prosozial GmbH

Wie erfüllt prosozial den Datenschutz?

- **DSGVO-konform** per Design: comp.ASS 21 und butler 21 Services
- Sicherheitsmaßnahmen im prosozial-Rechenzentrum
- Zertifikate, Freigaben, Befähigungsnachweise

INHALT

Hinweis:
Aufgrund der besseren Lesbarkeit wird in diesem Text nur die männliche Schreibweise verwendet. Wir bitten alle lesenden Personen um Verständnis.

1. Datenschutz per Design

DSGVO-Konformität der IT-Lösungen comp.ASS und butler im Hosting

IT-Lösungen aus dem Hause prosozial unterstützen öffentliche wie freie Träger bei einem optimalen Verwaltungshandeln in allen Bereichen der verschiedenen Sozialgesetzbücher (SGB) und des Betreuungsrechts. Das Erheben vieler Daten bei Leistungsberechtigten ermöglicht erst das gesetzlich geschuldete Planen und Bereitstellen passgenauer Hilfeangebote. Es ist die Voraussetzung für die Verknüpfung der Informationen zu optimal gesteuerten Fachprozessen rund ums „Fallmanagement“.

So umfasst z.B. **comp.ASS** insgesamt die fachlichen Großbereiche der SGB II, III, VIII, IX und XII sowie des Asylrechts, Bildungs- und Teilhabeleistungen, Landesblindengeld usw. mit den Funktionsbereichen:

- Leistungssachbearbeitung (Antrag, Berechnung, Bescheidung, Gewährung usw.),
- Hilfeplanung und Case-, Care- oder Fallmanagement,
- Träger- und Hilfemanagement.

butler wird von Betreuungsbehörden, Betreuungsvereinen und Betreuern eingesetzt für die fachlichen Bereiche Sachverhaltsermittlung, die Registrierung von Betreuern, das Führen von Betreuungen, Pflegschaften, Vormundschaften und anderen Dienstleistungen, sowie die Betreuungsplanung.

Im Folgenden wird dargestellt, welche Anforderungen beide Lösungen bereitstellen, um datenschutzkonform eingesetzt zu sein.

Der Datenschutz in Deutschland ist seit dem 25.05.2018 federführend durch die *Datenschutz-Grundverordnung der EU (DSGVO)* und ergänzend durch das Bundesdatenschutzgesetz (BDSG) und entsprechende Landesdatenschutzgesetze (LDSG) sowie die Datenschutzgesetze der Kirchen geregelt. Darüber hinaus greifen spezielle Rechtsnormen, die den allgemeinen vorausgehen. So ist der Sozialdatenschutz für die einzelnen Sozialgesetzbücher im SGB I und SGB X im Allgemeinen und in den einzelnen Sozialgesetzbüchern im Speziellen geregelt. Eine Broschüre („*Sozialdatenschutz* (Info 3)“) des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gibt hier einen guten Überblick: *www.bfdi.bund.de.* Das *Betreuungsorganisationsgesetz* (BtOG) liefert eine erste Orientierung, wie die einzelnen Akteure innerhalb des Betreuungswesens (BtOG: § 4 Behörden, § 18 Vereine, § 20 Betreuer) mit der Verarbeitung personenbezogener Daten umgehen sollten.

Der Datenschutz bezieht sich auf alle personenbezogenen Äußerungen und Medien. Dazu gehören Aufzeichnungen auf Papier z.B. Gesprächsaufzeichnungen, Protokolle und Mitschriften, sowohl in der Handakte, auf der Schreibauflage, aber auch im Papierkorb. Digitale Dokumentationen erfolgen heutzutage in einer Fachsoftware, über die allein Bescheide erzeugt und Hilfen in Gang gebracht werden können. Schutzwürdige personenbezogene Daten sind also in der Fachsoftware und ggfs. in einem externen Dokumentenmanagementsystem (DMS) oder einem E-Akte-System zu finden.

1.1 Grundsätze für die Datenverarbeitung nach der DSGVO und deren Umsetzung in butler und comp.ASS

Es gelten nach Artikel 5 DSGVO folgende „Grundsätze für die Verarbeitung personenbezogener Daten“:

1.1.1 Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Artikel 5 Abs. 1 lit. a DSGVO

Nach Artikel 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten „auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise“ verarbeitet werden. Darauf sind IT-Lösungen von prosozial zugeschnitten:

- **Rechtmäßigkeit:** In der Regel werden butler und comp.ASS in Bereichen angewendet, in denen Daten zur Erfüllung rechtlicher Verpflichtungen erhoben werden bzw. in denen entsprechende Gesetze die Datenerhebung erlauben. Beispielsweise werden Einrichtungen der freien Träger beauftragt, Maßnahmen nach SGB II, SGB VIII, SGB IX oder SGB XII durchzuführen. Mit unseren IT-Lösungen kann dieser Kontext abgebildet und Personendaten auf z.B. eine Maßnahme, ein Projekt, einen Betreuungsbeschluss etc. bezogen werden.
- **Treu und Glauben:** Der Zugang zu unseren Expertensystemen ist durch ein klares Benutzersystem geregelt. Jeder Nutzer hat eine eigene Anmeldung mit Kennwort und individuell zugeteilte Berechtigungen. Dabei sind unsere Anwender meist ausgebildete, sensibilisierte Fachkräfte aus Sozialwesen, Verwaltung und Betreuungswesen, die von Berufs wegen bzw. von Amts wegen dem Datenschutz verpflichtet sind.
- **Transparenz:** butler und comp.ASS sind so konzipiert, dass alle Zugänge und Zugriffe auf Daten mitgeloggt werden. So bleibt stets nachvollziehbar, wer Daten eingegeben oder verändert hat bzw. welcher Anwender auf welche Daten zugegriffen hat. Die Kontrolle ist abhängig von entsprechenden Benutzerberechtigungen.

1.1.2 Zweckbindung

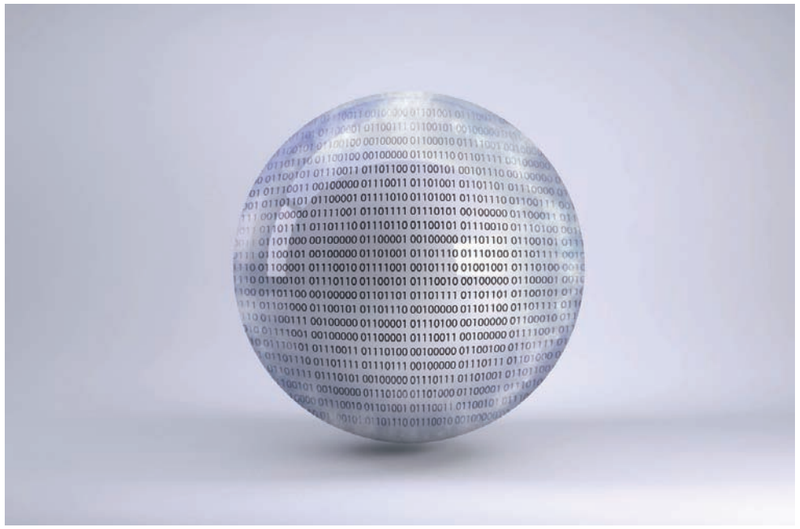
Artikel 5 Abs. 1 lit. b DSGVO

Personenbezogene Daten dürfen nur für die Zwecke verarbeitet oder genutzt werden, für die sie erhoben worden sind. Nun sind die „Zwecke“, die unsere Kunden zu erfüllen haben (etwa im Rahmen der Fürsorgepflicht eines kommunalen oder freien Trägers der jeweiligen Sozialgesetzbücher) vielfältig, komplex und umfassend. Sie bestehen darin,

- arbeitslose Menschen mit ihren Ressourcen, aber auch multiplen „Vermittlungshemmnissen“ in Arbeit zu vermitteln,
- Leistungen zu bewilligen und auszuzahlen, um ein dem Existenzminimum entsprechendes Dasein zu ermöglichen,
- Bildungsmaßnahmen rechtlich zu organisieren,
- Menschen im Sinne des Betreuungsrechts zu betreuen oder
- einen passenden Berufsbetreuer zu finden und dem Gericht vorzuschlagen

u.v.m.

Solche Aufgaben sind notwendigerweise mit sehr vielen Informationen und Daten verbunden. butler und comp.ASS sind Expertensysteme, die zu diesen Zwecken in z.T. komplexen Organisationsstrukturen eingesetzt werden. Dabei steuern verschiedene Voreinstellungen, die systemimmanent sind oder von einer verantwortlichen Stelle vorgenommen werden können, welche Funktionen, Datenfelder und Akten den unterschiedlichen Anwendern zum jeweiligen Zweck zur Verfügung stehen.



Organisatorisch können die IT-Systeme so eingestellt werden, dass bestimmte Anwender nur auf bestimmte Datenbereiche Zugriff haben, wobei darauf zu achten ist, dass die Aufgaben noch erfüllt werden können.

Unsere IT-Lösungen bieten hierzu folgende Möglichkeiten:

- die Zuordnung von Anwendern zu Organisationseinheiten,
- die Vergabe von Eigentums-, Besitz- und Leserechten an Dokumenten und Akten,
- die Nutzung der Sozialgeheimnisfunktion in entsprechenden Situationen.

1.1.3 Datenminimierung bzw. Datensparsamkeit

Artikel 5 Abs. 1 lit. c DSGVO

Datenverarbeitungssysteme haben sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Unsere IT-Lösungen kommen dieser Maßgabe folgendermaßen nach:

- comp.ASS und butler verlangen nur wenige Dateneingaben durch ihre Nutzer. Jeder Anwender entscheidet entsprechend den Organisationsrichtlinien und eigener Fachkenntnis, welche Daten zu erfassen sind. Unterstützt wird die Datenerfassung durch „Eingabemasken“, die sich auf relevante Angaben, die zur Erfüllung des Zwecks erforderlich und somit datenschutzrechtlich erlaubt sind, beschränken.
- Grundsätzlich befinden sich im „Büro“ des Anwenders (also im individuellen comp.ASS- oder butler-Arbeitsbereich) nur Personenakten, die der jeweilige Anwender aktiv aufgerufen hat. Außerdem findet jeder Nutzer in seinem butler- oder comp.ASS-Büro nur die "Maßnahmen" vor, für die er zuständig ist. In allen Auswahlfeldern (Rollbalken) sind zuerst nur die Personenakten sichtbar, die ein Anwender in seiner Aktennutzung hat. Weitere Personenakten muss der Nutzer zur Auswahl aktiv laden. Das bedeutet: Jeder sieht zunächst nur „seine“ Daten, d.h. Daten, die er selbst bearbeitet hat bzw. für die er zuständig ist.
- Die Archivierungsfunktion führt ebenfalls dazu, dass Daten sparsam angezeigt werden: Dokumente, Personenakten, Maßnahmen und andere Akten können archiviert werden und sind somit nur dann in den Rollbalken und Listen sichtbar, wenn dies inhaltlich erforderlich ist.

1.1.4 Richtigkeit

Artikel 5 Abs. 1 lit. d DSGVO,
(siehe auch Artikel 16 DSGVO „Recht auf Berichtigung“)

Unsere IT-Lösungen unterstützen Anwender – soweit möglich – Fehler bei der Datenerfassung zu vermeiden. Beispielsweise verfügen comp.ASS und butler über eine automatische und ausgeklügelte Dublettensuche. Das bedeutet, dass bei der Erfassung von Personendaten geprüft wird, ob bereits ein ähnlich lautender Datensatz hinterlegt ist. Wird die Dublettensuche fündig, zeigt das System den oder die gefundenen Namen an, damit der Anwender ggf. prüfen und entscheiden kann, ob es sich um die gleiche Person handelt. So kann vermieden werden, dass zu einer Person versehentlich mehrere Akten angelegt werden. Oft kann die Dublettensuche aber auch einfach einen Hinweis auf die Schreibweise von „schwierigen“ oder seltenen Namen geben, weil diese dem System schon bekannt sind.

Während Personennamen sehr individuell ausfallen können, gibt es andere Angaben wie z.B. bestimmte Aktenzeichen, deren Länge und Zusammensetzung eindeutigen Regeln unterliegen. Unsere IT-Systeme helfen hier mit Plausibilitätsprüfungen, Fehler bei der Eingabe zu vermeiden.

Generell liegt die Datenhoheit beim Anwender, der die Daten erfasst („Eigentümer“) und sie einfach (ggf. mit Korrekturprozessen) anpassen kann.

1.1.5 Speicherbegrenzung/Speicherform

Artikel 5 Abs. 1 lit. e DSGVO
(siehe auch Artikel 17 DSGVO „Recht auf Löschung“)

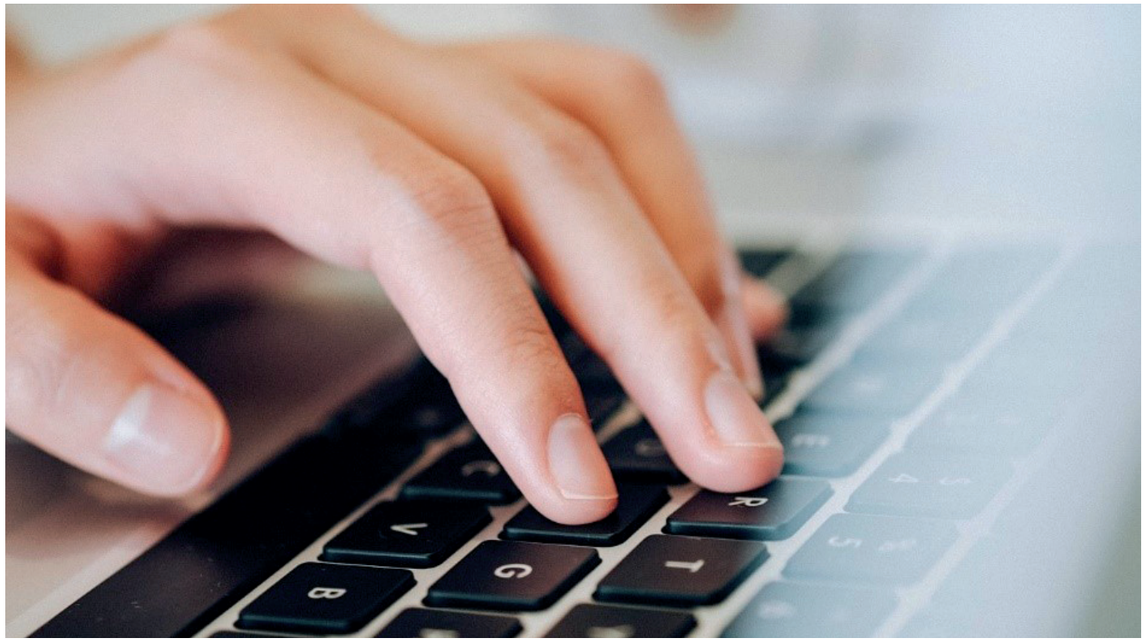
comp.ASS- und butler-Systeme werden für die Gewährung rechtlicher oder sozialer Unterstützung eingesetzt. Die Identifizierung der Betroffenen ist daher zu jeder Zeit notwendig. Ist die Unterstützung oder Begleitung beendet, so schreiben Aufbewahrungsfristen fest vor (z.B. 8 Jahre im SGB II-Bereich, 10 Jahre im Betreuungsbereich, in Ausnahmen auch länger), wie lange ein Zugriff auf die Akten möglich sein soll. Hierzu bieten butler und comp.ASS die Möglichkeit, solche Daten nur noch einem ausgewählten Kreis zugänglich zu machen, z.B. durch die Einrichtung eines eingeschränkten Leserechts bei einer Personenakte, einer Maßnahme-Akte oder einem Dokument. Zudem können verschiedene Archivierungs- oder Löschregelungen hinterlegt werden.

1.1.6 Integrität, Vertraulichkeit und Datensicherheit

Artikel 5 Abs. 1 lit. f DSGVO

Bei der Verarbeitung personenbezogener Daten ist nach Artikel 5 Abs. 1 lit. f DSGVO eine „angemessene Sicherheit“ und der „Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“ zu gewährleisten.

Bei der Arbeit mit unseren IT-Lösungen, besonders in größeren Organisationen, werden in Millisekunden neue Daten verarbeitet, erhoben, verändert, gespeichert. Aus diesem Grund sorgen wir mit erheblichem technischem und organisatorischem Einsatz dafür, dass die Systeme rund um die Uhr zur Verfügung stehen und ein Datenverlust möglichst auszuschließen ist. Für Szenarien, in denen mit einem unerwarteten technischen „Unfall“ kalkuliert wird, gibt es ein *Disaster-Recovery*-Konzept. Es werden also technische Maßnahmen sowohl in der Programmierung als auch der technischen Bereitstellung und der Sicherung, sowie dem Schutz vor falschen, unerlaubten Zugriffen getroffen und dazu korrespondierend organisatorische Maßnahmen (siehe Kapitel 3 „Technische und organisatorische Sicherheitsmaßnahmen“). Dabei werden Anpassungen entsprechend der technischen Entwicklung regelmäßig geprüft und entsprechend des Prüfergebnisses durchgeführt.



Als IT-Unternehmen sind wir in hohem Maße auf die Einhaltung der Prinzipien Integrität und Vertraulichkeit ausgerichtet und auf deren Sicherstellung in jedem Fall angewiesen. Diesem tragen wir auch Rechnung durch eine Organisation, in welcher die betroffenen Mitwirkenden und Abteilungen die Datensicherheit aus den jeweiligen Perspektiven betrachten und erforderliche Maßnahmen umsetzen. Aber auch die Kundenbetreuung, der Seminarbetrieb, unsere Reinigungskräfte und das Facility-Management sind konsequent im Sinne des Datenschutzes geschult und sensibilisiert.

1.2 Weitere datenschutzrechtliche Aspekte und deren Umsetzung bei prosozial

1.2.1 Auskunftsrecht

Artikel 15 DSGVO

In der Regel werden in comp.ASS-und butler-Systemen eine große Anzahl an Daten über einen langen Zeitraum verarbeitet, da die Betroffenen (z.B. Betreute, Langzeitarbeitslose) häufig über längere Zeit auf Unterstützung angewiesen sind. So entstehen, in Papier umgerechnet, mehrere Aktenordner an Daten unterschiedlichster Art. Mit unseren IT-Lösungen können Berichte erstellt werden, die in einer standardisierten Form die jeweiligen Stammdaten, Dokumentationsdaten und Maßnahme-Daten (welche meist die Zwecke der Verarbeitung darstellen) enthalten, um sie dem Betroffenen übergeben zu können.

1.2.2 Betrieblicher Datenschutzbeauftragter

Artikel 37 DSGVO und § 38 BDSG

In unserem Unternehmen ist ein betrieblicher Datenschutzbeauftragter gemäß Artikel 37 DSGVO und § 38 BDSG bestellt, dessen Position im gesetzlich vorgegebenen Umfang geschützt ist.

1.2.3 Das gesamte prosozial-Personal ist datenschutzverpflichtet

Die Beschäftigten, Auszubildenden, Praktikanten, usw. im Hause prosozial sind über den Datenschutz belehrt worden und haben eine Verpflichtungserklärung auf Vertraulichkeit über die Einhaltung des Datenschutzes unterzeichnet. Alle Bediensteten sind in Sachen Datenschutz sensibilisiert und geschult.

1.2.4 Die Datenschutz-Compliance ist in der prosozial-Firmenphilosophie verankert

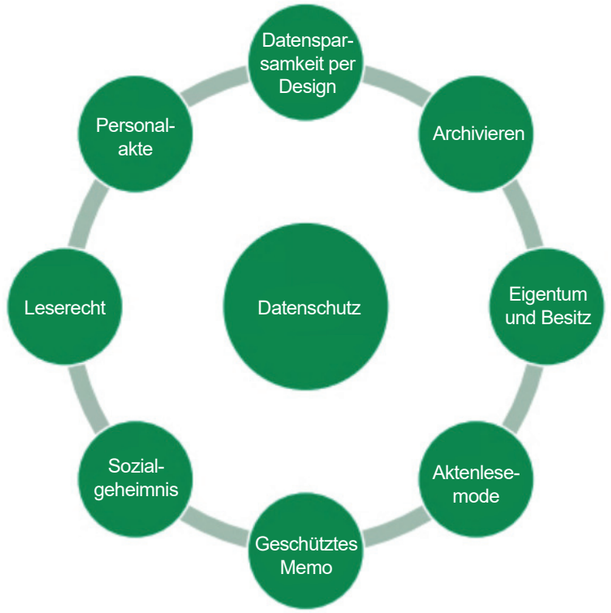
Die Sensibilität für die besonders hohen Sorgfaltspflichten bei der Auftragsdatenbearbeitung ist jedem Beschäftigten bei prosozial allein durch unsere Philosophie und Arbeitsweise, aber auch durch das Risiko und den hohen Schaden, der dem Unternehmen, seinem Image in dieser Branche zugefügt werden kann, voll bewusst. Denn: Sobald prosozial-Anwendungen im Einsatz sind, werden damit personenbezogene Daten aus dem besonders schutzwürdigen Sozial- und Bildungsbereich verarbeitet. Unsere Lösungen kommen an mehr als 20.000 Arbeitsplätzen in Deutschland, Österreich und Belgien zum Einsatz – bei öffentlichen Trägern, sozial-karitativen Einrichtungen und in Bildungsstätten, bei Berufsbetreuern, Betreuungsvereinen und in Betreuungsbehörden – und es werden täglich mehr. Dabei leisten wir betriebsalltäglich fachliche und technische Hotline-Unterstützung, erbringen vielfältige Leistungen an und um die Verarbeitung der Daten in unseren Datenbanksystemen beim Kunden und zunehmend auch in unserem Rechenzentrum.

1.2.5 Fallmanagement und Datenschutz

► **Besonderheiten des Fallmanagements**

In Jobcentern, Arbeitsagenturen, Jugendämtern, aber auch im Bereich der Eingliederungshilfe und im Betreuungsmanagement hat sich für die professionelle Fallarbeit das Handlungskonzept des Fall- oder Casemanagements durchgesetzt. Nach diesem Handlungskonzept ist es erforderlich, personenbezogene Daten aus vielen Lebensbereichen eines Menschen bei und mit dem Betroffenen zu erheben. Gesundheit, Wohnen, Finanzen, Qualifikation, Familie, Arbeit, Recht: Angaben zu all diesen Bereichen werden gespeichert und genutzt, um die jeweils am besten passende Hilfe für die betreffende Person zu erreichen. Diese "beste Hilfe" (die passende Stelle, Beratung, Betreuung, Einrichtung, Schule, Wohnung, Therapie, etc.) wird in der Betreuungsarbeit z.T. im Team von Experten ausgesucht. Dabei müssen ggfs. auch personenbezogene Daten von mehreren Experten genutzt werden.

► **Fallmanagement mit comp.ASS und butler**



comp.ASS und butler sind von Anbeginn ihrer Entwicklung an genau auf die Methoden des professionellen Fallmanagements hin ausgelegt worden. Mittlerweile sind sie z.T. auch in großen, komplexen Institutionen, Behörden oder Organisationen im Einsatz. Durch detailgetreue Abbildung der jeweiligen Organisation und ihrer Regeln, durch Zuordnung einzelner Nutzer zu Funktionsgruppen und durch bestimmte Aktenlesemodi bzw. durch Prozesse der Beantragung und Erteilung von Eigentums-, Besitz- oder Leserechten an Akten oder Dokumenten, kann die Organisation den Kreis der Nutzer für professionell bestimmte Zwecke begrenzen. Und zwar so zweck- und zielgenau begrenzen, dass bei der Realisierung der Zwecke **(Zweckbindungsgrundsatz)** dennoch die Nutzung der Daten eingeschränkt ist **(Trennungsgebot)**. Somit wird überhaupt erst möglich, ein der gesetzlichen Fürsorgeverpflichtung entsprechendes professionelles Fallmanagement durchzuführen, indem dabei zugleich auch die dem Datenschutz geschuldeten notwendigen Einschränkungen organisatorisch sichergestellt sind.

Unsere Software befreit die jeweilige Organisation also nicht von, sondern „befähigt“ sie zu organisatorischen Maßnahmen. Dabei ist auch ganz besonders wichtig, die Schulung der Nutzer im Datenschutz zu unterstützen. Die Implementierung von comp.ASS und butler beinhaltet daher immer auch eine Datenschutzschulung im Sinne einer Aufklärung darüber, welche „Datenschutztools“ durch und mit unserer Software für die gesamte Organisation, Fach- und Führungskräfte, Teams und natürlich für jeden einzelnen Nutzer entsprechend seiner Berechtigung bereitgestellt werden.

Aktenlesemode	Auswirkung
keine Berücksichtigung	Es wird kein Zugriff protokolliert (nicht empfohlen).
Akteneinsicht protokollieren	Es wird der Zugriff auf die **Personenakte** protokolliert.
Nur Akten mit Zuständigkeit öffnen	Der Nutzer kann nur seine zuständigen **Maßnahmen** und die dazugehörigen **Personenakten** direkt öffnen.
Akteneinsicht auf Nachfrage	Es wird vor dem Zugriff nachgefragt, ob der Nutzer auf diese **Personenakte** zugreifen will.
Personenakten- und Maßnahmeakteneinsicht auf Nachfrage	Er wird vor dem Zugriff nachgefragt, ob der Nutzer auf diese **Personenakte** oder diese **Maßnahme** zugreifen will.
Nur Akten mit Einsicht öffnen	Für den Zugriff auf die **Personenakte** muss der Nutzer entweder Eigentümer sein oder schon einen aktiven Aktenzugriff haben. Gewähren kann diesen der Eigentümer.
Nur Personenakten und Maßnahmeakten mit Einsicht öffnen	Für den Zugriff auf die **Personenakte** oder die **Maßnahme** muss der Nutzer entweder Eigentümer sein oder bereits einen aktiven Aktenzugriff haben. Gewähren kann diesen der Eigentümer. Zugriff auf die Personenakte gewährt auch Zugriff auf alle Maßnahmen der Personenakte.

Beispiel: Der Zugriff auf Personen- und Maßnahme-Akten kann durch den Aktenlesemodus gesteuert werden.

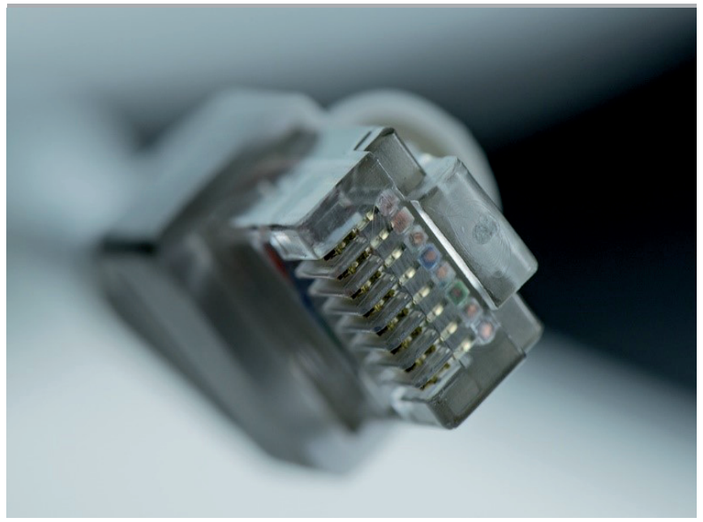
1.2.6 Hosting und Datenschutz

Artikel 28 DSGVO „Auftragsverarbeiter“

Es gibt verschiedene Arten des Hostings, bekannt und gebräuchlich sind z.B. Webhosting und E-Mail-Hosting. Grundsätzlich geht es beim Hosting darum, Datenspeicher, Software oder sogar Hardware über eine Internetverbindung von einem Hoster zu beziehen. Es bietet Geschäftsleuten, Privatpersonen und Behörden die Möglichkeit, diese Ressourcen äußerst flexibel dann und dort zu nutzen, wann und wo sie benötigt werden. Gleichzeitig bietet es die Möglichkeit, technische Sicherheit und fachliches technisches Know-how nicht selbst aufbauen und aktuell halten zu müssen, sondern vertraglich abgesichert einzukaufen. Unter dem Begriff „Cloud-Computing“ ist das obengenannte Geschäftsmodell stärker bekannt geworden. Es wird mittlerweile von vielen staatlichen Stellen genutzt und durch die Bundesregierung als Zukunftstechnologie einer modernen Wissensgesellschaft öffentlich gefördert (siehe auch die Kampagne *„Arbeiten 4.0“* des BMAS).

Content, Medien und Informationen sind Daten und gelten als „das Gold der Zukunft“. Aus Sicht der Datenschützer wurde Cloud-Computing in der Vergangenheit kritisch betrachtet, u.a. deshalb, weil Datenschutz grundsätzlich Sparsamkeit als Wert und besonders den Schutz personenbezogener Daten als Aufgabe lebt. Große Mengen an Daten, die via Internet als einem neuen öffentlichen Raum erreichbar sind, wirken da zunächst nicht gerade vertrauensbildend.

Die von prosozial angebotenen *Software-as-a-Service*-Dienstleistungen entsprechen fachlich und technisch konsequent den an Datenschutz und -sicherheit ausgerichteten Systemen. Die Freigaben, die unsere Systeme überall erhalten haben, zeigen den Erfolg dieses datenschutzkonformen Angebots. Der Artikel 28 DSGVO regelt, wie verantwortliche (öffentliche und nicht öffentliche) Stellen vorgehen müssen, wollen sie personenbezogene Daten im Auftrag durch andere Stellen verarbeiten lassen. Genau auf diese Auftragsverarbeitung sind unsere Softwarelösungen und das Kommunale Gebietsrechenzentrum (KGRZ) in Koblenz, in dem unser Rechenzentrum beheimatet ist, ausgelegt.



Die Regelung des Artikels 28 DSGVO taucht entsprechend auch für den Bereich der Sozialgesetzbücher im § 80 SGB X allgemein auf. Bei einer Auftragsdatenverarbeitung wird davon ausgegangen, dass die beauftragende öffentliche Stelle die komplette Verantwortung über ihre Daten behält. Aus diesem Grund hat sie mit dem Auftragnehmer (SaaS-Anbieter) die Fragen zu Datensicherheit und -schutz wie auch die Fragen zum Zugriff, zum Löschen und Sperren von Daten wie auch die Fragen zu weiteren Verfahrensweisen vertraglich verbindlich zu regeln. Für alle Träger des SGB II, die Bundesagentur für Arbeit (BA) und Kommunen bzw. Jobcenter gibt es hierzu im § 51 SGB II eine besondere Öffnungsnorm oder Ausnahmeregelung, die ausdrücklich die Beauftragung nichtöffentlicher Stellen abweichend von § 80 SGB X vorsieht.

Die prosozial GmbH hat seit Beginn des SaaS-Angebots im Jahr 2007 und schon in den Jahren zuvor bei Datenüberlassungen zu Testzwecken oder z.B. bei der Migration von Datenbeständen aus alten Verfahren nur unter Abschluss von **Vereinbarungen zur Auftragsverarbeitung** im Sinne des Artikel 28 DSGVO bzw. dem entsprechenden Landesgesetz gearbeitet. prosozial hat seitdem sein Know-how über den Betrieb eines modernen Rechenzentrums ständig ausgebaut. Wir sind überzeugt, dass wir damit unseren Kunden in Bezug auf alle Belange des Datenschutzes und der Datensicherheit ein sicheres, verlässliches und datenschutzkonformes Verfahren, welches in der Summe nicht nur leistungsfähiger, sondern auch wirtschaftlich günstiger als im Eigenbetrieb ist, anbieten können.

1.2.7 Weitere Aspekte zum Hosting im prosozial-Rechenzentrum

Im Hosting bei prosozial wird die gesamte Lösung im Rechenzentrum der prosozial GmbH in Koblenz betrieben. Die dort erhobenen Daten unterliegen den hohen Anforderungen zum Datenschutz nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz im Allgemeinen und zusätzlich den besonderen Bestimmungen zum Sozialdatenschutz.

Dem wird u. a. Rechnung getragen durch die folgenden Regelungen und Vorkehrungen:

- Zugriffe auf die Bereiche des Rechenzentrums sind umfassend reglementiert;
- Kameraüberwachung, insbesondere der besonders geschützten Bereiche und nach den regulären Geschäftszeiten der prosozial GmbH (Filmdateien werden ebenfalls im geschützten Bereich des Rechenzentrums gespeichert);
- Kein digitaler Wildwuchs: native Installationen, keine Risiken durch inkompatible Fremdsoftware, die das Risikomanagement unüberschaubar machen;
- Jede bei uns im Rechenzentrum gehostete Lösung ist „dedizierte Instanz“ und erhält eine eigenständige Umgebung mit einer eigenen Datenbank;
- Permanente Aktualisierung der Virenscanner;
- Monatliche, feste Update-Zyklen: Im Abgleich nach den Patch-Days von Microsoft halten wir unsere IT-Lösungen auf dem neuesten Stand;
- Exit-Strategie: Die Beendigung der Nutzung ist mit dem endgültigen Löschen der Daten von vorneherein technisch-organisatorisch und vertraglich abgesichert vorgesehen. So können Sie jederzeit auf eine datenschutzkonforme Exit-Strategie zurückgreifen;
- Im Verbund mit dem webbasierten Bürgerportal können beauftragte Dritte (z.B. Ehrenamtliche und Klienten) als zugelassene Nutzer per Registrierung innerhalb des geschützten CRM-Bereichs Daten, Dokumente und Nachrichten austauschen;
- Kommunikation nach außen: Sollen Daten, E-Mails, Dokumente den geschützten Bereich verlassen (z.B. SGB-II-Statistik, Sozialdatenabgleich, Trägerbeauftragung, eM@W, usw.), dann auf geschützten Wegen;
- Steigern sich Anforderungen, Gesetze und Technik, passen wir unsere Hosting-Systematiken an.

Darüber hinaus gelten die Datenschutz- und Sicherheitsmaßnahmen, die in Kapitel 3 „**Technische und organisatorische Sicherheitsmaßnahmen**“ und in Kapitel 1.1.6 **Integrität und Vertraulichkeit/ Datensicherheit** beschrieben sind.

1.3 Fazit: butler und comp.ASS sind DSGVO-konform – Voreinstellungen, Schulungen, Qualitätskontrollen

Artikel 25 DSGVO und Artikel 32 DSGVO

comp.ASS und butler sind DSGVO-konform designt. Sie unterstützen den Verantwortlichen und dessen Anwender bei der Aufgabe, nach Artikel 25 DSGVO ein System auszuwählen und so zu gestalten, dass die Prinzipien des Datenschutzes eingehalten werden können.

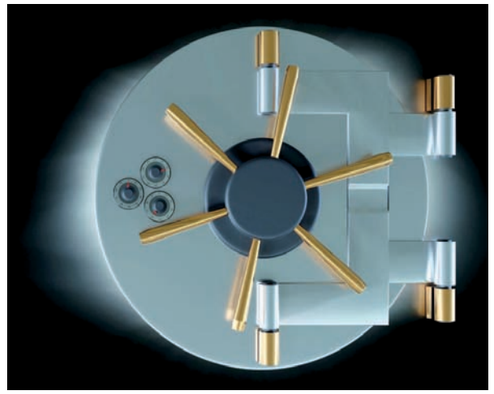
Datenschutz-Beratung und Datenschutz-Schulungen runden den Service der prosozial GmbH ab, sodass auch den Forderungen des Artikels 32 DSGVO entsprochen werden kann. Durch den Betrieb im Rechenzentrum in Deutschland, die regelmäßige Anpassung an den Stand der Technik, sowie die Überprüfung der technischen und organisatorischen Maßnahmen mit einem Team von IT- und Datenschutzexperten wird der Datenschutz einer ständigen Qualitätskontrolle unterzogen und damit sichergestellt.

„Von Grund auf datenschutzkonform – unsere Lösungen halten, was sich datensensible Kunden wie Kommunen und Behörden von ihnen versprechen. Und das seit über 20 Jahren.“

Christoph Spitzley, in der Geschäftsführung verantwortlich für den Datenschutz der prosozial GmbH

2. Technische und organisatorische Sicherheitsmaßnahmen

Folgende technische und organisatorische Maßnahmen gelten im Bereich des Serverbetriebs im Kommunalen Gebietsrechenzentrum Koblenz (KGRZ).



2.1 Zutrittskontrolle (Vertraulichkeit)

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Das Gebäude ist durch ein Schließsystem gesichert, wird bewacht und überwacht. Der Standort ist nicht allgemein bekannt.
- Der Zutritt zum Gebäude und dem Serverraum ist rund um die Uhr (24/7), aber nur nach Voranmeldung beim Betreiber möglich. Der Zutritt zum Rechenzentrum wird mittels eines Personalausweises verifiziert und protokolliert.
- Nur autorisierte Mitarbeiter der Abteilung „IT operativ“ haben nur nach schriftlicher Ermächtigung durch den IT-Leiter gegenüber dem Betreiber und einer Anmeldung beim Betreiber Zutritt.
- Unternehmensfremde Besucher und Lieferanten sind nicht vorgesehen. Eine Inspektion gemäß Artikel 28 Abs. 3 (h) DSGVO ist aber nach Absprache möglich.
- Das Gebäude ist in unterschiedliche Sicherheitszonen mit Schleusen aufgegliedert.
- Innerhalb des Rechenzentrums und der Serverräume erfolgt eine 24/7-Videoaufzeichnung.

2.2 Zugangskontrolle (Vertraulichkeit, Integrität)

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Der Zugang zu den Systemen ist durch entsprechende zentrale Firewallsysteme geschützt.
- Der Zugang zu den Systemen ist nur auf autorisierte Mitarbeiter/innen begrenzt. Das Management der Zugriffsberechtigungen erfolgt über das firmeneigene Dokumentationssystem und hier hinterlegte Organisationsvorschriften.
- Für die Verwaltungsaufgaben steht das Modell „Mobile Workplace“ zur Verfügung. Dabei können sich Administratoren und sonstige Berechtigte auf speziellen Servern mit ihrem individuellen Desktop anmelden. Erst von da aus erreichen sie, nach entsprechender Freigabe, die zu verwaltenden Server.

- Ebenso wird mit Fernwartungsverbindungen verfahren. Die Mitarbeiter verbinden sich, nach vorheriger Freigabe, zunächst mit speziellen Fernwartungssprungservern (Sprungserver) und erst von da aus mit den betreuten Systemen der Kunden. Es wird also sichergestellt, dass nur berechtigte Mitarbeiter Zugriff erhalten und Mitarbeitercomputer niemals direkten Kontakt zu betriebsrelevanter Infrastruktur haben.
- Alle Computer-Systeme bei prosozial sind durch hinreichend sichere Passwörter geschützt. Passwortlose Systeme sind gemäß Dienstanweisung nicht zulässig.
- Beim Verlassen des Computers ist dieser laut Dienstanweisung zu sperren.
- Ein Überlassen des eigenen Computers an Andere, mit Ausnahme der Firmen-Administratoren, ist nicht gestattet.

2.3 Zugriffskontrolle (Vertraulichkeit, Integrität, Verfügbarkeit)

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Eine Zugriffskontrolle wird durch die Infrastruktur erzwungen und ist von den Mitarbeitern nicht beeinflussbar.
- Der Zugriff erfordert einen Benutzernamen und ein Kennwort, für das eine Passwortrichtlinie gilt. Der Zugriff ist jeweils personalisiert. Ein Überlassen eigener Zugangsdaten an Andere ist nicht gestattet.
- Alle Mitarbeiter/innen der prosozial GmbH haben nur für ihre Zwecke eingerichtete Benutzerberechtigungen, die von den verantwortlichen Bereichsleitern oder Geschäftsführern festgelegt und freigegeben werden müssen.
- Der Zugriff auf das Rechenzentrum unterliegt ausschließlich autorisierten Mitarbeiter/innen.
- Der Zugang zu den Systemumgebungen (Programmanmeldung) ist technisch durch Einrichtung von Benutzernamen und Kennwörtern gesichert.
- Der Zugriff auf die Systemumgebungen (Programmanmeldung) ist zweistufig durch eine Anmeldung am Rechenzentrum (1) und Anmeldung auf der Kundendatenbank (2) geschützt.
- Die Passwörter der Systemumgebungen (Programmanmeldung) werden in einem eigenem Passwortverfahren mit Passwortrichtlinie erstellt und aufbewahrt. Der Zugriff ist auf autorisierte Mitarbeiter/innen beschränkt.
- Zugriff auf die Datenbank des Auftraggebers haben ausschließlich autorisierte Mitarbeiter/innen der IT-Abteilung zum Zwecke der Wartung und Fehlerbehebung.
- Zugriff auf die Anwendung des Kunden haben ausschließlich die Kundenberater mit personalisierten Zugangsdaten für vom Auftraggeber autorisierte Dienstleistungen (z.B. Second-Level-Support, Büroservice, Fehlerbehebungen, Konfiguration).
- Löschungen im Auftrag des Kunden während des Vertragsverhältnisses werden dokumentiert und im Vier-Augen-Prinzip (innerhalb prosozial) durchgeführt.

2.4 Offenlegung (Vertraulichkeit, Integrität, Verfügbarkeit)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft bzw. festgestellt werden kann, an welchen Stellen eine Offenlegung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Alle Mitarbeiter werden routinemäßig auf Datenschutz und Verschwiegenheit verpflichtet.
- Die Festplatten aller Mitarbeitercomputer sind nach Stand der Technik verschlüsselt.
- Die Datensicherungen werden durchgehend nach Stand der Technik verschlüsselt.
- Die Transportwege zum Rechenzentrum und zur Anwendung sind grundsätzlich und nach Stand der Technik verschlüsselt (https, RDP).
- Bei Fehlerbehebungsaufträgen werden die Daten ausschließlich zu Testzwecken in den EDV-Systemen der prosozial GmbH zurückgesichert, die wiederum dem oben beschriebenen Zutrittskontroll-, Zugangskontroll- und Zugriffskontrollsystem unterliegen.
- Der Einsatz mobiler Datenträger wie z.B. USB-Stick, CD-Rom etc. ist nicht vorgesehen und nicht erlaubt. Verlangt der Auftraggeber die Ausgabe per Datenträger, dann geschieht dies ausschließlich verschlüsselt mit Kennwort oder per verschlüsseltem Datentransport an eine von ihm benannte autorisierte Person.
- Wir leben das „papierarme Büro“, was bedeutet, dass 98 % der eingehenden „analogen“ Post zentral gesichtet, gescannt, zugeordnet und mit Leseberechtigungen im System weitergeleitet werden. Der größte Anteil der Post wird digital zugestellt und automatisiert den Empfängern zugestellt werden. Die Mitarbeiter im Homeoffice bekommen keine Papierunterlagen und damit keine personenbezogenen Daten in physischer Form.
- Papierdaten werden mit zertifiziertem Aktenvernichter DIN 66399 entsorgt.
- Datenträger werden von einem zertifizierten Entsorger nach DIN 66399 entsorgt.

2.5 Eingabekontrolle (Integrität)

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Eine Eingabekontrolle wird durch die Infrastruktur und die standardisierten Workflows erzwungen und ist von den Mitarbeitern nicht beeinflussbar.
- Änderungen an Datenobjekten (Entitäten), bzw. Zugriffe auf Datenobjekte (Entitäten) werden protokolliert (Transparenzprinzip, Änderungslogs, Dokumentenversionierung).
- Dienstanweisungen werden revisionssicher archiviert.
- Die Logdateien sind gesichert und können durch den Anwender nicht gelöscht werden.
- Die Zugriffe auf das Rechenzentrum werden nachvollziehbar mitgeloggt.
- Datenempfang und Datenversand werden schriftlich dokumentiert.
- Änderungen werden im Kundensystem mit Nutzernamen – nicht löschbar – protokolliert.
- Zugriffe auf Datenbanken und schreibende Zugriffe auf Datenobjekte (Entitäten) werden mitprotokolliert.
- Das Löschen von Daten nach Kündigung des Hauptvertrages ist vertraglich geregelt, Daten werden standardmäßig 90 Tage nach Beendigung des Hauptvertrages, wenn nichts anderes schriftlich vereinbart ist, im Vier-Augen-Prinzip gelöscht. Die Löschung wird dokumentiert.

2.6 Auftragskontrolle (Vertraulichkeit, Verfügbarkeit)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

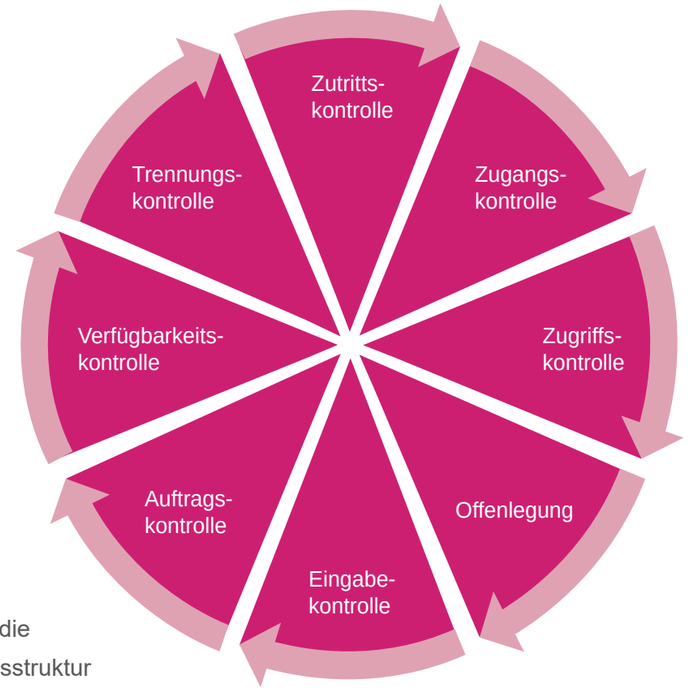
- Die Auftragskontrolle wird durch die Organisationsstruktur erzwungen und ist von den Mitarbeitern nicht beeinflussbar.
- Der Gegenstand des Auftrages wird in einer Vereinbarung schriftlich festgehalten.
- Die berechtigten Weisungsgeber und -empfänger werden im Dokumentationssystem des Auftragnehmers hinterlegt.
- Bei Löschaufträgen muss ein schriftlicher Auftrag des Kunden mit genauer Beschreibung vorliegen. Die Löschung wird dokumentiert.
- Insbesondere das Löschen durch den Auftragnehmer der Daten erfolgt ausschließlich auf Weisung des Auftraggebers. Soweit eine Löschung der Daten technisch nicht möglich bzw. der Aufwand im Verhältnis zum angestrebten Schutzzweck zu hoch ist, werden die Daten gesperrt.
- Die Löschung der Daten nach Herausgabe an den Auftraggeber erfolgt entsprechend den in der Systembeschreibung definierten Sicherheitsintervallen, bzw. bei Virenbefall entsprechend den in der Systembeschreibung definierten Ausnahmen.
- Es existiert eine Liste der zur Nutzung freigegebenen und auch untersagten Software. Der Einsatz nicht freigegebener Software wird sanktioniert. Vor dem Einsatz neuer Software ist eine Freigabe durch die IT-Abteilung zwingend vorgeschrieben.

2.7 Verfügbarkeitskontrolle (Verfügbarkeit, Wiederherstellung der Verfügbarkeit)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Das Rechenzentrum (KGRZ) ist in TSI-Verfügbarkeitsklasse 3 bzw. TIER 3 eingestuft.
- Die Infrastruktur wird permanent mit entsprechenden Monitoringsystemen überwacht. Überwacht wird auch, ob es zum Eintritt eines Brandes, Ausfall der Raumklimatisierung, Stromausfall etc. kommt.
- Die IT-Systeme werden mit Hilfe der *Windows Server Update Services (WSUS)* aktuell gehalten.
- Alle Computersysteme sind durch eine aktuelle Antivirensoftware geschützt. Ein Abschalten dieser ist nicht erlaubt und wird, wo möglich, technisch unterbunden.
- Die Datenbanken und Dateien der Kunden werden mindestens einmal täglich vollständig gesichert. Änderungen der relevanten Datenbanken werden alle 10-15 Minuten durch Transaktionslogs gesichert.
- Die für die Datensicherung nötige Hardware befindet sich immer in einem anderen Brandabschnitt des Gebäudes, um auch im Brandfall die Existenz eines Backups zu garantieren.
- Täglich werden sämtliche Daten verschlüsselt auf Backupservern abgelegt. Die Tagessicherungen werden für 31 Tage gehalten. Sollte aufgrund eines unvorhersehbaren Fehlers ein Datenverlust auftreten, kann so schnellstmöglich ein aktueller und konsistenter Datenstand wiederhergestellt werden.

- Am Ende eines Monats wird ein kompletter Datensatz auf Bandlaufwerke geschrieben. Diese werden extern aufbewahrt, um auch im Falle eines Verlustes des kompletten Gebäudes eine Wiederherstellung der Daten zu gewährleisten. Diese Monatssicherungen werden für mindestens 1 Jahr vorgehalten.
- Datenwiederherstellungen werden regelmäßig getestet.
- Ein Ausfall der Techniksysteme wird durch redundante Strukturen abgefangen.
- Gegen Stromausfälle schützt eine zentrale und redundante USV-Anlage. Für längere Stromausfälle stehen lokale Stromgeneratoren bereit.
- Die technischen Systeme im Gebäude sind in verschiedene Brandabschnitte aufgeteilt, um das Risiko eines Totalausfalls zu minimieren. Im Serverraum herrscht eine sauerstoffreduzierte Atmosphäre.
- Durch die im Clientcomputerkonzept beschriebenen Maßnahmen wird sichergestellt, dass ein Ausfall der Mitarbeitercomputer keinerlei Auswirkungen auf den Geschäftsbetrieb hat.



2.8 Trennungskontrolle (Vertraulichkeit, Integrität)

Maßnahmen, die sicherstellen, dass Daten entsprechend ihrem Zweck und den zugeordneten Berechtigungen verarbeitet werden:

- Die Trennungskontrolle wird durch die Infrastruktur und/oder Organisationsstruktur erzwungen und ist von den Mitarbeitern nicht beeinflussbar.
- Es existiert ein Berechtigungskonzept, welches die notwendigen Benutzergruppen und ihre Zugriffsberechtigungen beschreibt. Darin werden auch der Einsatzbereich und die Aufgaben des jeweiligen Mitarbeiters berücksichtigt.
- Die Vergabe von Zugriffs- und Zugangsrechten werden organisatorisch geregelt und technisch abgesichert.
- Die Vergabe von Rechten für die Mitarbeiter/innen des Auftragnehmers wird im Detail in der Verwaltungssoftware dokumentiert und gesteuert.
- Die Kundendatenbanken im Rechenzentrum sind technisch und logisch getrennt von den Daten der prosozial GmbH und denen der anderen Kunden.
- Die einzelnen IT-Infrastrukturgruppen werden durch VLANs sicher separiert und die Separierung durch Firewalls überwacht.

3. Vielfach zertifiziert und anerkannt: Freigaben, Auszeichnungen und Befähigungsnachweise

3.1 Informationstechnologie

► **Citrix Partner Silver**

prosozial erlangte bereits wenige Jahre nach der Firmengründung 1995 das Zertifikat im Status eines GOLD-Partners. Dies ist die höchste Stufe der Zertifizierung, die ein Unternehmen bei Microsoft erreichen kann, und damit ein Ausweis für das höchste Maß an Expertise, Kompetenz und Aktualität, das man in diesem Bereich erwarten kann. Unsere Mitarbeiter beweisen immer wieder neu durch ihre in persönlichen Prüfungen erlangten Zertifikate und Befähigungsnachweise, dass die bei uns und unseren Kunden eingesetzten IT-Systeme und Architekturen den höchsten Anforderungen moderner IT-Technologie standhalten. Darüber hinaus ist prosozial seit vielen Jahren Citrix-Partner, genauer gesagt **Citrix Partner Silver: Solution Advisor.**

► **TSI.Professional nach TÜV-Prüfung**

Unser langjähriger Rechenzentrumsleiter Holger Schmidt, der den Auf- und Ausbau des prosozial-Rechenzentrums von Anfang an maßgeblich gestaltet hat, ist einer von wenigen, handverlesenen Experten, die der TÜV Informationstechnik *(TÜViT)* als TSI. Professional ausweist (*www.tuvit.de*). Um den TSI. Professional-Status zu erwerben, hat er diverse Anforderungen erfüllt und u.a. den Ausbildungspfad zum *Data Center Specialist* bei der DCE acadamy absolviert. TSI steht hier für *Trusted Site Infrastructure* und bezeichnet einen Kriterienkatalog zur Prüfung hochverfügbarer IT-Infrastrukturen, der die europäische Norm EN 50600 abdeckt.


CERTIFICATE
OF COMPLETION 2018

Hiermit wird bestätigt, dass

Holger Schmidt
prosozial GmbH

den DCE academy Ausbildungspfad

Data Center Specialist

erfolgreich abgeschlossen hat.

Der Ausbildungspfad beinhaltete folgende Seminare:
Planen und Auditieren eines Rechenzentrums nach EN 50600 & TSI.STANDARD des TÜViT
DEEP DIVE - Energieversorgung & Klimatisierung nach EN 50600
Data Center Operations - Professional

Frankfurt am Main, 20.08.2018

Thomas Wawra
CEO DCE academy

Certificate DCE-18-A1-00-04

www.dce-academy.com

► **BA-zertifizierter eM@w-Provider**

prosozial ist seit 2006 ein bei der Bundesagentur für Arbeit (BA) akkreditierter Provider. Als solcher sind wir befugt, besonders schutzwürdige personen- und maßnahmebezogene Sozialdaten im vom Bundesdatenschutzbeauftragten freigegebenen elektronischen Maßnahmeabwicklungs-Verfahren **eM@w** zu verarbeiten und zwischen Trägern und Bundesagentur auszutauschen. Insbesondere, wenn Kunden nicht nur unsere Software sondern auch unsere Möglichkeit des Hostings nutzen, verbleiben die Daten nach der gesicherten Weitergabe durch die BA an uns als Provider allein im Koblenzer Rechenzentrum. Aufnahme, Weitergabe und Bereitstellung der Daten finden ausschließlich hinter den schützenden Mauern der Firewall und den organisatorischen und technischen Maßnahmen der Zugangs-, Zutritts- und Zugriffskontrolle statt. Das Vorhandensein von Daten außerhalb der Firewalls auf dem Weg zwischen geschützten Hoheiten wird so auf das absolute Minimum reduziert. Mehr Schutz geht nicht! Weiteres zu diesem äußerst anspruchsvollen Verfahren finden Sie unter *www.arbeitsagentur.de*.

► **XSozial-Datenmeldung (§ 51b SGB II)**

prosozial ist seit 2004 vom Deutschen Landkreistag berufenes Mitglied im gemeinsamen §-51b-Statistik-Unterausschuss mit der Bundesagentur für Arbeit. Der zugrundeliegende Gesetzesparagraph (§ 51b SGB II) regelt die Erhebung und Verarbeitung von Daten durch Träger der Grundsicherung und legt fest, dass die zuständigen kommunalen Träger entsprechende Datensätze an die Statistik der Bundesagentur übermitteln. Das dazu vereinbarte Datenmelde- und Austauschschema **XSozial**, Teil des **XÖV** (Standard für den elektronischen Datenaustausch der öffentlichen Verwaltung), wurde unter Beteiligung von prosozial entwickelt und weiterentwickelt.

Seit 2005 erzeugen und versenden kommunale Träger in einem vom Bundesdatenschutzbeauftragten freigegebenen Verfahren zertifiziert mit unserer Client-Server-Anwendung comp.ASS diesen vermutlich größten Sozialdatensatz in Deutschland. Und das Monat für Monat. Auswertungen zur Güte und Qualität der Daten haben alle Kunden von prosozial nachweislich in die obersten Rangplätze bei Datenqualitätsauswertungen gebracht.

Die mit der §-51b-Statistik verbundene Migrationshintergrunderhebung im Auftrag des Bundesministeriums des Inneren (BMI), eine auch vom Bundesbeauftragten für den Datenschutz freigegebene Erhebung mit sehr speziellen Melde- und Löschvorschriften, wurde ebenfalls in unseren comp.ASS-Systemen bei den SGB II-Trägern vor Ort erfolgreich implementiert.

3.2 Forschung und Wissenschaft

► **Forschung im Auftrag des Bundes – prosozial als Partner bei sensiblen Datenerhebungen im Rahmen von Sozialforschung und Wissenschaft**

Neben den Aufgaben als Hersteller einer Standardsoftware für den Sozialbereich haben wir uns seit vielen Jahren immer wieder an Forschungsprojekten zur Weiterentwicklung und Evaluation neuer sozialer (Dienst-) Leistungen beteiligt. Dabei kam uns der Part der Erhebung, Speicherung, Aufbereitung sowie Auswertung von Sozialdaten zu.

Hier seien u.a. die Modellprojekte des **Bundesministeriums für Arbeit und Soziales (BMAS)** zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe (MoZArT) und der Pauschalierung der Sozialhilfe nach § 101a BSHG (PASO) wie auch das Projekt „Sozialagenturen“ des Düsseldorfer Ministeriums für Arbeit, Soziales, Qualifizierung und Technik (MASQT) genannt.

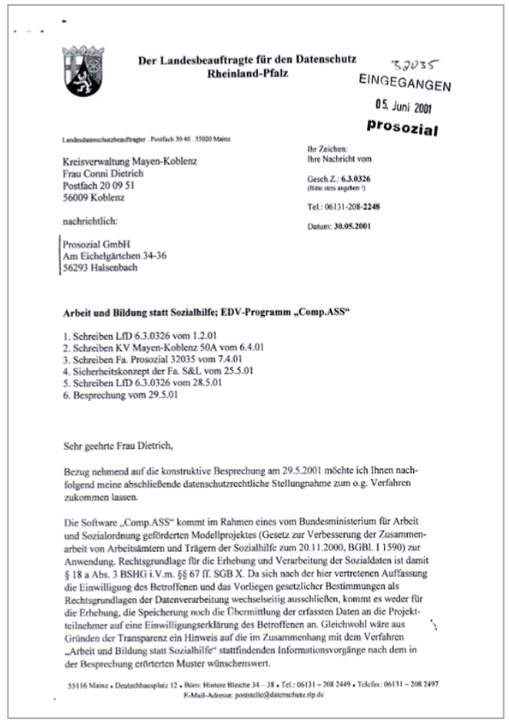
Im Auftrag des **Bundesministeriums der Justiz** und des Instituts für Sozialforschung und Gesellschaftspolitik Köln (ISG) haben wir 2016 eine Erhebung von Geschäftsdaten von Berufsbetreuern entwickelt und umgesetzt. Auch hier waren unsere Konzepte der Erhebung, Sicherung und Verarbeitung von Sozialdaten stets konform zu den hohen Anforderungen der Sozialgesetzbücher (SGB) und des Bundesdatenschutzgesetzes (BDSG) ausgestaltet.

3.3 Landesfreigaben

► **Rheinland-Pfalz:**

Freigabe von comp.ASS durch den Landesbeauftragten für den Datenschutz

Im Zuge des MoZArT-Projektes wurde unsere dort zum Einsatz kommende Software comp.ASS 2001 von der rheinland-pfälzischen Landesdatenschutzbehörde geprüft und als unbedenklich („... *keine datenschutzrechtlichen Bedenken*...“) freigegeben.



Der Landesbeauftragte für den Datenschutz
Rheinland-Pfalz

EINGEGANGEN
05. Juni 2001
Prosozial

Landesdatenschutzbeauftragter · Postfach 30 40 · 55020 Mainz

Kreisverwaltung Mayen-Koblenz
Frau Conni Dietrich
Postfach 20 09 51
56009 Koblenz

nachrichtlich:

Prosozial GmbH
Am Eichelgärtchen 34-36
56293 Halsenbach

Ihr Zeichen:
Ihre Nachricht vom

Gesch.Z.: 6.3.0326
(Bitte stets angeben !)

Tel.: 06131-208-2248

Datum: 30.05.2001

Arbeit und Bildung statt Sozialhilfe; EDV-Programm „Comp.ASS“

1. Schreiben LfD 6.3.0326 vom 1.2.01
2. Schreiben KV Mayen-Koblenz 50A vom 6.4.01
3. Schreiben Fa. Prosozial 32035 vom 7.4.01
4. Sicherheitskonzept der Fa. S&L vom 25.5.01
5. Schreiben LfD 6.3.0326 vom 28.5.01
6. Besprechung vom 29.5.01

Sehr geehrte Frau Dietrich,

Bezug nehmend auf die konstruktive Besprechung am 29.5.2001 möchte ich Ihnen nachfolgend meine abschließende datenschutzrechtliche Stellungnahme zum o.g. Verfahren zukommen lassen.

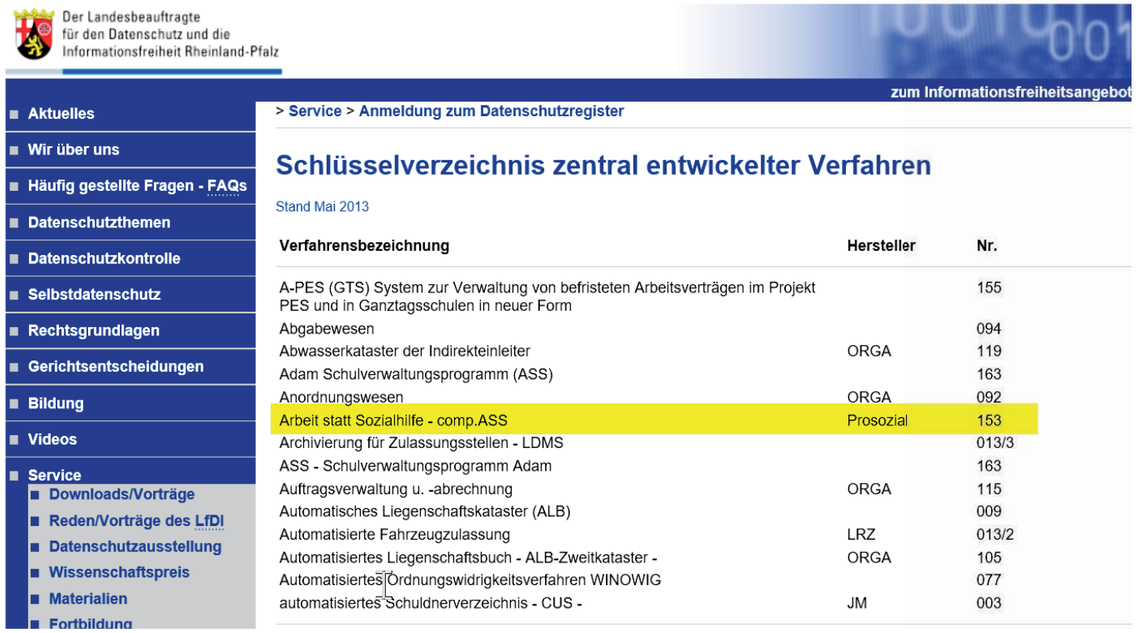
Die Software „Comp.ASS“ kommt im Rahmen eines vom Bundesministerium für Arbeit und Sozialordnung geförderten Modellprojektes (Gesetz zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe zum 20.11.2000, BGBl. I 1590) zur Anwendung. Rechtsgrundlage für die Erhebung und Verarbeitung der Sozialdaten ist damit § 18 a Abs. 3 BSHG i.V.m. §§ 67 ff. SGB X. Da sich nach der hier vertretenen Auffassung die Einwilligung des Betroffenen und das Vorliegen gesetzlicher Bestimmungen als Rechtsgrundlagen der Datenverarbeitung wechselseitig ausschließen, kommt es weder für die Erhebung, die Speicherung noch die Übermittlung der erfassten Daten an die Projektteilnehmer auf eine Einwilligungserklärung des Betroffenen an. Gleichwohl wäre aus Gründen der Transparenz ein Hinweis auf die im Zusammenhang mit dem Verfahren „Arbeit und Bildung statt Sozialhilfe“ stattfindenden Informationsvorgänge nach dem in der Besprechung erörterten Muster wünschenswert.

55116 Mainz • Deutschhausplatz 12 • Büro: Hintere Bleiche 34 - 38 • Tel.: 06131 – 208 2449 • Telefax: 06131 – 208 2497
E-Mail-Adresse: poststelle@datenschutz.rlp.de

► **Hessen:**

Verfahrensverzeichnis anerkannt vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit

Seit Anfang 2018 wird comp.ASS 21 vom Amt für Jugend und Integration einer Stadt im Vortaunus als Software für die Flüchtlingshilfe eingesetzt. Zuvor wurde das Verfahrensverzeichnis nach § 6 HDSG geprüft und anerkannt.



Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

zum Informationsfreiheitsangebot

- Aktuelles
- Wir über uns
- Häufig gestellte Fragen - FAQs
- Datenschutzthemen
- Datenschutzkontrolle
- Selbstdatenschutz
- Rechtsgrundlagen
- Gerichtsentscheidungen
- Bildung
- Videos
- Service
  - Downloads/Vorträge
  - Reden/Vorträge des LfDI
  - Datenschutzausstellung
  - Wissenschaftspreis
  - Materialien
  - Fortbildung

> Service > Anmeldung zum Datenschutzregister

Schlüsselverzeichnis zentral entwickelter Verfahren

Stand Mai 2013

Verfahrensbezeichnung	Hersteller	Nr.
A-PES (GTS) System zur Verwaltung von befristeten Arbeitsverträgen im Projekt PES und in Ganztagsschulen in neuer Form		155
Abgabewesen		094
Abwasserkataster der Indirekteinleiter	ORGA	119
Adam Schulverwaltungsprogramm (ASS)		163
Anordnungswesen	ORGA	092
Arbeit statt Sozialhilfe - comp.ASS	Prosozial	153
Archivierung für Zulassungsstellen - LDMS		013/3
ASS - Schulverwaltungsprogramm Adam		163
Auftragsverwaltung u. -abrechnung	ORGA	115
Automatisches Liegenschaftskataster (ALB)		009
Automatisierte Fahrzeugzulassung	LRZ	013/2
Automatisiertes Liegenschaftsbuch - ALB-Zweitkataster -	ORGA	105
Automatisiertes Ordnungswidrigkeitsverfahren WINOWIG		077
automatisiertes Schuldnerverzeichnis - CUS -	JM	003

► **Sachsen:**

Offizielle Verfahrensbeschreibung und Aufnahme ins Sächsische Verzeichnis nach § 10 SächsDSG

2013 wird comp.ASS vom Landkreis Görlitz dem Sächsischen Datenschutzbeauftragten vorgestellt und offiziell ins Sächsische Register der beschriebenen und überprüften Verfahren aufgenommen.

► **Mecklenburg-Vorpommern:**

Offizielle Verfahrensbeschreibung und Aufnahme ins Verfahrensverzeichnis (Mitteilung und Beschreibung der Verfahren nach § 18 DSGM-V für das Register beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern)

Auf Antrag des Landkreises Vorpommern-Rügen wird comp.ASS als Lösung für den Landkreis als SGB II-Träger nach dem Landesdatenschutzgesetz registriert. – Und zwar ohne Beanstandungen.

► **prosozial-Lösungen auch im Ausland im Einsatz**

IT-Lösungen von prosozial werden nicht nur im Bundesgebiet, sondern auch über dessen Grenzen hinaus genutzt. Beispielsweise hat sich das Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens 2004 für den Einsatz von comp.ASS entschieden. Auch die Pflegestützpunkte des österreichischen Bundeslandes Vorarlberg arbeiten mit comp.ASS und hosten ihre Lösung in unserem Rechenzentrum in Koblenz.

3.4 Zu guter Letzt: Nur Positiv-, keine Negativanzeigen. Kein Verstoß gegen den Datenschutz!

Ein gemäß den Datenschutzbestimmungen des Bundes und der 16 Bundesländer anzeigepflichtiges Ereignis im Zusammenhang mit unserem Unternehmen, seinen Leistungen und Produkten hat es bis zum heutigen Tag nicht gegeben. Wenn eine Freigabe, ein Aufnahme- und Registrierungsverfahren von unseren Kunden für und mit unseren Lösungen angestrebt wurde, war es immer erfolgreich.

Zu jeder Zeit haben wir uns mit unserer Software und mit den empfohlenen Installationen und Architekturen sowohl bei Kunden vor Ort als auch im Rechenzentrum Koblenz am Konzept des BSI-Grundschutzes, seinen *Goldenen Regeln* sowie weiterführenden Reglements orientiert.

Nie wurde einer unserer Lösungen die Freigabe durch den zuständigen Datenschutz verwehrt, der Betrieb einer Anwendung untersagt oder sonst eine mangelnde Datenschutzkonformität unterstellt. Bislang haben all unsere Produkte, Lösungen und Betriebsarchitekturen den hohen Anforderungen des Datenschutzes standgehalten. Die Sicherheit und der Schutz personenbezogener Sozialdaten wird von Anbeginn der prosozial GmbH an als ständige und bleibende Aufgabe von uns gelebt.

„Wir halten uns an die Erfüllung der Grundsätze und Regeln des BSI-Grundschutzes. Heute ebenso wie morgen!“

Wolfgang Hoffmann und Stephan Idel,
geschäftsführende Gesellschafter der prosozial GmbH

3.5 Starke Partnerschaften für Ihre Sicherheit

In puncto IT- und Datensicherheit geht prosozial keine Kompromisse ein, sondern vielmehr starke Partnerschaften, um gemeinsam noch besser gegen heutige und künftige Gefahren gewappnet zu sein. Zum Beispiel gegen die zunehmende Gefahr der Hackerangriffe. Hier lassen wir von eigens beauftragten Experten für Cyber-Sicherheit regelmäßig sogenannte **Penetrationstests** durchführen, um potenzielle Sicherheitslücken oder Designschwachpunkte frühzeitig zu erkennen.

Darüber hinaus arbeiten wir partnerschaftlich mit einem der weltweit führenden Anbieter von Vulnerability-Management-Lösungen zusammen, praktizieren ein entsprechendes **Schwachstellenmanagement** und führen entsprechende Tests durch. Eine Dienstleistung, die wir übrigens auch unseren Kunden anbieten.

Last, but not least ist prosozial Mitglied der **Allianz für Cyber-Sicherheit**, was uns einen frühzeitigen und exklusiven Zugang zu sicherheitsrelevanten Informationen verschafft. Das Netzwerk wurde 2012 unter der Schirmherrschaft des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gegründet und macht es sich zur Aufgabe, die digitale Sicherheit am Wirtschaftsstandort Deutschland zu stärken und weiterzuentwickeln.

Bildquellenangaben
Fotos und Grafiken: pixabay.com; fotolia.com; Bundesagentur für Arbeit; prosozial GmbH

Impressum:

prosozial GmbH
Emser Straße 10
56076 Koblenz

Telefon: 0261 201615-500
Telefax: 0261 2016180-501

Vertretungsberechtigte Geschäftsführer:
Wolfgang Hoffmann, Stephan Idel, Christoph Spitzley

Registergericht: Koblenz
HR: 5796

Ansprechpartner:
Christoph Spitzley
datenschutz@prosozial.de

Ein Service von prosozial GmbH