Datenschutz in Agenturen

TEIL 3
UMSETZUNG DER DSGVO IN AGENTURSOFTWARE

Datenschutz in Agenturen

TEIL 3 DIE EU-DATENSCHUTZGRUNDVERORDNUNG UND DIE UMSETZUNG IN AGENTURSOFTWARE

Einleitung

Viele Unternehmensprozesse werden digital abgebildet und Unternehmens- oder Agentursoftware stellt einen Schwerpunkt in der Umsetzung des kaufmännischen Kernprozesses – vom Angebot bis zur Rechnungserstellung – dar. Innerhalb der Lösungen werden personenbezogene Daten erfasst und verarbeitet: Mitarbeiterdaten, Informationen über Kunden und Lieferanten, Auskünfte zu Partnern, Abonnenten von Newslettern. Damit ist die eingesetzte Agentursoftware ein zentraler Ort der Datenspeicherung und unterliegt unterschiedlichen gesetzlichen Anforderungen und Vorschriften wie der DSGVO.

Für Sie als Anwender/in ist es wichtig zu wissen, was Ihre Software hier gewährleistet oder an welchen Stellen der Anbieter evtl. noch nachbessern muss.

Und auch, wenn Sie sich aktuell mit dem Gedanken beschäftigen, zukünftig eine Agentursoftware zu nutzen, sollten die Informationen, welche Agentursoftware welche Anforderungen umsetzt zu Ihrer eigenen Sicherheit in die Überlegungen einbezogen werden.

Serie

Die Artikelserie beinhaltet die folgenden Teile:

Teil 1: Worum geht es in der DSGVO, Erklärung wesentlicher Artikel und was müssen demnach Software-Produkte können?

Teil 2: Was müssen Agenturen nun beachten? Beschreibung weiterer Artikel und Schritte zur Umsetzung

Teil 3: Die DSGVO und die Umsetzung durch Software und Anbieter?

EINLADUNG AN DIE ANBIETER

Die Anforderungen des Datenschutzes an Software-Systeme sind wirklich nicht trivial. Viele Anbieter haben mit deren Umsetzung in ihren Systemen und der baldigen Lieferung eines entsprechenden Updates zu kämpfen. Trotzdem liegt es natürlich im ureigenen Interesse der Agenturen, hier nachdrücklich auf eine datenschutzkonforme Version Ihrer Software oder mindestens auf eine klare Terminierung eines entsprechenden Updates zu dringen, da Sie selbst ja zur Einhaltung der Bestimmungen verpflichtet sind.

Für diesen Beitrag wurden 30 Anbieter von Agentursoftware-Produkten angeschrieben. Die Antworten von 16 Anbietern sind hier enthalten.
Die anderen Anbieter hatten sich – nach Selbstauskunft – teils noch nicht (ausreichend) mit der Thematik befasst, waren noch nicht so weit oder haben aus anderen Gründen nicht teil genommen.

UM WAS GEHT ES?

Für die Einhaltung der datenschutzrechtlichen Bestimmungen in Software-Produkten ist es wichtig, wie die Software mit den in ihr gespeicherten Daten umgeht. Konkret betroffen sind die folgenden Themen und Artikel aus der DSGVO:

- „Einwilligung“ (Art.6) und Nachweispflicht (Art.7)
- „Vertraulichkeit“ und „Integrität“ (Art.5)
- Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18)
- Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16)
- Technischer Datenschutz

active.agency	Blue.office	Conaktiv4	easyJob
Thema „Einwilligung" (Art.6) und Nachweispflicht (Art.7)			
Erforderlich sind: • Möglichkeiten zur Bestimmung der gegebenen Einwilligung • Möglichkeit zum Entzug der gegebenen Einwilligung • Hinterlegung von Zeitpunkt und Art • Festhalten des aktuellen Status der Person			
Zustimmung und Entzug werden im Datensatz gespeichert. Optional können Dokumente dazu gespeichert werden. Zur Zustimmungermittlung kann eine autom. Email versendet werden.	Ja es ist möglich bei jedem Kontakt die Daten zur Einwilligung / zum Status und ggf. zum Entzug sowie der Art der Einwilligung zu hinterlegen.	In ConAktiv gibt es im Adressmodul grundsätzlich die Möglichkeit Art und Zeitpunkt der gegebenen Einwilligung nachzuvollziehen. Hier gibt es Felder, die inividuell auf die Bedürfnisse der Artikel 6 und 7 eingerichtet werden können. Der Entzug der Einwilligung kann ebenso in einem vorgesehene Feld dokumentiert werden.	vorhanden (Zusatzfelder, indiv. Auswahllisten)

active.agency	Blue.office	Conaktiv4	easyJob
Thema Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18)			
Datensätze müssen gelöscht und gesperrt werden können. Löschung eines Personendatensatzes aus Kontakt-Tabelle. Beseitigung der „Spuren", die diese Person ggf. in der Software hinterlassen hat, also z.B. Backups, Links etc.. Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, sollten entfernt, andere archiviert und wieder andere gesperrt werden können. Daten-Anonymisierung. (Kunden/Lieferanten/Partner/Mitarbeiter-Daten)			
Sofern die Daten keiner Aufbewahtungspflicht unterliegen können diese Daten gelöscht werden. Aufbewahrungspflichtige Daten können durch die Rechteverwaltung zur Einsicht beschränkt werden.	Kontakte und Firmen lassen sich löschen oder mit einem gesperrt Status versehen. Bei einem Löschen werden aber keine Rechnungen, Aufträge etc. dieses Kontaktes gelöscht, da diese steuerlich relevant sind und behalten werden müssen. Daten aus Backups lassen sich rückwirkend nicht löschen da Backups ja den Status zum Datum X wiedergeben müssen.	In ConAktiv können Daten gelöscht, gesperrt und archiviert werden. Alle zu einem Adressdatensatz gespeicherten Daten können über die Modulkommunikation (Contextcenter) gefunden und gelöscht werden. In der Datensatzhistorie kann das Datum und der Zeitpunkt der Löschung nachvollzogen werden.	Löschen: vorhanden Sperren: vorhanden Anonymisierung: vorhanden "Spuren" beseitigen: geplant

active.agency	Blue.office	Conaktiv4	easyJob
Thema Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16)			
Informationsrecht, das über die Risiken, Vorschriften und Rechte im Zusammenhang mit deren Verarbeitung, aufgeklärt. Unternehmen müssen dokumentieren, wie personenbezogene Daten erhoben, verwendet und verarbeitet werden. 1. Information über die Datenhaltung in Cloudsoftware oder bei Hostingangeboten. (ggf. Zertifikat oder Datenschutzsiegel)			
Hostinginstallation erfolgen durch Beauftragung des Kunden. (Freier Hosterwahl).	blue. Ist keine Cloudlösung sondern wird vom Endkunden lokal eingesetzt, daher sind wir als Entwickler einer Lösung kein Diensteanbieter. Grundsätzlich lassen sich alle Daten die zu einem Kontakt oder einer Firma gespeichert sind gedruckt als PDF oder exportiert als CSV Dokument exportieren und der anfragenden Person aushändigen.	In ConAktiv werden Informationen wie Anlagedatum und Zeitpunkt für jeden Datensatz dokumentiert. In ConAktiv kann dokumentiert werden, wie personenbezogene Daten erhoben, verwendet und verarbeitet werden.	private cloud, dezidierte Server, Rechenzentrum in Deutschland, ISO 9001 und PCI-DSS zertifiziert
2. Aus der Software soll ein Dokument erstellt werden können, das die personenbezogenen Daten zusammenfasst und an den/die Betroffene gesendet werden kann.			
Mit einem einfach Berichtsaufruf kann ein entsprechendes PDF erzeugt werden.	Ja das ist jederzeit möglich.	Ein Dokument mit den angegebenen Anforderungen kann erstellt werden.	Vorhanden

active.agency	Blue.office	Conaktiv4	easyJob
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
1. Schutz erhobener Daten vor unbefugtem Zugriff. Systeme stellt Mechanismen zur Verfügung, die verhindern, dass unberechtigte Personen Daten einsehen können, die dem Datenschutz unterliegen. Das System muss dafür geeignete Berechtigungskonzepte vorweisen können, die den Zugriff, das Löschen, die Weiterverarbeitung innerhalb und den Export regulieren (privacy by design).			
Über die Rechteverwaltung können Datensätze / Datenfelder zur Einsicht gesperrt werden.	Jeder Mitarbeiter im Unternehmen hat eigene Zugangsdaten die sich sehr detailiert eingrenzen lassen, so dass nur die Daten bearbeitet werden dürfen die für den Mitarbeiter relevant sind.	Durch ein differenziertes Rechtesystem in ConAktiv und die Einstellung von Rollen, Filter und Datensatzrechten ist ConAktiv in der Lage den erforderlichen Schutz vor unberechtigtem Zugriff zu gewährleisten.	Vorhanden (mehr als 300 Benutzerrechte)
2. Die oben genannten Berechtigungskonzepte sollen auch als Voreinstellungen vorhanden sein. (privacy/data protection by default).			
Vorgefertigte Berechtigungsgruppen können installiert und dem Kundenwunsch entsprechend angepasst werden.	Ja das ist so vordefinert.	ConAktiv wird mit voreingestellten Rechtegruppen/Einstellungen ausgeliefert! Privatadressen von Mitarbeitern sind automatisch über ein Recht geschützt.	Vorhanden

active.agency	Blue.office	Conaktiv4	easyJob
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
3. Auswirkungen auf die Vertragsgestaltung; z.B. Remote Zugriff auf die Daten bei Updates und Wartung; Datenschutzerklärung			
Bei unbeaufsichtigen Remotezugriffen durch uns wird vorher eine Entsprechende Erklärung vereinbart. U.a. wird definiert welche Personen (Name, Funktion) den Remotezugriff vornehmen darf	Da wir als Entwickler der Lösung auch Fragen zu den gespeicherten Daten erhalten, haben wir einen Vollzugriff auf die gesamte Datenbank. Im Regelfall aber sind wir projektbezogen via NDA und Verträge zur Verschwiegenheit zum Inhalt der Daten verpflichtet.	Es findet kein Remotezugriff auf die Daten bei einem Update statt. Die Datenschutzerklärung in Verbindung mit Wartung wird derzeit den Erfordernissen der DSGVO angepasst!	Vorhanden (Datenschutzerklärung, TOM, ADV)

HQ	KBMpro	Leading	PM//
Thema „Einwilligung" (Art.6) und Nachweispflicht (Art.7)			
Erforderlich sind: • Möglichkeiten zur Bestimmung der gegebenen Einwilligung • Möglichkeit zum Entzug der gegebenen Einwilligung • Hinterlegung von Zeitpunkt und Art • Festhalten des aktuellen Status der Person			
Alle erforderlichen Bestimmungen werden umgesetzt. Bevor personen-bezogene Daten (Userdaten) gespeichert werden, erfragen wir Im Buchungsprozess das Einverständnis des (Neu)Kunden. Der Kunde kann diese Einwilligung jederzeit zurückziehen. Bestandskunden erhalten eine neue Datenschutz-vereinbarung. Zeitpunkt und Art der Einwilligung werden mit Timestamp abgelegt.	Bei jedem Ansprechpartner gibt es Datenfelder, die die Art der Zustimmung, das Datum der Zustimmung und ggf. einen Kommentar dazu enthält. In einer Historie werden alle Änderungen dieser Felder chronologisch protokolliert. KBMpro ermittelt für Bestandskunden automatisch, wo eine Einverständniserklärung z.B. in Form einer Beauftragung vorliegt und trägt diese Informationen beim Ansprechpartner nach. Beim Anlegen neuer Kontakte bietet KBMpro die Option, das Einverständnis der Person mittels automatisch generierter Mail mit einem zur Bestätigung klickbaren Link einzuholen. Auch dies wird dann bei der Person automatisch vermerkt. KBMpro stellt Listen von Personen zur Verfügung, bei denen das Einverständnis fehlt und erlaubt daraus das Erstellen eines Anschreibens, um das Einverständnis nachträglich einzuholen. KBMpro stellt Listen zur Verfügung, in denen alle Personen geführt sind, deren Einverständnis in Kürze erlischt und erlaubt daraus direkt das Erstellen eines Mailings (Brief(Mail/Fax), um so ein Newsletter/Angebot o.ä. zu versenden und damit das Einverständnis einseitig zu erneuern.	Unsere Systeme halten für unsere Kunden nur Daten von Personen mit impliziter Zustimmung, da die Personen in vertraglichen Beziehungen zu unseren Kunden stehen. Das wäre zB bei einem B2C CRM-Tool anders zu sehen.	Lösung über den Funktionsbereich Merkmale bzw. alternativ Zusatzinfos

HQ	KBMpro	Leading	PM//
Thema Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18)			
Datensätze müssen gelöscht und gesperrt werden können. Löschung eines Personendatensatzes aus Kontakt-Tabelle. Beseitigung der „Spuren", die diese Person ggf. in der Software hinterlassen hat, also z.B. Backups, Links etc.. Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, sollten entfernt, andere archiviert und wieder andere gesperrt werden können. Daten-Anonymisierung. (Kunden/Lieferanten/Partner/Mitarbeiter-Daten)			
Auch diese Anforderungen werden bis zum 25. Mai 2018 vollständig erfüllt. Daten können jederzeit vom Kunden gelöscht werden. Nach 35 Tagen werden die Daten aus den Backups entfernt. Eine Daten-Anonymisierung findet nicht statt.	Alle Personendatensätze können gelöscht werden oder per Blacklist gesperrt werden. Die Löschung beseitigt auch alle Spuren z.B. in einer Kontakthistorie, die dort enthaltenen Einträge werden anonymisiert (ausgenommen sind Namen als Texteingaben, die der Benutzer selber z.B. in Kommentarfelder geschrieben hat. Generell Erhalten bleiben Einträge in Auftragsdokumenten wie Rechnungen und Angeboten.In Backups erden die Daten automatisch nach Ablauf der Aufbewahrungsfrist gelöscht. Für Bewerberdaten gibt es ein Portal, welches Bewerbungen direkt über ein Onlineportal in das System aufnehmen kann und zu den gesetzlichen Fristen zur Löschung erinnert. So wird vermieden, dass Bewerberdaten ungewollt in einem E-Mail-Archiv dauerhaft gespeichert werden.	Da nur risikolose Personendaten gespeichert werden und diese nur im Zusammenhang mit Erfüllung vertraglicher Notwendigkeiten erfolgt, ist nach 7 bzw 10 Jahren nach Vertragende die Pseudonymisierung oder Löschung vorgesehen.	Alle Anforderungen werden erfüllt. Daten können sowohl gelöscht, als auch archiviert (Gruppen-Zuordnung) oder gesperrt werden.

HQ	KBMpro	Leading	PM//
Thema Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16)			
Informationsrecht, das über die Risiken, Vorschriften und Rechte im Zusammenhang mit deren Verarbeitung, aufgeklärt. Unternehmen müssen dokumentieren, wie personenbezogene Daten erhoben, verwendet und verarbeitet werden. 1. Information über die Datenhaltung in Cloudsoftware oder bei Hostingangeboten. (ggf. Zertifikat oder Datenschutzsiegel)			
zu 1: Infos über die Datenhaltung etc. können über unsere Datenschutzvereinbarung eingesehen werden. zu 2: Wir bieten zwei Möglichkeiten zur Auskunft: Entweder können alle Daten über eine Exportfunktioniert exportiert oder über API-Schnittstelle abgerufen werden.	Wir bezeichnen unsere Software als „GSDVO-Ready“. Eine Zertifizierung wird angestrebt, sobald es hier etwas offizielles oder allgemein anerkanntes gibt.	Dazu gibt es unser Verarbeitungsverzeichnis gemäß Art 30 EU-DSGVO. Unser Cloud Hosting wird basierend auf ISO 27001 angeboten.	Das System protokolliert weitestgehend automatisch. Darüber hinaus können Daten in der Datei "Kontaktnotizen" erfasst und gepflegt werden.
2. Aus der Software soll ein Dokument erstellt werden können, das die personenbezogenen Daten zusammenfasst und an den/die Betroffene gesendet werden kann.			
Zu 2: Es kann kein automatisiertes Dokument erstellt werden, es sind aber alle Daten maschinenlesbar exportierbar sowie über die offene Rest Api abrufbar.	Hierfür gibt es eine Funktion, die ein entsprechendes PDF zur Verfügung stellt.	Das könnte eine Funktion sein, die sich Kunden wünschen, wobei Sie rechtlich nicht erforderlich ist aufgrund der Dateninhalte. Wir selbst leiten Anfragen an den Verantwortlichen, den Kunden, und beauskunften ja nicht.	Es sind diverse Möglichkeiten vorhanden, um ein derartiges Dokument individuell zu konfigurieren und als Formular und/oder Funktion zu hinterlegen.

HQ	KBMpro	Leading	PM//
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
1. Schutz erhobener Daten vor unbefugtem Zugriff. Systeme stellt Mechanismen zur Verfügung, die verhindern, dass unberechtigte Personen Daten einsehen können, die dem Datenschutz unterliegen. Das System muss dafür geeignete Berechtigungskonzepte vorweisen können, die den Zugriff, das Löschen, die Weiterverarbeitung innerhalb und den Export regulieren (privacy by design).			
Alle Verarbeitungsprozesse wurden kritisch überprüft. Wir führen nur Prozesse der personenbezogenen Datenspeicherung durch, wenn diese auch wirklich notwendig sind. Jeder Kunde kann den Datenzugriff je nach Rolle im Unternehmen unterschieldlich gestalten und den Zugriff auch beschränken. Der Kunde kann diese Konfiguration auf Wunsch selbst vornehmen. Grundsäztzlich ist vorgesehen, dass nur Nutzer mit Admin-Rolle Einsicht in alle Daten haben. Alle anderen User haben eine eingeschrönkte Einsicht. Disee Voreinstellungen können manuell angepasst werden. Alle Daten werden nur verschlüsselt gespeichert um den Zugriff von dritten zu verhindern.	KBMpro verfügt über ein detailliertes Rechtesystem, welches den Zugriff jedes einzelnen Mitarbeiters in Bezug auf einzelne Kunden regelt. Im Zuge der Novellierung des Datenschutzes wurden nun auch Funktionen integriert, die eine Einschränkung auf Personengruppenebene erlauben.	Eine große Zahl unserer Kunden dokumentieren das, indem sie mit unseren System SOX Compliance erreichen.	Individuelle Zugriffsrechte in der Datei "Passwörter" konfigurierbar. Über den Funktionsbereich "Gruppen" können einzelene Datensätze vor Zugriff durch Unberechtigte gewschützt werden. Darüber hinaus können "private" Informationen in Datensätzen zusätzlich geschützt werden.
2. Die oben genannten Berechtigungskonzepte sollen auch als Voreinstellungen vorhanden sein. (privacy/data protection by default).			
Das Berechtigungskonzept ist als Standard konfiguriert	Die o.g. Funktion ist standardmäßig aktiviert, wenn ein neuer Mitarbeiter angelegt wird, so dass neue Mitarbeiter erst einmal gar keine Personendatensätze sehen können.	Ist so.	Mit der Funktion "Passwortprofile" gelöst.

HQ	KBMpro	Leading	PM//
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
3. Auswirkungen auf die Vertragsgestaltung; z.B. Remote Zugriff auf die Daten bei Updates und Wartung; Datenschutzerklärung			
??	Wir stellen unseren Kunden eine Muster AV nach neuem Stand der DSGVO zur Verfügung, dort sind auch unsere TOM ausführlich erläutert, insbesondere auch in Bezug auf ein Support-/Update-Szenario. Hostet der Kunden unsere Software selber, fallen einige der TOM in den Verantwortungsbereich des Kunden (z.B. in Bezug auf Backups).	Ist teilweise bereits umgesetzt. Wir legen im April als Service allen unseren Kunden rechtzeitig bilaterale Vereinbarungen über die Auftragsverarbeitung nach Art 28 DSGVO vor. Durch deren Gegenzeichnung werden Sie sehr bequem ED-DSGVO compliant in Bezug auf die System von Qualiant.	Sofern erforderlich, werden wir unsere Verträge entsprechend ergänzen.

Poool	PowerAd	Projektron	ProSonata
Thema „Einwilligung" (Art.6) und Nachweispflicht (Art.7)			
Erforderlich sind: • Möglichkeiten zur Bestimmung der gegebenen Einwilligung • Möglichkeit zum Entzug der gegebenen Einwilligung • Hinterlegung von Zeitpunkt und Art • Festhalten des aktuellen Status der Person			
Kann für relevante Datensätze über das Poool-Tagging abgebildet werden. Über Notizen können noch weitere Details dokumentiert werden. Über das Poool-Kontakte Modul können nur Datensätze selektiert werden, welche die Einwilligung erteilt haben.	"Einwilligung" sollte nur das allerletzte Mittel für die rechtmäßige Verwendung pbD (*Personenbezo-gener Daten; Anm. Redaktion) sein, Wenn pbD in powerAD gespeichert werden, erfolgt dies zum Großteil auf Grund gesetzlicher Vorschriften (Rechnungslegungsgesetz), zur Erfüllung des Vertragsgegenstandes, oder eines im Verzeichnis der Verarbeitung festgelegten Zwecks,	Kann bis Vesion 18.4 durch den kunden konfiguriert werden. Ist ab Version 18.4 im Standard verfügbar.	Nutzung der frei konfigurierbaren Filter der Ansprechpartner; hier kann z.B. eine Checkbox „Datenverarbeitung zugestimmt" integriert werden. Zusätzlich steht ein Freitextfeld zur weiteren Dokumentation (wann, wie lange) Verfügung.

Poool	PowerAd	Projektron	ProSonata
Thema Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18)			
Datensätze müssen gelöscht und gesperrt werden können. Löschung eines Personendatensatzes aus Kontakt-Tabelle. Beseitigung der „Spuren", die diese Person ggf. in der Software hinterlassen hat, also z.B. Backups, Links etc.. Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, sollten entfernt, andere archiviert und wieder andere gesperrt werden können. Daten-Anonymisierung. (Kunden/Lieferanten/Partner/Mitarbeiter-Daten)			
Personen-Datensätze können aus dem Adressbuch gelöscht werden. Für sensible Mitarbeiterinformationen gibt es einen separten, zusätzlich abgesicherten Bereich. Das selektive Löschen von Datensätzen aus Backups ist nicht notwendig, da der Grundsatz in der DSGVO vorsieht, dass Daten auch verarbeitet / genutzt / verknüpft werden können. Backups mit gelöschten Datensätzen sondern sich über die Erstellung von neuen Backup-Zyklen laut unseren internen Sicherungsrichtlinien mit der Zeit automatisch aus.	Die Löschung ergibt sich aus der im Verarbeitungsverzeichnis festgelegten First, oder bei direkter Aufforderung durch den Betroffenen, sofern gesetzliche Fristen für die Aufbewahrungsplicht abgelaufen sind und der Betroffenen eindeutig seine Identität nachweisen kann, erfolgt die Löschung, wobei exakt dokumentiert wird, wer wann und was gelöscht wurde. Das in unserer Datenbank integrierte Backups darf aus Integritätsgründen, nicht verändert werden. Nach einen regulären Restore wird zwar der zu löschende Datensatz wiederhergestellt, das abgearbeitet Backup-Log löscht den Datensatz aber auch gleich wieder, bevor ein Benutzer Zugriff auf die Daten hat. Bei einem Restore ausserhalb unseres Datenbank-Backups können die in einer gesonderten Datei gespeicherten Lösch-Datensätze überprüft, manuell zur Überprüfung eingelesen werden, wodurch dann die Datensätze wieder gelöscht werden.	Personendaten werden in der Voreinstellung beim Löschen gesperrt (Papierkorbfunktion).	**Firmenkontakte:** Ansprechpartner können von Benutzern mit entsprechenden Rechten gelöscht werden (die Firmenadresse bleibt erhalten). Ggf. vorhandene CRM-Daten werden dabei ebenfalls gelöscht. In vorhandenen Belegen (Angebote, Rechnungen etc.) bleibt die Person aufgrund gesetzlicher Vorgaben (Aufbewahrungsfristen der original und unveränderten Belege) weiterhin genannt. **Mitarbeiter:** Die erfassten Daten sollten über Verträge oder Betriebsvereinbarungen festgelegt werden. Scheidet ein Mitarbeiter aus dem Unternehmen aus, kann der Benutzer entweder umbenannt und archiviert werden (es bleibt ein Bezug zur Person vorhanden) oder komplett gelöscht werden (volle Anonymisierung der erfassten Daten). **Backups:** Es besteht kein freier Zugriff auf die Backups seitens der Benutzer. Backups werden 4 Wochen vorgehalten. Sollte eine Person von ihrem Recht auf Löschung der Daten Gebrauch machen, können die Daten durch uns aus den Backups gelöscht werden.

Poool	PowerAd	Projektron	ProSonata
Thema Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16)			
Informationsrecht, das über die Risiken, Vorschriften und Rechte im Zusammenhang mit deren Verarbeitung, aufgeklärt. Unternehmen müssen dokumentieren, wie personenbezogene Daten erhoben, verwendet und verarbeitet werden. 1. Information über die Datenhaltung in Cloudsoftware oder bei Hostingangeboten. (ggf. Zertifikat oder Datenschutzsiegel)			
Wir stellen unseren Kunden neben einem Vertrag für Auftragsdatenverarbeiter auch ein Verarbeitungsverzeichnis inkl. Beschreibung personenbezogener Daten als kostenlosen Service für die eigene Dokumentation zur Verfügung.	Das Recht auf Auskunft und die Transparenz bzw. Information wo die pbD verwendet wurden steht im Verarbeitungsverzeichnis und kann bei berechtigter Anfrage (Identitätsnachweis) sofort ausgedruckt und Übermittelt werden (ist die Vorstufe zur Löschung und erfolgt im gleichen Ablauf). Die Daten unserer Software werden in keiner Cloud gespeichert, sondern auf lokalen Servern der Agentur und somit im EU Raum.	Projektron ist nach ISO 27001 zertifiziert. Die VAV sind Bestandteil des Vertrages und werden auf Nachfrage auch Interessenten zugeschickt.	Wir schließen mit jedem Kunden einen Vertrag zur Auftragsverarbeitung gemäß DSGVO ab, der alle Details dokumentiert und regelt.
2. Aus der Software soll ein Dokument erstellt werden können, das die personenbezogenen Daten zusammenfasst und an den/die Betroffene gesendet werden kann.			
Diese Information stellen wir unseren Kunden bei Bedarf kostenlos über unseren Support zur Verfügung.	Die im vorherigen Punkt ermittelten Daten können als xml-Datei exportiert und zur Verfügung gestellt werden.	So ein Bericht kann durch den Kunden erstellt werden.	Eine entsprechende Funktion steht demnächst zur Verfügung: Es kann ein PDF mit den vorhandenen personenbezogenen Daten eines Firmen Ansprechpartners erstellt werden. Weitere Daten, wie CRM Ereignisse sind ebenfalls exportierbar.

Poool	PowerAd	Projektron	ProSonata
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
1. Schutz erhobener Daten vor unbefugtem Zugriff. Systeme stellt Mechanismen zur Verfügung, die verhindern, dass unberechtigte Personen Daten einsehen können, die dem Datenschutz unterliegen. Das System muss dafür geeignete Berechtigungskonzepte vorweisen können, die den Zugriff, das Löschen, die Weiterverarbeitung innerhalb und den Export regulieren (privacy by design).			
Zugriffsrechte können über Rollen oder auch personenbezogen vergeben werden. Es besteht die Möglichkeit den Bereichszutritt zu gewähren. Je nach Bereich können zusätzlich Lese- und Schreibrechte wie auch die Angabe von kaufmännischen Informationen gesondert geregelt werden.	Das Berechtigungssystem in unserer Software war von Beginn an und ist natürlich jetzt genau für diesen Zweck eingerichtet. Es wird jetzt noch um eine weitere Berechtigung erweitert, dass die DSGVO-Funktionen (Löschen, Auskunft, Export usw.) nur der/dem Datenschutz-Verantwortliche(n) oder Datenschutzbeauftragte(n) zur Verfügung stehen.	Projektron verfügt über ein detailliertes Berechtigungskonzept. Durch das Rechtekonzept können Rechte zum Einsehen, zur Weiterverarbeitung, Export von Daten und zum Löschen je nach Rolle und Objekttyp definiert werden.	Schutz der Server und Software durch verschlüsselte und beschränkte Zugriffe. ProSonata besitzt schon immer das Konzept der vordefinierten Benutzergruppen (Rechte). Mitarbeitern werden je nach Rechtestufe Programmbereiche angezeigt. Die Firmenverantwortlichen (Administrator) entscheiden, welche Benutzer welche Rechtestufe erhalten.
2. Die oben genannten Berechtigungskonzepte sollen auch als Voreinstellungen vorhanden sein. (privacy/data protection by default).			
Kann über das Rollen-System vordefiniert werden.	Diese Berechtigungen können nur über die Voreinstellungen durch den Verantwortliche(n) vor Ort übertragen werden und können von uns (Softwarehersteller) nicht zugewiesen werden.	Es gibt eine grobe Voreinstellung. Das Rechtekonzept muss aber je nach Branche und Zweck der Dokumentation an die Vorgaben der DSGVO angepasst werden.	siehe Punkt 1. Rechte der Benutzergruppen sind immer vordefiniert.

Poool	PowerAd	Projektron	ProSonata
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
3. Auswirkungen auf die Vertragsgestaltung; z.B. Remote Zugriff auf die Daten bei Updates und Wartung; Datenschutzerklärung			
Der Poool Datenschutz und die Vertraulichkeit werden in einem Höchstmaß über unsere AGB und unser Verarbeitungsverzeichnis gewährleistet und vor allem und auch am Wichtigsten, in der Praxis auch so gehandhabt.	Da ein direkter Remote Zugriff ohne Verwendung der Client Software nicht möglich ist, kann ein Remotezugriff auf die Daten ohne Zustimmung des Kunden nicht erfolgen. Während eines Remotezugriff kann jeder Schritt vom Datenschutzverantwortlichen mitverfolgt werden, dafür gibt es eigene SLA. Sollte die Übertragung aller Daten an uns notwendig sein, erfolgt dies nach einer gesonderten Vereinbarung und stellen für den Transfer eine verschlüsselte Verbindung und einen sicheren Aufenthaltsort auf unserer eigenen privaten Cloud zur Verfügung, Daten, die via öffentlich zugänglichen unverschlüsselten Transport, oder über ungesicherte Drittländer (z.B. Dropbox) von den Kunden zur Verfügung gestellt werden, werden von uns nicht angenommen.	Im Hostingvertrag ist die VAV nach EU DS-GVO enthalten.	Details sind im Vertrag zur Auftragsverarbeitung geklärt.

QuoJob	Revolver	Teambox	Troi
Thema „Einwilligung" (Art.6) und Nachweispflicht (Art.7)			
Erforderlich sind: • Möglichkeiten zur Bestimmung der gegebenen Einwilligung • Möglichkeit zum Entzug der gegebenen Einwilligung • Hinterlegung von Zeitpunkt und Art • Festhalten des aktuellen Status der Person			
Funktion für die Hinterlegung der gegebenen Einwilligung inkl. Datum. Löschung des Datensatzes bei entzogener Einwilligung. Selektionsmöglichkeiten.	Die erteilte Einwilligung kann unter dem jeweiligen Datensatz eingetragen und als PDF hinterlegt werden. Zusätzlich ist es möglich den Zeitpunkt des Entzugs zu hinterlegen. Der aktuelle Datenschutz-Status der Person ist in der Adressliste jederzeit einsehbar.	Bei Personen kann die Einwilligung (inkl. Datum und Info) sowie der aktuelle Status hinterlegt werden. Die Änderungen können über ein detailliertes Änderungsjournal nachvollzogen werden.	Troi plant ein Datenschutzmodul umzusetzen, über welches Agenturmitarbeiter (berechtigte Personen) pro Verfahrensverzeichnis und Nutzer eine Übersicht der Einwilligungen und Ablehnungen sowie deren Verlauf managen können. Der Nutzer kann über einen persönlichen Bereich Einwilligungen geben und entziehen.

QuoJob	Revolver	Teambox	Troi
Thema Datenspeicherung: Begrenzung und Löschung (Art.5, 17, 18)			
Datensätze müssen gelöscht und gesperrt werden können. Löschung eines Personendatensatzes aus Kontakt-Tabelle. Beseitigung der „Spuren", die diese Person ggf. in der Software hinterlassen hat, also z.B. Backups, Links etc.. Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, sollten entfernt, andere archiviert und wieder andere gesperrt werden können. Daten-Anonymisierung. (Kunden/Lieferanten/Partner/Mitarbeiter-Daten)			
Personenbezogene Datensätze, die keiner Aufbewahrungsfrist unterliegen, lassen sich komplett und rückstandslos aus dem System löschen. Datensätze, die einer Aufbewahrungsfrist unterliegen, lassen sich ausblenden und stehen nur noch für aufbewahrungspflichtige Dokumente zur Verfügung.	Revolver bietet ab der Version 8.8 eine Lösch- und Sperr-Funktion an. Jede Änderung und Löschung wird in einer eigenen Liste dokumentiert. Für jede Datenverarbeitung werden entsprechende Gesetzesvorlagen für die Speicherung hinterlegt.	Personen können entweder gelöscht (Beseitigung der "Spuren") oder über Deaktivierung gesperrt werden. Zusätzlich wird die Möglichkeit einer Löschliste geschaffen, in der automatisch Datensätze aufgelistet werden, die nach hinterlegten Löschfristen gelöscht werden können/sollen. Die Mitarbeiterzuordnung wird beim Löschen anonymisiert.	Im geplanten Modul können Nutzer über Troi die Löschung Ihrer Daten beantragen.

QuoJob	Revolver	Teambox	Troi
Thema Information/Auskunft und Transparenz (Art.5, 12, 13, 15, 16)			
Informationsrecht, das über die Risiken, Vorschriften und Rechte im Zusammenhang mit deren Verarbeitung, aufgeklärt. Unternehmen müssen dokumentieren, wie personenbezogene Daten erhoben, verwendet und verarbeitet werden. 1. Information über die Datenhaltung in Cloudsoftware oder bei Hostingangeboten. (ggf. Zertifikat oder Datenschutzsiegel)			
Rechenzentrumanbieter ist nach ISO 27001Zertifiziert	Über das revolvereigene DSGVO-Modul werden personenbezogen alle Verfahren inkl. aller dazugehörigen Informationen zusammengestellt.	Wir schließen mit unseren Kunden eine Vereinbarung zur Auftragsverarbeitung. Zudem wird in unserer Datenschutzerklärung festgehalten, wie wir mit erhobenen Daten umgehen.	Im geplanten Modul kann der Nutzer über seinen persönlichen Bereich Informationen über die einzelnenen Verfahren einsehen. 1. Die Datenhaltung bzw. -speicherung und das Hosting wird über ein Sicherheitskonzept gemäß der ISO/IEC 27001(zertifiziert) sichergestellt.
2. Aus der Software soll ein Dokument erstellt werden können, das die personenbezogenen Daten zusammenfasst und an den/die Betroffene gesendet werden kann.			
Kontakthistorie kann als PDF ausgegeben werden.	Wird eine Auskunft eingefordert, kann ein automatisierter Ausdruck alle Daten zusammenfassen und dem Antragsteller zugestellt werden.	Ein Werkzeug zur Datenauskunft wird umgesetzt.	2. Im geplanten Modul kann der Nutzer in seinen persönlichen Bereich einen verschlüsselten Export seiner personbezogenen Daten anfordern.

QuoJob	Revolver	Teambox	Troi
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
1. Schutz erhobener Daten vor unbefugtem Zugriff. Systeme stellt Mechanismen zur Verfügung, die verhindern, dass unberechtigte Personen Daten einsehen können, die dem Datenschutz unterliegen. Das System muss dafür geeignete Berechtigungskonzepte vorweisen können, die den Zugriff, das Löschen, die Weiterverarbeitung innerhalb und den Export regulieren (privacy by design).			
Spezielle Berechtigung für vertrauliche HR-Daten. Generelles Berechtigungskonzept für den Zugriff auf Kontakte mit Zugriffsrechten für lesen/schreiben/nein	Revolver bietet ein Berechtigungssystem, mit dem bestimmte Nutzergruppen vom Zugriff auf personenbezogenen Daten ausgeschlossen werden können.	Die TEAMBOX verfügt über ein differenziertes Berechtigungskonzept mit speziellen Berechtigungen für private bzw. sensible personenbezogene Daten.	Die technisch organisatorischen Maßnahmen (Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle, Übertragungskontrolle, Eingabekontrolle, Transportkontrolle, Wiederherstellbarkeit, Zuverlässigkeit, Datenintegrität, Auftragskontrolle, Verfügbarkeitskontrolle, Trennbarkeit) werden bei Troi eingehalten und in der ADV dokumentiert .
2. Die oben genannten Berechtigungskonzepte sollen auch als Voreinstellungen vorhanden sein. (privacy/data protection by default).			
Berechtigungskonzepte lassen sich pro Usergruppe voreinstellen	Voreingestellte DSGVO - Gruppen mit den entsprechenden Rechten wird es in einer späteren Beta Version geben.	Die Berechtigungen sind bie Neuinstallationen nach dem "Privacy by Default" Prinzip voreingestellt. Die Verwaltung erfolgt dann durch den Agentursoftware Administrator in der Agentur.	In Troi werden Berechtigungs-konzepte zur Verfügung gestellt. Da die Rechteverwaltung in Troi jedoch sehr individuell justiert werden kann, wird diese beim System-Set-Up zusammen mit dem Kunden aufgesetzt. So kann gewährleistet werden, dass das Konzept auf den jeweiligen Kunden abgestimmt ist.

QuoJob	Revolver	Teambox	Troi
Thema „Vertraulichkeit" und „Integrität" (Art.5), Technischer Datenschutz			
3. Auswirkungen auf die Vertragsgestaltung; z.B. Remote Zugriff auf die Daten bei Updates und Wartung; Datenschutzerklärung			
Datenschutzvertrag nach DVSGO	Der Punkt „Auftragsverarbeitungsvertrag" wird in einer späteren Beta-Version eingearbeitet werden. Hierbei wird ein personalisierter Vertrag aus dem System heraus generiert. Die entsprechenden Unterlagen können dem Datensatz des Auftragnehmers hinzugefügt werden.	Wir schließen mit unseren Kunden eine gesonderte Vereinbarung zur Auftragsverarbeitung.	Troi aktualisiert seine Verträge, insbesondere die ADV, um die Anforderungen gemäß der DSGVO umzusetzen.

Diese Liste erhebt keinen Anspruch auf Vollständigkeit.

Für die Richtigkeit und Vollständigkeit der Angaben wird keine Gewährleistung oder Haftung übernommen: Die Angaben wurden durch die Anbieter erstellt und von uns übernommen.