Vorbemerkung:
Wir sind Softwarehersteller und nur nach individueller Beauftragung bzw. zur Analyse von Fehlersituationen Auftragsdatenverarbeiter. Im ersten Fall wird jeweils ein separater Verarbeitungsvertrag vereinbart, beim Softwaresupport liegt ein Supportvertrag zugrunde. Die DSGVO ermöglicht uns als Kleinunternehmen erhebliche Erleichterungen bei den bürokratischen Auflagen zum Datenschutz. Das heißt aber keineswegs, dass wir die Themen Datenschutz und -sicherheit auf die leichte Schulter nehmen. Als Softwarehersteller haben wir selbstverständlich größtes Interesse an der Einhaltung von Sicherheitsstandards, da das für uns existenzielle Bedeutung hat.

Organisatorische Maßnahmen	• Datenschutzbeauftragter aufgrund Unternehmensgröße nicht erforderlich • Wir sind ein inhabergeführtes Unternehmen und regelmäßig über datenschutzrechtliche Themen auf dem Laufenden. • Sicherhheitsüberprüfungen müssen wir zwar nicht durchführen, haben aber die Themen Datenschutz und -sicherheit aufgund ihrer existenziellen Bedeutung für unser Unternemen zur Daueraufgabe gemacht. • Wir verwenden ausschließlich Dienstleister, die ihre Server in Deutschland betreiben.
Zutrittskontrolle	Kontrollierte Schlüsselvergabe

Zugangskontrolle	• Domänen abhängiger User
	• Sicherheitseinstellungen per Gruppenrichtlinie
	• komplexes Zugangspasswort
	  ▪ mind. 12-stellig
	  ▪ gemeinsame Verwendung von Zeichen aus mind. 3 der Gruppen Groß-, Kleinschreibung, Sonderzeichen und Ziffern
	• Zwangsänderung nach 90 Tagen
	• Sperrung des Rechners bei Verlassen und nach Zeitablauf mit erneuter Kennworteingabe
	• Getrennte Konten von Systemadmin und Usern

Zugriffskontrolle	• Restriktive Zuweisung von Ordnerberechtigungen • Mandantenbezogene Ordnerstruktur • Zugriff eingeschränkt für Supportmitarbeiter • Mobile Datenträger dürfen nur nach Virenprüfung verwendet werden • Datenträger/Dokumente werden inhaus unwiederbringlich vernichtet

Transportsicherheit	• Software der edv-idee verwendet für den Datentransport das Tool 7-zip
	• Komprimierung der Daten
	• Verschlüsselung
	  ○ 256-bit AES
	  ○ Software der edv-idee: komplexes, 18 stelliges Passwort
	  ○ Individualaufträge: Passwort nach Vereinbarung

Eingabekontrolle	• Daten werden im Original in maschinenlesbarer Form aus der jeweiligen Software angeliefert.
Auftragsdurchführung bei Supportabwicklung	• Eröffnung eines Supportfalles per Telefon oder eMail durch Auftraggeber • Auftragsdatenverarbeitung erfolgt nur, wenn eine Datenanalyse zur Ursachenlokalisierung erforderlich ist • Supportfunktion mit automatischer Verschlüsselung der Daten und Komprimierung (siehe Transport von Daten) • Datenanalyse durch Sichtung und/oder Testverarbeitung • Unverzügliche, endgültige Löschung der Daten nach Abschluss des Supportfalles • Rückmeldung per Telefon / E-Mail Eine Pseudonymisierung der Daten wird nicht vorgenommen, weil diese die Identifikation und Analyse der Fehler deutlich erschweren, meist sogar verhindern würde.
Auftragsdurchführung bei Individualaufträgen	• Auftragserteilung durch Zustellung von komprimierten und verschlüsselten Daten durch den Auftraggeber • Datenanalyse und Erstellung der Auswertungen durch den Auftragnehmer • Zustellung der Ergebnisse an den Auftraggeber • Löschung der Daten beim Auftragnehmer nach Auftragsabschluss spätestens nach Projektende
Verfügbarkeitskontrolle	• Plattenspiegelung RAID 1 • Regelmäßige Datensicherung • Aktueller Virenschutz auf Server und Arbeitsplatz • Firewall auf Router und Workstations • Aktuelle Sicherheitsupdates für System und Programme

Trennungskontrolle	• Mandantenfähige Testsoftware
	• Getrennte Datenhaltung von
	  ○ Daten des Auftragnehmers
	  ○ Daten anderer Auftraggeber
	  ○ Entwicklungs-, Test- und Produktionsdaten

Programmzugang	Wir haben in unserem Sicherheitskonzept die hohen Anforderungen in den Sparkassen für den Zugriff auf Anwendungen berücksichtigt und auf zusätzliche hohe Hürden verzichtet. Der Programmzugang für den User wird durch die IT-Administratoren ermöglicht. In der Anwendung haben wir die IT-relevanten Einstellungen und die fachliche Administration getrennt. Beide Bereiche können durch separate Passwörter gesichert werden. Es gibt je Bereich nur ein programmweites Passwort (nicht user-spezifisch).
Protokollierung	In der Datenbank wir in der Tabelle LizenzConcurrent die Programmnutzung mit Username, Start- und Endzeit protokolliert. Zu der Datenverarbeitung jeder Aktion wird ein Protokoll geschrieben, in dem folgende Sachverhalte dokumentiert werden: Plausibilitätsprüfung (alle relevanten Komponenten Vorlagen, Textbausteine, Anhänge, Beraterdaten, Signaturen), Inhalt von (Datums-)Variablen, Umleitung von BeraterOEs, Ergebnis beim Erzeugen der Briefe bzw. entsprechende Fehlermeldungen, generierte Listen, Anzahl aufgetretener Warnungen bzw. Fehler, Leeren der Datentabellen, Anzahl Briefe je Berater, Datum, Start- und Endzeit, Dauer, Anzahl Briefe in der Datenbank Beim Briefempfänger: Post-, Mailadressen und Briefanrede original und geändert (User mit Datum) Beim Dokument: Datenübernahme, Erzeugen des Dokumentes, Ausgabe (Druck und/oder Mail, blockiert) mit Datum und User, Berater/Sachbearbeiter original und geändert, verwendete Vorlage, Empfängeradresse, individuelle Briefergänzungen mit der Memo-Variablen, manuell bzw. automatisch unterdrückte Unterlagen Protokolle je Aktion: Unterdrückte Unterlagen (Dok-ID, Kunde, Berater, Unterlage mit Stichtag, Unterdrückungsanlass (manuell/automatisch) Liste OE-Routing (Dok-ID, Empfänger und Kunde mit Personal.Nr., Berater/Sachbearbeiter original und neu Im Mailprotokoll (Menü Tools-Mailprotokoll) werden alle mit der Anwendung versendeten Mails dokumentiert. Im Protokoll sind folgende Inhalte: Datum, User, Absender- und Empfängeradressen, Betreff, Anzahl Anhänge, verwendete Anhänge, Aktionsnummer, Beraternummer

Daten- und Prozesssicherheit	supplyKWG18 verarbeitet Daten aus der OSP-Anwendung KWG18. Selbst wenn die mit supplyKWG18 erzeugten Briefe gelöscht würden, ist der Anforderungsprozess dadurch jederzeit nachvollziehbar. Mit der Sicherung von Datenbank und Datenordnern sind alle Einstellungen und Dokumente vorhanden. Mit einer Neuinstallation der Anwendung sind diese jederzeit zugänglich und können auch nachträglich wieder erstellt werden. Vorgenommene inhaltliche Änderungen in den Brefen sind in diversen Listen (s.o.) dokumentiert. Die Änderung der Briefe durch die User kann in den administrativen Einstellungen verhindert werden.
Schnittstellen nach außen	Für Supportanalysen gibt es im Menü Wartung die Funktion 'Paket auschecken'. Damit wird das Arbeitsumfeld komprimiert und verschlüsselt und kann vom User per SMTP-Versand an unsere Supportadresse gesendet werden. Wir haben dazu ein 32-stelliges Systempasswort hinterlegt, das durch den Anwender mit einem beliebigen Passwort ersetzt werden kann. Die Funktion muss aktiv ausgewählt werden, kann aber in den administrativen Einstellungen auch generell gesperrt werden. Das kann allerdings unsere Unterstützung im Support erheblich einschränken kann, weil über 90 % der Supportfälle in den zugrundeliegenden Daten resultieren, die wir zur Reproduktion und Analyse der Fehlersituation benötigen. Einstellungen Mailserver: Der programminterne Zugriff auf Mailfunktionalitäten ist durch eine Usertabelle bei den Einstellungen zum Mailserver abgesichert. Durch Eintragung des Users und seiner Mailadresse wird dieser dazu berechtigt. Durch Verwendung einer Whitelist kann ein Versand an nicht erlaubte Domains unterbunden werden.