sichtbar.

3. Datensatzeinträge wie Notizen, Historien und Aktivitäten können auf den Status „Privat“ festgelegt werden. Sie sind dann nur für den angegebenen Datensatzmanager sichtbar.

4. Fünf Standard-Sicherheitsrollen definieren verschiedene Zugriffsberechtigungen für die Datenbank. Diese reichen vom Zugang nur zu Suchzwecken bis zu vollständigen Administrationsrechten. Diese Rollen legen fest, ob der Nutzer zum Exportieren, Erstellen, Löschen oder Bearbeiten von Datensätzen berechtigt ist.

Informationen zum Einrichten der Zugriffsberechtigungen finden Sie in den folgenden Knowledgebase-Artikeln:

Ändern des Status Öffentlich/Privat von mehreren Notizen, Historien oder Verkaufschancen: Antwort-ID 39119

Überprüfen Sie in Act!, ob die richtigen Sicherheitsrollen und Zugriffsberechtigungen für Nutzer entsprechend ihrer jeweiligen Aufgaben eingerichtet sind.

Wie kann ich eine Zugriffssteuerung für Kontakte für Nutzer in Act! festlegen?: Antwort-ID 39121

Die Funktion zur Datenbanksynchronisierung, mit der Sie eine Remote-Datenbank erstellen können, kann mit einem „Sync Set" durchgeführt werden. Dabei werden nur die Kontaktdaten an den Remote-Nutzer übertragen, die bestimmte Kriterien erfüllen.

Wie kann ich die „Sync Sets" der Remote-Datenbank in Act! verwalten?: Antwort-ID 14072 (in englischer Sprache)

Senden Sie ein Ticket an unser Cloud-Team, um ein „Sync Set" in einer Cloud-Version von Act! hinzuzufügen.

Sie können in Act! für jeden Nutzer einen Benutzernamen und ein Kennwort einrichten. Darüber hinaus bietet Act! die Möglichkeit, eine genaue Kennwortrichtlinie zu konfigurieren, die die Länge, Komplexität, Änderungshäufigkeit und Wiederverwendung von Kennwörtern festlegt.

Nutzer werden im Abschnitt zur Nutzerverwaltung in Act! verwaltet. Hier können Sie ebenfalls ein Kennwort einrichten:

Wie kann ich Datenbanknutzer in Act! erstellen und verwalten?: Antwort-ID 19474 (in englischer Sprache)

Wie kann ich Benutzer für meine Act!-Premium-Cloud-Datenbank hinzufügen oder bearbeiten?: Antwort-ID 38432

Wie kann ich die Einstellungen zur Kennwortkomplexität bearbeiten? Antwort-ID 19180 (in englischer Sprache)

Durch das Erstellen einer Sicherungskopie in Act! schützen Sie Ihre Daten vor Verlust, Zerstörung oder Schäden. Mit einer Zeitgeber-Funktion werden Sicherungskopien in festgelegten Zeitabständen automatisch erstellt. Nutzen Sie diese Funktionen am besten in Verbindung mit einer soliden Backup-Richtlinie.

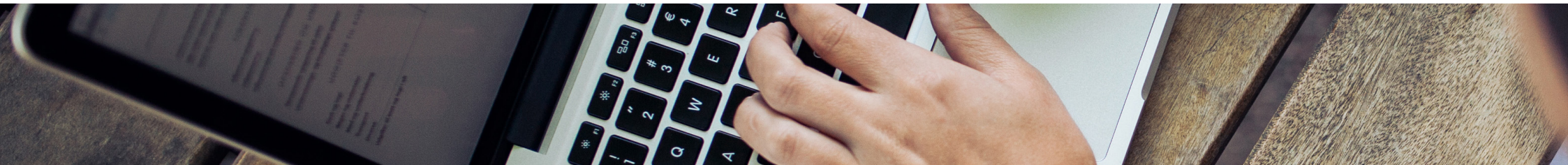
Wie erstellt man eine Sicherungskopie und stellt diese wieder her?: Antwort-ID 38982

Wie kann man den Act! Scheduler nutzen, um automatisierte Sicherungskopien meiner Act! Datenbank zu erstellen?: Antwort-ID 38986

In der Cloud-Version von Act! die Datenbanken alle sechs Stunden automatisch. Informationen zu Sicherungskopien finden Sie in den folgenden Artikeln:

Wie häufig wird ein Backup meiner Act! Premium Cloud Datenbank durchgeführt?: Antwort-ID 39080 (in englischer Sprache)

Wie kann ich die Wiederherstellung eines Backups meiner Act! Premium Cloud Datenbank beantragen? Antwort-ID 39079 (in englischer Sprache)



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. In diesem Dokument befassen wir uns nur mit der Zustimmung als Rechtsgrundlage. Jedoch ist in den meisten Fällen mindestens eine weitere Grundlage für die Datenverarbeitung ebenso wichtig wie die Zustimmung, wenn nicht sogar wichtiger. Die rechtlichen Grundlagen für Unternehmen 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.
Gesetzliche Verpflichtungen	Diese müssen klar und in Bezug auf einen bestimmten Prozess angegeben werden.
Lebenswichtige Interessen	Die Verarbeitung ist erforderlich, um lebenswichtige Interessen einer Person zu schützen.
Öffentliche Aufgabe	Dies gilt nur für Organisationen des öffentlichen Sektors.
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.

Zustimmung

Häufig ist die Zustimmung die rechtliche Grundlage für die Datenverarbeitung zu Marketingzwecken. 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.

Weiter unten wird beschrieben, wie Sie die Zustimmung in Act! emarketing[1] mithilfe von Opt-ins und Opt-outs verwalten.

---

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.

Ganz gleich, welche Daten Sie erfassen – Sie müssen die betroffenen Personen stets darüber informieren, welche personenbezogenen Daten Sie aufbewahren und was Sie damit tun werden. Alle Mitteilungen an Ihre Kunden zur Datenverarbeitung müssen klar formuliert und kostenlos zugänglich sein.

Sie können in Act! ein Feld erstellen, das anzeigt, wenn betroffene Personen über die Verarbeitung ihrer Daten in einem Kontaktdatensatz 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.

Datenbankfelder in Act! erstellen und verwalten: Antwort-ID 39125

Wenn Sie ein Feld erstellt haben, müssen Sie angeben, ob Sie das Feld zu Ihrem Layout hinzufügen möchten. Informationen zur Verwendung des Layout-Designers erhalten Sie hier:

Layouts in Act! erstellen: Antwort-ID 15332 (in englischer Sprache)

Sie können auf Ihrer Website ein Act! Webformular mit doppeltem Opt-in hinzufügen. Das Formular muss ausgefüllt werden, bevor Sie die Daten der betroffenen Person in Act! als Kontaktdatensatz speichern. Wenn die Person das Formular einreicht, wird ein entsprechender Bericht an Act! emarketing[1] gesendet, der zu Audit-Zwecken dient.

Wie kann ich die Funktion „Webformulare" (vormals „Lead-Erfassung") in Act! nutzen?: Antwort-ID 37906 (in englischer Sprache)

Nutzer von Act! sollten einen Prozess implementieren, der regelt, wann und wie Personen über die in Formularen erfassten Daten informiert werden.

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 müssen in einem gängigen Datenformat übermittelt 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.

Act! enthält einen ausführlichen Kontaktbericht. Hier können Sie nach einzelnen Kontakten suchen und eine vollständige Auflistung der gespeicherten Daten zu einem Kontakt erstellen.

Wie kann ich in Act! Berichte erstellen und verwalten?: Antwort-ID 14022 (in englischer Sprache)

Die Daten in den Kontaktfeldern können auch in verschiedene Dateiformate (einschließlich CSV-Dateien) exportiert und so auf einfache Weise an Kunden gesendet werden.

Exportieren Ihrer Kontakt-, Firmen- oder Gruppendaten aus Act! in eine Text- oder durch Kommas getrennte Datei: Antwort-ID 38146

6.3 Recht auf Berichtigung

Die betroffene Person hat das Recht, die Berichtigung ihrer personenbezogenen 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 Act! können Sie einen Datensatz zum Antrag auf Berichtigung anlegen, beispielsweise als Historie. Das Erstelldatum der Historie wird gespeichert. Folgeaktionen bezüglich des Antrags werden dann als zusätzliche Historie oder Aktivität für einen bestimmten Nutzer festgehalten.

Erfassen Sie in Act!, wenn Informationen an Drittanbieter weitergegeben wurden. So können Sie diese schnell kontaktieren, falls die Daten gelöscht werden müssen.

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, die in der DSGVO geregelt sind, müssen personenbezogene Daten gelöscht und dürfen nicht weiter verarbeitet werden. Drittanbieter, an die Daten weitergegeben wurden, müssen ebenfalls informiert werden.

In Act! ist das Löschen von Kontaktdatensätzen einfach: Dabei werden alle Einträge und mit dem Datensatz verknüpfte Daten gelöscht (es sei denn, diese sind mit anderen, verbleibenden Kontakten verbunden). Der Löschvorgang wird in der Act! Historie des Nutzers protokolliert, der die Daten gelöscht hat. Das Protokoll enthält Datum, Uhrzeit und Name des Kontakts.

Erfassen Sie in Act!, wenn Informationen an Drittanbieter weitergegeben wurden. So können Sie diese schnell kontaktieren, falls die Daten gelöscht werden müssen. Setzen Sie einen Prozess für Daten auf, die an Drittanbieter weitergegeben werden.

Wie kann ich Historien in Act! manuell erstellen?: Antwort-ID 38835 (in englischer Sprache)

6.5 Recht auf Einschränkung der Verarbeitung

Natürliche Personen haben das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. In diesem Fall dürfen Sie die personenbezogenen Daten speichern, aber nicht verarbeiten. Speichern Sie nur so viele Informationen, wie es die eingeschränkte Verarbeitung zulässt.

In einem benutzerdefinierten Feld können Sie angeben, dass der Kunde keine Verarbeitung seiner Daten gestattet. Nutzer von Act! müssen darauf achten, diese Vorgabe einzuhalten.

Datenbankfelder in Act! erstellen und verwalten: Antwort-ID 39125

Als weitere Vorsichtsmaßnahme können Sie Kontaktdaten wie Telefonnummern und E-Mail-Adresse aus den Standardfeldern entfernen. So verhindern Sie, dass die betroffene Person unbeabsichtigt kontaktiert wird oder eine E-Mail-Kampagne erhält. Verschieben Sie die Daten in andere benutzerdefinierte Felder, die von Act! nicht gelesen werden, um eine unbeabsichtigte Kontaktaufnahme zu vermeiden.

Wie kann ich die Optionen „Ersetzen", „Tauschen" und „Kopieren" in Act! nutzen? Antwort-ID 38137 (in englischer Sprache)

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 muss innerhalb eines Monats antworten und sollte in der Lage sein, die Daten sicher und ohne Behinderung zwischen IT-Services zu verschieben, zu kopieren oder zu übertragen. 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.

6.7 Widerspruchsrecht

Bei der Nutzung von Act! sind folgende Grundlagen für den Widerspruch relevant:

- Verarbeitung aufgrund von berechtigtem Interesse (einschließlich Profiling)
- Direktmarketing (einschließlich Profiling)

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. Die betroffene Person 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.

In Act! emarketing[1] und Act! emarketing haben Empfänger in der Fußzeile die Möglichkeit, E-Mails einer Kampagne abzubestellen. Die Auswirkungen eines solchen Opt-outs werden in diesem Artikel erläutert.

Wenn ein Kunde meine E-Mail-Kampagnen abbestellt, verhindert das System den Versand an diese Personen oder muss ich diese E-Mail-Adressen aus meiner Datenbank löschen?: Antwort-ID 38681 (in englischer Sprache)

In Act! emarketing[1] können Sie die Empfänger nachverfolgen, die Ihre Kampagnen abbestellt haben. Folgen Sie dazu den Anweisungen in diesem Artikel:

Wie erstelle ich in Act! emarketing eine Suche nach nicht zustellbaren Nachrichten oder Opt-outs für Act! v17.2 und höher: Antwort-ID 39122

Der folgende Artikel beschreibt, wie Sie Opt-outs in Act! emarketing[1] anzeigen:

Wie kann ich auf meine Act! emarketing Opt-out-Liste zugreifen?: Antwort-ID 28591 (in englischer Sprache)

Können Empfänger erneut ihre Einwilligung zum Erhalt von Kampagnen geben?

Falls Empfänger eine E-Mail-Kampagne versehentlich abbestellen oder sich anders entscheiden, können sie erneut ihr Einverständnis zum Erhalt der Kampagne geben. Folgen Sie den Anweisungen in diesem Artikel, um ein Opt-out rückgängig zu machen:

Wie kann ich nicht zustellbare oder abbestellte E-Mails aus meiner Act! Datenbank entfernen?: Antwort-ID 37150 (in englischer Sprache)

Wie importiere ich eine Liste von Opt-outs in Act! emarketing[1]?

Wenn Sie bisher einen anderen E-Marketing-Dienst genutzt oder manuell eine Liste der Opt-outs erstellt haben, können wir diese Liste zu Ihrem Konto hinzufügen. Schicken Sie die Liste im CSV-Format an den technischen Support. Wir senden Ihnen eine Bestätigung, sobald die Opt-outs zu Ihrem Konto hinzugefügt wurden.

Sie wissen nun, wie Sie Opt-outs in Act! emarketing[1] verwalten. Sie können in Act! auch Opt-outs für andere Kommunikationswege nachverfolgen, z. B. SMS oder Postsendungen. Nutzen Sie dazu benutzerdefinierte Felder in Act!. Ausführliche Informationen, wie Sie benutzerdefinierte Felder erstellen und zu Ihrem Layout hinzufügen, finden Sie in den beiden nachfolgenden Artikeln.

Datenbankfelder in Act! erstellen und verwalten: Antwort-ID 39125

Layouts in Act! erstellen: Antwort-ID 15332 (in englischer Sprache)

6.8 Verwalten von Opt-outs und Opt-ins

Kunden können Kampagnen zwar abbestellen, um in Zukunft keine E-Mail-Kampagnen zu erhalten. Bei der Verwendung von Feldfunktionen kann es jedoch zu einer unbeabsichtigten Kontaktaufnahme kommen. Um das Problem zu umgehen, erstellen Sie ein zusätzliches E-Mail-Feld. Wenn Sie Feldfunktionen nutzen oder E-Mail Kampagnen senden, verwendet Act! nur das Standard-E-Mail-Feld. Beispiel: Der Kunde möchte keine Marketing-E-Mails mehr erhalten, Sie müssen aber weiterhin Rechnungen an seine E-Mail-Adresse senden. Das benutzerdefinierte Feld kann verwendet werden, um die E-Mail-Adresse des Kunden zu speichern. Nutzen Sie dazu die Funktionalität von Act! wie im folgenden Artikel beschrieben:

Wie kann ich die Optionen „Ersetzen", „Tauschen" und „Kopieren" in Act! nutzen? Antwort-ID 38137 (in englischer Sprache)

Bei dieser Vorgehensweise benötigen Sie zunächst eine Liste der Opt-outs Ihrer Kampagnen. Der folgende Artikel beschreibt, wie Sie Ihre Opt-outs in Act! anzeigen:

Wie erstelle ich in Act! emarketing[1] eine Suche nach nicht zustellbaren Nachrichten oder Opt-outs für Act! v17.2 und höher?

Wie kann ich auf meine Act! emarketing Opt-out-Liste zugreifen? Antwort-ID 28591 (in englischer Sprache)

6.9 Automatisierte Entscheidungen einschließlich Profiling

Die DSGVO gewährt natürlichen Personen bestimmte Rechte, wenn Sie einer automatisierten Entscheidung und automatisiertem 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.

Act! Administratoren müssen Unternehmens- und Rechtsberater darüber informieren, dass bei der Verwendung von Act! 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 von Act!, 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.

In Act! ist die Funktion „Intelligente Aufgaben" von automatisierten Entscheidungen betroffen. Sie sind dafür verantwortlich, die einzelnen Vorgänge intelligenter Aufgaben regelmäßig zu prüfen und sicherzustellen, dass sie nicht gegen die DSGVO verstoßen. Ein Beispiel hierfür wäre das Einrichten intelligenter Aufgaben mit Bedingungen. Ein Kunde, der Ihre Kampagnen abbestellt hat, könnte beim Ausführen einer intelligenten Aufgabe automatisch eine E-Mail erhalten, wenn die Informationen in seinem Kontaktdatensatz nicht aktuell sind.

In Act! stehen verschiedene intelligente Aufgaben zur Verfügung. (Standardmäßig werden diese jedoch nicht automatisch angewendet.) Informationen zu intelligenten Aufgaben finden Sie in den folgenden Artikeln:

Was sind „Smart Tasks" in Act!?: Antwort-ID 37910 (in englischer Sprache)
Wie kann ich „Smart Tasks" in Act! erstellen und verwalten?: Antwort-ID 26944 (in englischer Sprache)

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.

Dokumentation

Laut DSGVO sind Sie verpflichtet, die Einhaltung der Richtlinien nachzuweisen. Dazu ist es hilfreich, Entscheidungen bezüglich der Verarbeitung personenbezogener Daten zu dokumentieren.

Act! besitzt mehrere Funktionen, mit denen Sie Entscheidungen bezüglich der Verwendung personenbezogener Daten festhalten können:

- Nachverfolgen einer Datensatzquelle in einem Feld
- Anhängen zusätzlicher Dokumente an einen Datensatz, zum Beispiel E-Mails, gescannte Dokumente und Anrufaufzeichnungen.

Einem Kontakt, einer Gruppe, einem Unternehmen oder einer Verkaufschance in Act! ein Dokument anfügen: Antwort-ID 39120

- Speichern von Notizen mit Zeitstempel und Historiedaten für eine Interaktion oder Kennzeichnen eines internen Prozesses, der angewendet wurde.

Die Historienliste in Act! verwenden: Antwort-ID 39123

- Konfigurieren von Feldern zum Aufzeichnen eines Historieeintrags, um Datensatzänderungen zu speichern und zurückverfolgen.

Datenbankfelder in Act! erstellen und verwalten: Antwort-ID 39125

Speichern Sie in Act! Nachweise über die DSGVO-konforme Datenverarbeitung, um der Rechenschaftspflicht nachzukommen. Ein Nutzer kann beispielsweise einen Historieneintrag vornehmen oder auf der Registerkarte für Dokumente eine Datei speichern, z.B. eine archivierte HTML-Seite mit dem Formular, in dem die Daten erfasst wurden. Bieten Sie Schulungen an, die die Mitarbeiter über die Compliance-Anforderungen und deren Auswirkungen auf die Nutzung von Act! informieren.

Nutzer können außerdem interne Dokumente wie Standardarbeitsanweisungen in Act! speichern, entweder als Anhang an Kontaktdatensätze oder als Verknüpfung zu Dokumenten, die außerhalb von Act! gespeichert sind.

Der folgende Artikel erklärt, wie Sie eine Historie erstellen und relevante Dokumente oder Dateien anhängen:

Wie kann ich Historien in Act! manuell erstellen?: Antwort-ID 38835 (in englischer Sprache)

Unternehmen mit weniger als 250 Mitarbeitern müssen ein Verzeichnis über die Verarbeitung von Daten führen, wenn die Verarbeitung der Daten ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt sowie eine Verarbeitung besonderer Datenkategorien oder von personenbezogenen Daten über Straftaten erfolgt. Auch in diesem Fall unterstützt Sie Act! bei der Einhaltung der Richtlinie und kann als Dokumentenspeicher genutzt werden.

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, Act! 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).

Was sind benutzerdefinierte Tabellen in Act! Premium Plus?: Antwort-ID 39057

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.

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 und anderer geltender Datenschutzrichtlinien verfügen. Dies gilt auch, wenn ein Unternehmen nicht zur Ernennung eines Datenschutzbeauftragten verpflichtet ist. Die Mindestanforderungen an diese Tätigkeit sind klar definiert.

9. 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 britischem Recht oder 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).

Meldung von Verletzungen des Schutzes personenbezogener Daten

Datenverarbeitende Unternehmen sind verpflichtet, Datenschutzverletzungen an die zuständige Aufsichtsbehörde zu melden, wenn sie voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Dies ist 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.

Informieren Sie Ihre Mitarbeiter über die Meldepflicht und treffen Sie Vorkehrungen, um Datenschutzverletzungen im Unternehmen zu erkennen, zu untersuchen und zu melden.

Datenverarbeitung von Kindern nach der DSGVO

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 der CRM-Software Act! 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.

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!

1 Die Act! emarketing Server befinden sich in den USA. Wir erfüllen die DSGVO, indem wir personenbezogene Daten auf diese Server übertragen. Falls Sie Act! emarketing nutzen, versichern Sie sich bitte, dass Sie die Anforderungen der DSGVO zur Benachrichtigung Ihrer Act! emarketing E-Mail-Empfänger erfüllen. Laut der DSGVO sind Sie verpflichtet Ihren E-Mail-Empfängern mitzuteilen, dass deren Daten in die USA übertragen werden.

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