



prosozial GmbH

Wie erfüllt prosozial den

Datenschutz?

Freigaben, Ausweise, Belege und Befähigungsnachweise der prosozial GmbH

Datenschutzkonformität der Lösungen
comp.ASS 21 und butler 21

Technische und organisatorische (Sicherheits-)
Maßnahmen

INHALT	3
	4
(K)ein kleines ABC des Datenschutzes bei prosozial.....	4
1. A wie anerkannt: Freigaben, Ausweise, Belege und Befähigungen der prosozial GmbH.....	5
1.1 Technologisch.....	6
1.2 Betrieblich.....	7
1.3 Forschung und Wissenschaft.....	9
1.4 Landesfreigaben.....	
1.5 Zu guter Letzt: Nur Positiv-, keine Negativanzeigen – kein Verstoß gegen den Datenschutz!.....	10
	10
2. B wie BSI-Grundschutz-konform: Datenschutzkonformität der prosozial-Lösungen comp.ASS 21 und butler 21 im Hosting.....	11
2.1 Hosting im prosozial-Rechenzentrum.....	12
2.2 prosozial minimiert und trägt Ihr Risiko - beim Hosting im Rechenzentrum.....	12
2.3 Datensparsamkeit.....	13
2.4 Zweckbindung.....	13
2.5 Besonderheiten des Fallmanagements.....	14
2.6 Fallmanagement und Datenschutz	16
2.7 Hosting und Datenschutz.....	17
2.8 Datensicherheit.....	
3. C wie Compliance: Technische und organisatorische (Sicherheits-) Maßnahmen bei der prosozial GmbH als Auftragnehmer (Stand 09/2016).....	

Hinweis:

Aufgrund der besseren Lesbarkeit wird in diesem Text nur die männliche Schreibweise verwendet. Diese schließt automatisch die weibliche Form mit ein. Wir bitten alle Leserinnen und Leser um Verständnis.



(K)ein kleines ABC des
Datenschutzes bei prosozial

A

wie anerkannt: Freigaben, Ausweise, Belege und Befähigungsnachweise der prosozial GmbH

B

wie BSI-Grundschutz-konform: Datenschutzkonformität der prosozial-Lösungen comp.ASS 21 und butler 21 im Hosting

C

wie Compliance: Technische und organisatorische (Sicherheits-) Maßnahmen bei der prosozial GmbH als Auftragnehmer (Stand 09/2016)

1. A wie anerkannt:

Freigaben, Ausweise, Belege und Befähigungen der prosozial GmbH

1.1 Technologisch

Microsoft Gold Certified Partner: Das Unternehmen prosozial erlangte bereits wenige Jahre nach seiner Gründung 1995 das Zertifikat im Status eines GOLD-Partners, was die höchste Stufe der Zertifizierung ist, die ein Unternehmen bei Microsoft erreichen kann. Dieser Status ist ein Ausweis und Zertifikat für das höchste Maß an Expertise, Kompetenz und Aktualität, die man beim Unternehmen und seinen Mitarbeiter erwarten kann. Diesen Status hat prosozial immer gehalten und nie verlassen. 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 aus der gesamten Microsoftumgebung und darüber hinaus den höchsten Anforderungen moderner IT-Technologie standhalten. Darüber hinaus ist prosozial ebenfalls seit vielen Jahren Citrix-Partner – genauer gesagt: **Citrix Partner Silver: Solution Advisor.**

Microsoft®
GOLD CERTIFIED
Partner



BA-zertifizierter eM@w-Provider: prosozial ist seit 2006 ein bei der Bundesagentur für Arbeit (BA) akkreditierter Provider und darf demnach als solcher im vom Bundesdatenschutzbeauftragten freigegebenen elektronischen Maßnahmeabwicklungsverfahren **eM@w** besonders schutzwürdige personen- und maßnahmebezogene Sozialdaten verarbeiten und zwischen Trägern und Bundesagentur für

Arbeit austauschen. Insbesondere wenn Kunden nicht nur unsere Software comp.ASS nutzen, sondern sie auch durch uns im Hosting in Koblenz betreiben lassen, verbleiben die Daten nach der gesicherten Weitergabe durch die BA an uns als Provider allein bei uns im Rechenzentrum. Aufnahme, Weitergabe und Bereitstellung der Daten finden samt und sonders hinter den schützenden Mauern der Firewall und den scharf geschalteten organisatorischen und technischen Maßnahmen der Zugangs-, Zutritts- und Zugriffskontrolle der prosozial GmbH 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 BA. Das dabei vereinbarte Datenmelde- und Austauschschema **XSOZIAL**, Teil der **XÖV**, wurde unter Beteiligung von prosozial mit entwickelt und weiterentwickelt. Unsere zugelassenen kommunalen Träger erzeugen und versenden in einem vom Bundesdatenschutzbeauftragten freigegebenen Verfahren zertifiziert mit unserer Client-Server-Anwendung comp.ASS diesen vermutlich größten Sozialdatensatz in Deutschland seit 2005 in jedem Kalendermonat. 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 ebenfalls 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.



1.2 Betrieblich

Betrieblicher Datenschutzbeauftragter nach § 4f BDSG: prosozial erklärt, dass in unserem Unternehmen ein betrieblicher Datenschutzbeauftragter gemäß § 4f BDSG bestellt ist und dass seine Position im gesetzlich vorgegebenen Umfang geschützt ist.



Das gesamte Personal ist datenschutzverpflichtet: prosozial erklärt, dass sämtliches Personal - alle Beschäftigten, Auszubildenden, Praktikanten, usw. - im Hause über den Datenschutz belehrt und eine Verpflichtungserklärung über die Einhaltung des Datenschutzes vor Arbeitsantritt unterzeichnet haben müssen. Alle Bediensteten unterliegen den Richtlinien der Zutrittskontrollen im Firmengebäude mit Büro- und Serverräumen. Das Rechenzentrum von prosozial befindet sich im Firmengebäude und verfügt über eine eigene, zusätzliche Zutrittskontrolle. Nur eigens dafür ausgebildete, authentifizierte Administratoren mit Berechtigung und Geheimcode für die elektronische Schließanlage können diesen Bereich betreten.

Datenschutzcompliance in Firmenphilosophie und Mitarbeitern verankert: Die Sensibilität für die besonders hohen Sorgfaltspflichten bei der Auftragsdatenbearbeitung ist jedem Beschäftigten bei prosozial allein durch die Philosophie und Arbeitsweise, aber auch durch das Risiko und den hohen Schaden, der dem Unternehmen,

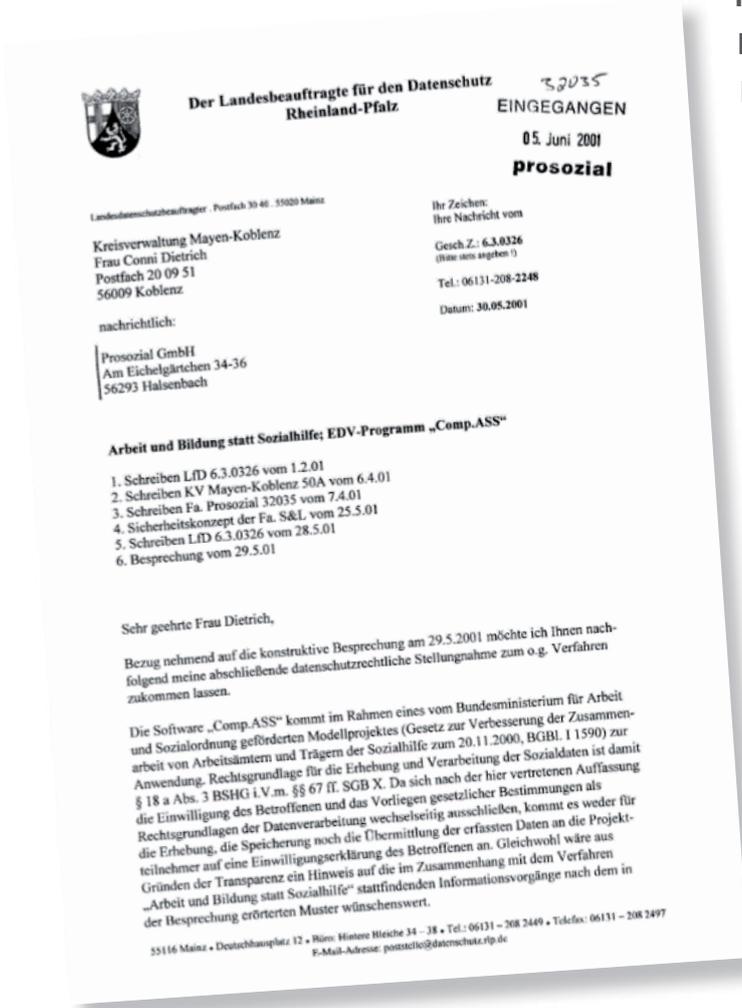
seinem Image in dieser Branche zugefügt werden kann, täglich plastisch vor Augen und voll bewusst. Denn: Sobald prosozial-Anwendungen im Einsatz sind, verarbeiten diese personenbezogene Daten aus dem besonders schutzwürdigen Sozial- und Bildungsbereich. Unsere Lösungen kommen auf mehr als 14.000 Arbeitsplätzen in Deutschland, Österreich und Belgien bei öffentlichen Trägern wie sozialkaritativen Einrichtungen und in Bildungsstätten täglich zum Einsatz. Dabei leisten wir betriebsalltäglich fachliche und technische Hotlineunterstützung, erbringen vielfältige Leistungen an und um die Verarbeitung der Daten in unseren Datenbanksystemen beim Kunden und zunehmend mehr auch im Kundenauftrag in unserem Rechenzentrum.

1.3 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 Zusammenarbeit von Arbeitsamt 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 des SGB und BDSG ausgestaltet.

1.4 Landesfreigaben



Freigabe von comp.ASS durch den Landesbeauftragten für den Datenschutz Rheinland-Pfalz: Im Zuge des MoZArT-Projektes wurde unsere dort zum Einsatz kommende Software comp.ASS 2001 von der rheinland-pfälzischen Landesbeauftragten für den Datenschutz geprüft und als unbedenklich („... keine datenschutzrechtlichen Bedenken...“) freigegeben.

Offizielle Verfahrensbeschreibung und Registrierung von comp.ASS nach § 8 Niedersächsisches Datenschutzgesetz (NDS). comp.ASS kommt bei der Verwaltung einer niedersächsischen Großstadt zum Einsatz und wird vor dem Einsatz einer Verfahrensbeschreibung nach § 8 NDS unterzogen und registriert. Seitdem ist unsere Lösung dort ohne Störung im Einsatz. Der Betrieb wird datenschutzrechtlich als unbedenklich angesehen.



zum Informationsfreiheitsangebot

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

> 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 Ganztagschulen in neuer Form		155
Abgabewesen		094
Abwasserkataster der Indirekteileiter	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

Sachsen:

Offizielle Verfahrensbeschreibung und Aufnahme ins Sächsische Verzeichnis nach § 10 SächsDSG für das Register beim Sächsischen Datenschutzbeauftragten nach § 31 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 Verzeichnis (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 Datenschutzgesetz Mecklenburg-Vorpommern nach § 18 registriert. Ohne Beanstandungen.



prosozial-Lösungen auch im Ausland im Einsatz: prosozial gewann die Ausschreibung des Königreichs Belgien für eine JobCenter-Softwarelösung. Die JobCenter des deutsch-sprachigen Teils Belgiens, der Deutschsprachigen Gemeinschaft, arbeiten bis heute mit comp.ASS. Die Pflegestützpunkte des österreichischen Bundeslandes Vorarlberg arbeiten nicht nur mit unserer Software comp.ASS, sondern hosten ihre Lösung in unserem Rechenzentrum in Koblenz.

1.5 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 auf den heutigen Tag nicht gegeben. Wenn ein Freigabe, 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 als auch mit den empfohlenen Installationen und Architekturen bei Kunden vor Ort wie auch beim Betrieb im Rechenzentrum bei uns in Koblenz am Konzept des BSI-Grundschutzes, seinen Goldenen Regeln (www.bsi.bund.de) 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

2. B wie BSI-Grundschutz-konform:

Datenschutzkonformität der prosozial-Lösungen
comp.ASS 21 und butler 21 im Hosting

2.1 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 dem Bundesdatenschutzgesetz im Allgemeinen und zusätzlich den besonderen Bestimmungen zum Sozialdatenschutz. Dem wird u. a. Rechnung getragen durch:

- Zutrittskontrolle zum Gebäude nur mit Chipkarte, keine unbegleiteten Besucher.
- Zusätzliche und eigenständige Zugangskontrolle zum Serverraum.
- Nur autorisiertes Personal hat Zutritt.
- Zugriff 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 Regime des Rechenzentrums gespeichert).
- Kein digitaler Wildwuchs: lupenreine, reinrassige Installationen, keine Risiken durch inkompatible Fremdsoftwares, die Ihre Lösung unübersichtlich und das Risikomanagement unhandlebar machen.
- Jede bei uns im Rechenzentrum gehostete Lösung ist „dedizierte Instanz“ und erhält ein eigenständiges Regime mit einer eigenen Domäne.
- Permanente Aktualisierung der Virens Scanner.
- Monatliche, feste Update-Zyklen. Im Abgleich nach den Patch-Days von Microsoft halten wir Ihre Lösung 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 Sie beauftragte Dritte, Ehrenamtliche, Klienten und Bürger als zugelassene Nutzer per Registrierung in den CRM-Bereich Ihrer Anwendung in unserem Rechenzentrum hinter die Firewall in einen geschützten und dennoch von Ihren hoheitlichen Daten getrennten Bereich lassen und Daten, Dokumente und E-Mails austauschen, ohne dass diese den geschützten Bereich je verlassen.
- Kommunikativ nach außen: Sollen Ihre Daten, E-Mails, Dokumente einmal den geschützten Bereich nach außen verlassen (z.B. SGB-II-Statistik, Sozialdatenabgleich, Trägerbeauftragung, usw.), dann wird jedes Kommunikat kryptifiziert und Ende-zu-Ende-verschlüsselt.
- Steigern sich Anforderungen, Gesetze und Technik, passen wir unsere Hosting-Systematiken an.

2.2 prosozial minimiert und trägt Ihr Risiko - beim Hosting im Rechenzentrum

IT-Lösungen aus dem Hause prosozial unterstützen öffentliche wie freie Träger bei einem optimalen Verwaltungshandeln in allen Bereichen der verschiedenen SGB und des Betreuungsrechts. Das Erheben vielfältiger Informationen bei Leistungsberechtigten ermöglicht erst das gesetzlich geschuldete Planen und Bereitstellen passgenauer Hilfeangebote. Erst dies ermöglicht die Verknüpfung beider 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 Asyl und Bildungs- und Teilhabeleistungen, Landesblindengeld, usw. mit den Funktionsbereichen:

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

und **butler** in Betreuungsbehörden, Betreuungsvereinen, bei Betreuern mit den Funktionsbereichen:

- Sachverhaltsermittlung
- Betreuermanagement
- Betreuungsmanagement

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

Der Datenschutz in Deutschland ist im Wesentlichen im Bundesdatenschutzgesetz (BDSG) und in den entsprechenden Landesdatenschutzgesetzen geregelt und darüber hinaus in weiteren speziellen 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) der Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) gibt hier einen guten Überblick: www.bfdi.bund.de

Der Datenschutz bezieht sich natürlich auf alle personenbezogenen Äußerungen und Medien, insbesondere auf Aufzeichnungen auf Papier, auf der Schreibaufgabe und im Papierkorb im Büro, in der Handakte, bei Gesprächsaufzeichnungen, Protokollen und Mitschriften. Digitale Dokumentationen erfolgen heutzutage in einer Fachsoftware, über die allein Bescheide erzeugt und Hilfen in Gang gebracht werden können. Heutzutage sind schutzwürdige personenbezogene Daten in der Fachsoftware und ggfs. in einem externen Dokumentenmanagementsystem (DMS) oder einem E-Akte-System zu finden.

Folgende Regeln sind beim Datenschutz besonders zu beachten:

2.3 Datensparsamkeit

Gemäß § 3a BDSG; 78b SGB X haben Datenverarbeitungssysteme sich an dem Ziel auszurichten, so wenig Sozialdaten wie möglich zu erheben, zu verarbeiten und zu nutzen. comp.ASS und butler verlangen grundsätzlich keine Dateneingaben durch ihre Nutzer. Beide Programme unterstützen dabei dadurch, dass sie Nutzern „Masken“ zur Verfügung zu stellen, die sich auf die wesentlichen relevanten Daten, die zur Erfüllung des Zwecks erforderlich und somit datenschutzrechtlich erlaubt sind, zu beschränken.

2.4 Zweckbindung

Personenbezogene Daten dürfen nur für die Zwecke verarbeitet oder genutzt werden, für die die Daten erhoben bzw. gespeichert worden sind. Nun sind die „Zwecke“ unserer Kunden - sei dies im Rahmen der Fürsorgepflicht eines örtlichen Trägers der jeweiligen Sozialgesetzbücher oder auch freien Trägers

- wie z.B. arbeitslose Menschen mit ihren Ressourcen, aber auch multiplen „Vermittlungshemmnissen“ wieder in Arbeit zu vermitteln und ein dem Existenzminimum entsprechendes Dasein zu ermöglichen
- wie auch Menschen im Sinne des Betreuungsrechts zu betreuen oder einfach „nur“
- einen passenden Berufsbetreuer zu finden und dem Gericht vorzuschlagen zu können

vielfältig, komplex und umfassend und notwendigerweise mit sehr vielen Informationen und Daten verbunden.

Ohne diese Daten sind diese Zwecke schlechterdings nicht zu erreichen. Und darüber hinaus ist der Wille des Trägers, sei es die Politik oder auch die Verwaltung selbst, unterschiedlich ausgeprägt. Nirgends ist das Gesetz im Vollzug vollständig gleich. Es gibt also eine gewisse Bandbreite, wie durch entsprechende Organisations- und Handlungskonzeptionen diese Ziele, Aufgaben und Zwecke erreicht werden sollen. Dem muss die Softwareentwicklung Rechnung tragen und auf die Anforderung, wie variabel Kunden entsprechend ihren Organisations- und Handlungskonzepten umfassend die oben genannten Aufgaben und Ziele erreichen können, eingehen. Dieser Aufgabe stellen wir uns in der Software und all ihren empfohlenen Betriebsvarianten wie besonders auch im Hosting.

2.5 Besonderheiten des Fallmanagements



In Bereichen wie Jobcenter, Arbeitsagenturen, Jugendämtern, aber auch im Bereich der Eingliederungshilfe, des Betreuungsmanagements 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), zu speichern und zu nutzen, um die jeweils am besten passende Hilfe für den Betroffenen zu erreichen. Die 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.

2.6 Fallmanagement und Datenschutz

comp.ASS und butler sind von Anbeginn ihrer Entwicklung an genau auf die Methoden professionellen Fallmanagements hin ausgelegt worden. Durch detailgetreue Abbildung der Organisation und ihrer Regeln, durch Zuordnung einzelner Nutzer zu Funktionsgruppen und durch bestimmte Aktenlesemodi bzw. durch Prozesse der Beantragung und Erteilung von Eigentum, Besitz oder Leserechten an einzelnen Datenstücken zu Personen- und Maßnahmeakten, kann die Organisation den Kreis der Nutzer für professionell bestimmte Zwecke 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. Die Software befreit die 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 Datenschutzeschulung 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.

2.7 Hosting und Datenschutz



Es gibt verschiedene Arten von Hosting, sehr bekannte und häufig verwendete Hostingarten sind das Webhosting/E-Mail-Hosting. Organisationen und Privatpersonen haben hierbei grundsätzlich die Möglichkeit, Datenspeicher, Software, ja sogar Hardware über eine Internetverbindung von einem Hoster zu beziehen. Es bietet Geschäftsleuten, Privatpersonen und Behörden die Möglichkeit, Ressourcen äußerst flexibel dann und dort zu beziehen, 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, www.arbeitenviernull.de).

Content, Medien, 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 (Big Data) und übers Internet als einem neuen öffentlichen Raum erreichbar, wirken da zunächst nicht gerade vertrauensbildend. Die von prosozial angebotenen Hosting-Dienstleistungen entsprechen jedoch ganz anderen, nämlich fachlich und technisch konsequent an Datenschutz und -sicherheit ausgerichteten Systemen. Die Freigaben, die unsere Systeme überall erhalten haben, zeigen den Erfolg dieses datenschutzkonformen Angebots. Der § 11 BDSG regelt, wie verantwortliche (öffentliche und nicht öffentliche) Stellen vorgehen müssen, wollen sie personenbezogene Daten im Auftrag durch andere Stellen verarbeiten lassen. Genau auf dieses Hosting sind unsere Software und das Rechenzentrum in Koblenz ausgelegt.

Die Regelung des § 11 BDSG 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 (Hostanbieter) 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 BA und Kommunen als Jobcenter, gibt es hierzu im § 51 SGB II eine besondere Öffnungsnorm oder Ausnahmeregelung, die ausdrücklich die Beauftragung nicht-öffentlicher Stellen abweichend von § 80 SGB X vorsieht.

Die prosozial GmbH hat seit Beginn des Hostingangebots 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 Auftragsdatenverarbeitungsverträgen im Sinne des § 11 BDSG bzw. dem entsprechenden Landesgesetz gearbeitet. prosozial hat seitdem sein Know-how über den Betrieb eines modernen Rechenzentrums ständig ausgebaut und ist 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.

2.8 Datensicherheit

Bei der Datensicherheit geht es um **alle Daten** einer Unternehmung und den darauf bezogenen Maßnahmen, die z.B. gemäß dem BSI-Grundsatz, an dem sich prosozial orientiert, festgelegt und regelmäßig überprüft werden. Hier gelten die Prinzipien **Verfügbarkeit, Vertraulichkeit und Integrität**. Als IT-Unternehmen sind wir in hohem Maße auf die Einhaltung der Prinzipien - wie im BSI-Grundsatz kodifiziert - ausgelegt und natürlich auf deren Sicherstellung in jedem Fall angewiesen. Diesem tragen wir Rechnung durch eine Organisation, in welcher die betroffenen Abteilungen wie z. B. die „Interne IT“, „Kunden IT“ oder die „Entwicklungsabteilung“ 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 BSI-Grundsatzes geschult und sensibilisiert.

„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

3. C wie Compliance:

Technische und organisatorische (Sicherheits-) Maßnahmen bei der prosozial GmbH als Auftragnehmer (Stand 09/2016)

Folgende technische und organisatorische Maßnahmen zur Sicherung von Daten im Sinne der Anlage zu § 9 BDSG sind beim Auftragnehmer getroffen und werden gemäß dem Stand der Technik ständig weiterentwickelt (siehe hierzu auch die aktuelle Systembeschreibung):

Zutrittskontrolle

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

- Das Firmengebäude ist durch ein Schließsystem gesichert. Nur autorisierte Personen haben Zutritt durch eine Chipkarte. Besucher und Lieferanten müssen sich per Sprechanlage anmelden, werden persönlich empfangen und begleitet. Außerhalb der Geschäftszeiten ist der Zutritt zum Gebäude und zum Serverraum videoüberwacht.
- Der Zutritt zu Technikräumen und Serverraum ist ebenfalls durch ein Chipsystem nochmals gesichert. Zutritt haben lediglich autorisierte Personen der IT-Abteilung „Interne IT“. Die Schlüsselgewalt hat der IT-Leiter inne. Alle Zutritte werden protokolliert.



Zugangskontrolle

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

- Die Daten der Kundendatenbanken sind technisch und logisch getrennt von den Daten der prosozial GmbH.
- Der Zugang zu den Datenbanksystemen ist technisch durch Einrichtung von Benutzernamen und Kennworten gewährleistet. Die Kennwortrichtlinie reglementiert, welche Kennworte als sicher zugelassen werden.
- Der Zugang zu den Systemen ist nur auf autorisierte Mitarbeiter begrenzt.
- Der Zugang von außen ist durch entsprechende Firewall-Systeme geschützt.

Zugriffskontrolle

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

- Der Zugriff zu den Kundendatenbanken ist durch ein Berechtigungssystem gesichert. Alle Mitarbeiter der prosozial GmbH haben nur für ihre Zwecke eingerichtete Benutzerberechtigungen, die von den verantwortlichen Abteilungsleitern oder Geschäftsführern festgelegt und freigegeben werden müssen.
- Zugriff auf das Rechenzentrum unterliegt ausschließlich autorisierten Mitarbeitern.
- Zugriff auf die Datenbank des Auftraggebers haben ausschließlich:
 - a) die Mitarbeiter der Kunden-IT zum Zwecke der Fehlerbehebung;
 - b) die Mitarbeiter der internen IT zur Sicherung der Verfügbarkeit durch Wartungsarbeiten;
 - c) der Kundenberater oder seine Vertretung in Abwesenheit zur Fehlerbehebung;b) und c) nur auf Veranlassung des Auftraggebers, die Veranlassung wird vom Auftraggeber mit Name des Ansprechpartners, Uhrzeit dokumentiert sowie die Zeiten zur Fehlerbehebung.



Weitergabekontrolle

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

- Zutritte und Zugänge per Anmeldung am Rechenzentrum werden nachvollziehbar mitgeloggt.
- Die Daten werden nach einem definierten Sicherheitsplan gesichert.
- Zu Testzwecken bei Fehlerbehebungsaufträgen werden Daten ausschließlich in den EDV-Systemen der prosozial GmbH zurückgesichert, die wiederum dem oben beschriebenen Zutrittskontroll-, Zugangskontroll- und Zugriffskontrollsystem unterliegen.
- Die Weitergabe auf andere Datenträger wie USB-Stick, CD-ROM etc. ist verboten, es sei denn, der Auftraggeber verlangt die Ausgabe per Datenträger oder per verschlüsseltem Datentransport an eine von ihm benannte autorisierte Person.

Eingabekontrolle

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

- Die Zugänge und Zugriffe zum System werden mitgeloggt.
- Die Logdateien werden gesichert und geschützt aufbewahrt.

Auftragskontrolle

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

- Der Auftrag erstreckt sich auf das Verarbeiten der Daten und hier insbesondere auf das Aufbewahren und zur Verfügung stellen über eine verschlüsselte Verbindung (Dateihosting).
- Das Verändern, Sperren und Löschen ist nicht Bestandteil der Auftragsdatenverarbeitung.
- Insbesondere das Löschen der Daten erfolgt ausschließlich auf Weisung des Auftraggebers. Und soweit es technisch möglich ist und der Aufwand im Verhältnis zum angestrebten Schutzzweck steht.
- Die Löschung der Daten nach Beendigung der Auftragsdatenverarbeitung erfolgt entsprechend der in der Systembeschreibung definierten Sicherheitsintervalle nach Herausgabe an den Kunden.

Verfügbarkeitskontrolle

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

- Die Verfügbarkeit der Daten wird durch Maßnahmen entsprechend der aktuell vorhandenen technischen Möglichkeiten sichergestellt.

Gültig seit 01.09.2016



Bildquellenangaben

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

© Alle Rechte vorbehalten prosozial GmbH 2016

Mit dem Copyright zeigen wir an, dass prosozial die Urheberrechte und wirtschaftlichen Nutzungsrechte für von prosozial erstellte Texte, Bilder, Filme, PDF sowie alle weiteren Medien beansprucht. Es handelt sich, wenn dieses Zeichen erscheint, um urheberrechtlich geschützte Werke. Änderungen, Löschungen bzw. Ergänzungen sind unseren Kunden im Rahmen des Servicevertrages für eigene Zwecke erlaubt, fallen aber unter die Verantwortung des jeweiligen Autors und sind als solche zu kennzeichnen. Eine Gewähr für die Richtigkeit, Angemessenheit usw. des geänderten Mediums als Ganzem sowie aller einzelnen Änderungen übernimmt prosozial nicht.