Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Die afm assekuranz-finanz-makler GmbH trifft als Verantwortliche folgende technisch-organisatorische Maßnahmen, um die gesetzlichen Sicherheits- und Schutzanforderungen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

1. Vertraulichkeit (Artikel 32 Abs. 1 lit. b) DSGVO)

Zutrittskontrolle Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	Technische Maßnahmen ▪ Automatisches Zugangskontrollsystem ▪ Chipkarten-Schließsystem ▪ Zutritt Bürogebäude über Klingel/Rufanlage ▪ Sicherheitsschlösser ▪ Bewegungsmelder ▪ Videoüberwachung der Zugänge und im Serverraum - Zugang zu den Aufzeichnungen haben die System-Administration und die Geschäftsleitung - Nach Sichtung zeitnahe Löschung der Aufnahmen ▪ Der Serverraum ist immer abgeschlossen (Feuerschutztür, Einbruchhemmend), Klimaanlage ist installiert Organisatorische Maßnahmen ▪ Kontrollierter Einlass von Besuchern nach Klingelzeichen ▪ Besucher werden am Empfangsbereich abgeholt und bis zum gewünschten Ziel begleitet ▪ Restriktive Schlüsselregelung | Schlüsselbuch ▪ Sorgfältige Auswahl von Reinigungspersonal ▪ Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
Zugangskontrolle Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Technische Maßnahmen ▪ Authentifikation mit Benutzer | Passwort ▪ Kennwortverfahren (u.a. Festlegung hinsichtlich Verwendung von Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts) ▪ Abschottung interner Netzwerke durch Einrichtung von Firewall-Systemen ▪ Einsatz von Anti-Viren-Software ▪ Automatische Sperrung des Bildschirms bei Inaktivität nach Zeit ▪ Sperren von Arbeitsplätzen und/oder Benutzernamen bei mehrfachen fehlerhaften Zugriffsversuchen Organisatorische Maßnahmen ▪ Erstellen von Benutzerprofilen | Benutzergruppen ▪ Regelmäßige Überprüfung der Zugangsberechtigungen ▪ Definierte Passwortregeln ▪ Regeln zur sicheren E-Mail und Internetnutzung

Zugriffskontrolle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.	Technische Maßnahmen ▪ Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen ▪ Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit ▪ Physische Löschung von Datenträgern vor deren Wiederverwendung ▪ Mechanische Zerstörung von Datenträgern vor Entsorgung durch zertifizierte Entsorgungs-Dienstleister Organisatorische Maßnahmen ▪ Beschränkung der Anzahl der Administratoren auf das „Notwendigste“ ▪ Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat) ▪ Vorgabe zur Festlegung von Passwörtern (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts) ▪ Berechtigungskonzept auf Applikations- und Datenebene mit differenzierten Berechtigungsstufen (Profile, Rollen, Transaktionen und Objekte) ▪ Sichere Aufbewahrung von Datenträgern ▪ Verwaltung der Benutzerrechte durch Systemadministratoren
Trennungskontrolle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Technische Maßnahmen ▪ Logische und technische Trennung von Daten (softwareseitig) ▪ Speicherung in spezifischen Speicherbereichen Organisatorische Maßnahmen ▪ Benutzerprofile | Trennung von Nutzerkonten ▪ Unterschiedliche Zugriffsberechtigungen | Festlegung von Datenbankrechten
Pseudonymisierung Maßnahmen, die gewährleisten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.	▪ Eine Pseudonymisierung der Daten wird nicht vorgenommen
Verschlüsselung	▪ Verschlüsselung der E-Mails über TLS (Transport Layer Security) und S/MIME-Zertifikat ▪ Verschlüsselung der Übertragungswege via VPN

2. Integrität, Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b) DSGVO)

Weitergabekontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Technische Maßnahmen ▪ Verschlüsselung der Übertragung von Daten, insbesondere bei der Übertragung über öffentliche Netze (z.B. TLS; S/MIME) ▪ Verwendung von Virtual Private Networks (VPN) ▪ Elektronische Signatur ▪ Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken Organisatorische Maßnahmen ▪ Identifizierungs-/Authentifizierungsverfahren bei Fernwartungen
Eingabekontrolle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Technische Maßnahmen ▪ Protokollierung der Eingabe, Änderung und Löschung von Daten Organisatorische Maßnahmen ▪ Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelles Loggen mit Benutzernamen ▪ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts ▪ Festlegung der Befugten für die Erstellung von Datenträgern ▪ Gesetzeskonforme Vertragsgestaltung von Verträgen über die Datenverarbeitung personenbezogener Daten mit Dienstleistern mit entsprechender Regelung von Kontrollmechanismen
Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind, und dass Daten möglichst schnell wieder hergestellt werden können.	Technische Maßnahmen ▪ Geräte zur Überwachung von Temperatur und Feuchtigkeit in den Serverräumen ▪ Brandschutztüren ▪ Klimaanlage in Serverräumen ▪ Unterbrechungsfreie Stromversorgung (USV) ▪ Mehrschichtige Virenschutz- und Firewall-Architektur Organisatorische Maßnahmen ▪ Zentrale Beschaffung von Hard- und Software ▪ Regelmäßige Durchführung von Datensicherungen ▪ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort ▪ Notfallplanung (Notfallplan für Sicherheits- und Datenschutzverletzungen mit konkreten Handlungsanweisungen) ▪ Testen von Datenwiederherstellung ▪ Datensicherungs- und Wiederherstellungskonzept

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d) DSGVO; Artikel 25 Abs. 1 DSGVO)

Datenschutz-Management	Technische Maßnahmen ▪ Regelmäßige Prüfung der Hardware (Lifecycle, Performance) Organisatorische Maßnahmen ▪ Bestellung eines Datenschutzbeauftragten ▪ Datenschutzkonzept ▪ Eskalationsverfahren für Notfälle
Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung	Technische Maßnahmen ▪ Minimierung von Pflichtfeldern ▪ Deutliche Kennzeichnung von freiwilligen Angaben ▪ Beschränkung der Angaben und weiteren Verwendung auf das notwendige Maß Organisatorische Maßnahmen ▪ Transparente Datenverarbeitung ▪ Regelungen zur Datenminimierung, Datensparsamkeit und Erforderlichkeit ▪ Einhaltung von Branchenstandards

4. Auftragskontrolle: Auftragsverarbeitung im Sinne von Art. 28 DSGVO

Auftragskontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Technische Maßnahmen ▪ Möglichkeit der Durchführung von Kontrollen durch den Auftraggeber zur Vertragsausführung Organisatorische Maßnahmen ▪ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) ▪ Regelmäßige Überprüfung des Auftragnehmers hinsichtlich Datenschutz | Datensicherheit ▪ Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Artikel 28 DSGVO ▪ Führung eines Verzeichnisses für jeden AV-Vertrag