Technisch-organisatorische Maßnahmen („TOM“) i.S.d. DSGVO

der

XPS-Finanzsoftware GmbH (nachfolgend „XPS“ genannt) vertreten durch den Geschäftsführer Volker Weg Zugspitzstr. 6, 81541 München

Stand 03.02.2024

Vorbemerkung

Mit der webbasierten finanzmathematischen Anwendung „XPS-Privatfinanz“ und ihren verschiedenen Anwendungsmodulen Finanzplanung, Ruhestandsplanung, Generationen-Tool etc. wird XPS von den Lizenznehmern beauftragt, personenbezogene Daten zu erheben und zu verarbeiten („Software as a Service“).

Die Daten für die jeweilige Finanzanalyse werden persistent in einer SQL-Server Datenbank gespeichert. Im Rahmen der Auftragsdatenverarbeitung findet keine Speicherung von Dokumenten statt. Gespeichert werden lediglich Finanzdaten, die für die jeweiligen Analysen erforderlich oder sinnvoll sind.

Aufgrund der Unternehmensgröße ist XPS nicht verpflichtet, einen Datenschutzbeauftragten zu benennen.

XPS hat technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Es werden die aktuell getroffenen Maßnahmen dargelegt. Weitere Maßnahmen, die den Schutz von Informationen verbessern, kann XPS jederzeit und ohne weitergehende Informationspflichten gegenüber den jeweiligen Lizenznehmern ergreifen.

XPS erfüllt den gesetzlich geforderten Anspruch nach DSGVO durch folgende Maßnahmen:

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, durch:

Rechenzentrum

Die Speicherung und Verarbeitung der Daten erfolgt auf einem XPS-eigenen Server in einem gesicherten Rechenzentrum in der Balanstraße 73, 81541 München. Inhaber des Rechenzentrums ist die NorthC Deutschland GmbH, Am Tower 5, 90475 Nürnberg (übernommen von der IP Exchange

GmbH als Tochter der q.beyond AG, Köln). Das Rechenzentren wird regelmäßigen nach den folgenden Standards auditiert: Qualitätsmanagement nach ISO 9001, Informationssicherheit nach ISO 27001, TÜV Saarland: „Geprüftes Rechenzentrum“ hochverfügbar Stufe 3.

Der Zutritt zum Rechenzentrum ist über eine Stahltüre per RFID-Chipkarte und Codes geregelt, der personenbezogen freigeschaltet ist. Die Chipkarten werden vom Rechenzentrumsbetreiber ausgegeben. Der Zugang wird elektronisch durch den Rechenzentrumsbetreiber protokolliert. Dies betrifft auch fehlgeschlagene Versuche, Zugang zu erhalten. Eine Übertragung der Chipkarten und Codes ist untersagt. Ein Verlust ist durch den betroffenen Mitarbeiter unverzüglich anzuzeigen. Das Rechenzentrum besteht aus verschiedenen Räumen, die von unterschiedlichen Unternehmen gemietet werden. Der Servicepartner von XPS verfügt dort über einen eigenen abgesperrten Serverschrank. Der Zutritt zu diesem Raum wird noch einmal separat über eine Stahltüre mit RFID-Chipkarte gesichert. Nur Mitarbeiter des Rechenzentrumsbetreibers können die Schranktüre entsperren. Der gesamte Bereich wird videoüberwacht und ein Mitarbeiter des Rechenzentrumsbetreibers protokolliert und gestattet durch Ausstellung eines Besucherausweises (Chipkarte) nach Verifizierung durch Reisepass / Personalausweis / Führerschein jedes Betreten des Rechenzentrums. Die Bilddaten der Videoüberwachung werden im Rahmen der gesetzlichen Vorgaben gespeichert. Das Rechenzentrum ist durch eine Einbruchmeldeanlage alarmgeschützt. Der Zutritt von Fremdpersonal ist nur in Begleitung durch einen Mitarbeiter gestattet. Die Rechenzentrumsräume sind fensterlos und werden nur für den Betrieb von Servern verwendet.

Systemadministrator

Zutritt zu den Servern im Rechenzentrum hat ausschließlich unser Servicepartner people4.net GmbH, Germaniastr. 38, 80805 München (nachfolgend „people4.net“ genannt), ein kleines inhabergeführtes Unternehmen, das XPS seit Firmengründung im Jahr 2004 EDV-technisch betreut.

people4.net ist als Hosting-Dienstleister Vertragspartner des Rechenzentrums. XPS selbst hat keine vertragliche Beziehung zum Rechenzentrum. Ein Wechsel des Rechenzentrums durch people4.net erfolgt nur mit Zustimmung von XPS.

Sonstige Rechner

Eine Speicherung von Produktivdaten auf anderen Rechnern, die nicht im Rechenzentrum stehen, ist Mitarbeitern und Entwicklern untersagt. Hiervon ausgenommen ist die Speicherung von Backups auf verschlüsselten oder in einem Tresor bzw. Bankschließfach gelagerten Datenträgern. Die Zutrittskontrolle ist daher auf den Zutritt zum Rechenzentrum beschränkt.

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort wie auch der Einsatz von Chipkarten zur Anmeldung. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Keine unbefugte Systembenutzung durch:

Für den Login gibt es Sicherheitsfunktionen. Nach einer vernünftig bemessenen Anzahl von Fehlversuchen wird der Zugang gesperrt, um Brute-Force-Angriffe zu verhindern.

Der Zugang zur Anwendung erfolgt über Login mit E-Mail und Passwort. Die Eingabe des Passwortes erfolgt über die SSL-gesicherte Webseite. Initiale Passwörter mit Zusendung per E-Mail werden nicht verwendet. Bei der Neuvergabe des Passworts wird ein Passwort-Checker für Mindestanforderungen an das Passwort verwendet.

Mandantentrennung

Die Anwendung sieht eine Mandantentrennung vor. Zugang zu den Produktivdaten des Auftraggebers haben daher nur der Auftraggeber und seine Berater, für die von ihm angelegten Kunden und Interessenten, sowie die Kunden und Interessenten selbst zu ihren eigenen Daten, falls ihnen vom Berater ein Zugang gewährt wurde. Der Auftraggeber kann Berater und Kunden bzw. Interessenten anlegen, sperren und löschen.

Verschlüsselung / Aufbewahrung von Datenträgern

Die Datenbank mit den Produktivdaten ist über ein AES-256-Verfahren verschlüsselt. Backups der Produktivdaten werden auf Datenträger gespeichert, die in einem Tresor oder Bankschließfach aufbewahrt werden oder verschlüsselt sein müssen.

Zugänge und Passwörter

Zugangs- und Datenbankpasswörter müssen Zahlen, Buchstaben und Sonderzeichen enthalten. Ein regelmäßiger Wechsel der Passwörter ist nicht vorgesehen. Sollte die Zusammenarbeit mit einer mitarbeitenden Person enden, so sind alle relevanten Passwörter neu zu vergeben.

1.3 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 können.

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

Rollen-Rechte-Konzept / Identitymanagement

Die Berechtigungen für den Server und deren Zugänge werden von unserem Serveradministrator people4.net verwaltet.

Der Datenzugriff erfolgt über eine gesicherte SSL-Verbindung. Der Server ist mit einer Firewall und einer Anti-Virus-Software ausgestattet. Zugriffe durch die Entwickler auf den Server erfolgen über eine gesicherte VPN-Verbindung.

Supportmitarbeiter haben keinen Zugriff auf Kunden- und Interessentendaten der Berater.

Verwaltung durch den Auftraggeber

Nach Einrichtung des Anwendungszugangs durch XPS, verwaltet der Auftraggeber selbst das Anlegen, Löschen und Sperren von Beratern. Über die Mandantentrennung wird gewährleistet, dass der Auftraggeber keine Fremddaten einsehen kann. Ebenso kann ein vom Auftraggeber angelegter Berater keine Daten eines anderen vom Auftraggeber angelegten Beraters ohne dessen Zustimmung einsehen. Die Berater des Auftraggebers können ihre eigenen Kunden und Interessenten anlegen, löschen und sperren. Ob die Kunden und Interessenten einen eigenen Zugang zu ihrer Analyse erhalten, entscheidet der Auftraggeber entweder grundsätzlich für alle Berater bzw. wenn ein Kunden-/Interessentenzugang vom Auftraggeber gewünscht ist, der Berater fallweise für seine Kunden und Interessenten.

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, durch:

Entwicklung / Testserver

Die Entwicklung findet auf den lokalen Rechnern der Entwickler und mit anonymisierten Daten statt. Um größere Änderungen im Echtbetrieb zu testen, steht auf einem virtuellen Server ein getrenntes Testsystem zur Verfügung. Nach erfolgreichem Test in der lokalen Umgebung bzw. auf dem Testserver wird die Anwendung auf den Produktionsserver publiziert.

Rechentest

Die Analysen basieren auf finanzmathematischen Berechnungen, deren Rechenkern unter EXCEL Visual Basic entwickelt und anschließend in einem gekapselten Rechenkern zur Verfügung gestellt wird. Je nach Modul gibt es einen Testbestand von Analysen, die nach wesentlichen Änderungen im Rechenkern einer Abweichungskontrolle unterworfen werden.

Neben der Offlinekontrolle gibt es ein Testsystem in den Onlineanwendungen. Die offline erstellten Testbestände werden regelmäßig in das Onlinesystem eingespielt, um sicherzustellen, dass die Rechenkerne online und offline identisch rechnen.

Datenbanken

Neben den Anwendungsdaten werden zu Informationssicherheitszwecken Logdaten ermittelt und temporär gespeichert. Die Speicherung von Anwendungsdaten und Logdaten erfolgt in getrennten Datenbanken.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen, durch:

Anonymisierung / Pseudonymisierung

Entwickler von XPS verwenden für die Entwicklung der Anwendung ausschließlich anonymisierte Datenbanken und Datensätze.

Bei der Anonymisierung werden beispielsweise:

- Name auf Initialen reduziert
- Adressen und Bemerkungen gelöscht
- Bezeichnungstexte auf 3 Zeichen gekürzt
- E-Mails auf Zufallstexte „67bede99-a05d-4a96-bcc2-c0abbf03528d@anonym.de“ abgebildet
- Datums- und Wertfelder bleiben wegen der Rechenfunktionen unverändert

Sollte aus Gründen der Fehlerbehebung in begründeten Ausnahmefällen die Fehleranalyse für die Entwickler tatsächlich nur auf Basis der Produktivdatenbank möglich sein, so sind die Produktivdaten nach erfolgter Fehleranalyse unverzüglich wieder zu löschen.

Support und Fernwartung

Supportmitarbeiter und auch die Anwender sind angehalten, den fachlichen Support ausschließlich auf Basis von anonymisierten Analysen vorzunehmen. Die Anwendungen sind zu diesem Zweck mit Makros ausgestattet, die eine vollständig anonymisierte Kopie der relevanten Analyse erstellen.

Dies gilt auch und insbesondere beim Einsatz von Fernwartungstools oder bei Unterstützung per E-Mail. Hier hat die Bildschirmübertragung soweit möglich bzw. der E-Mailversandt unbedingt auf Basis der anonymisierten Supportkopie zu erfolgen.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

Die Weitergabe personenbezogener Daten durch den Auftragnehmer an Subunternehmer wie z.B. Serveradministrator ist außer zur Unterstützung bei Fehlerbehebung oder bei technischen Störungen nicht gestattet; ggfls. sind die weitergegebenen Daten nach erfolgter Behebung des Fehlers oder der technischen Störung unverzüglich zu löschen.

XPS verwendet in der Anwendung keine Analysetools wie Google-Analytics oder ähnliches und keine Like-Buttons etc. von sozialen Medien, die eine Analyse und Weitergabe von Benutzerdaten oder Benutzerverhalten der Anwender zur Folge haben.

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch:

Die jeweiligen Analysen können den Kunden oder Interessenten optional zugänglich gemacht werden. Dabei entscheidet der Berater, ob die Analyse mit einem Schreibschutz versehen wird oder nicht. Die Eingabe der Daten des Auftragsgebers erfolgt durch den Auftraggeber, die Berater oder bei Erteilung eines Zugangs ggfls. auch durch die Kunden oder Interessenten selbst.

Es findet keine automatische Änderungsprotokollierung in der Anwendung statt. Eine Änderungsprotokollierung kann der Berater selbst über eine Notizfunktion innerhalb der Anwendung vornehmen.

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

Alle Systemkomponenten des Servernetzwerks werden regelmäßig überprüft und Bauteile proaktiv ausgetauscht. Wichtige Systeme wie Router, Switche und Mailserver sind redundant ausgelegt. Die Wände des Rechenzentrums sowie die Wände des Raums des Auftragnehmers bestehen aus Massivsteinen. Der Raum im Rechenzentrum verfügt über ein Brandfrüherkennungssystem sowie eine automatische Gaslöschanlage. Bei Auslösung eines Alarms wird automatisch der Rechenzentrumsbetreiber sowie ein Sicherheitsdienst informiert. Alle Türen im Rechenzentrum sind feuerfest. Es existiert eine Klimaanlage, die dreifach redundant ausgelegt ist. Alle Server sind über eine unterbrechungsfreie Stromversorgung („USV-Anlage“) gesichert. Das Rechenzentrum verfügt über redundante Dieselgeneratoren. Wartungen der genannten Komponenten finden regelmäßig durch den Rechenzentrumsbetreiber statt.

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Nach einem technischen Zwischenfall wird eine rasche Wiederherstellbarkeit der Daten ermöglicht durch:

Alle Daten werden zusätzlich auf Backupsystemen gesichert. Eine Wiederherstellung von Teilsystemen ist dadurch für die Serveradministratoren zeitnah möglich. Für jedes Teilsystem existieren dafür unterschiedliche Notfall- und Backupkonzepte. Des Weiteren findet täglich ein Backup auf andere Server im gleichen Raum statt. Es existieren Notfallkonzepte für die Wiederherstellung aller Teilsysteme, die nicht dokumentiert sind, aber jedem Systemadministrator von people4.net bekannt sind.

Die Produktivdatenbank für die Anwendung ist getrennt von anderen Datenbanken und wird damit klein gehalten (Datenvolumen derzeit kleiner 3 GB). Backup und Wiederherstellung der Datenbank werden dadurch erleichtert und beschleunigt.

Von XPS wird regelmäßig getestet, ob die Datenbank-Backups funktionsfähig sind, d.h. eine Wiederherstellung der Datenbank tatsächlich möglich ist.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Management und innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird, durch:

Aufgrund der Unternehmensgröße ist die Bestellung eines Datenschutzbeauftragten nicht vorgeschrieben. Verantwortlich für die Einhaltung der Datenschutzbestimmungen ist der Geschäftsführer.

Unternehmensstrategie und -politik von XPS ist es, dass personenbezogene Daten – bis auf Datensicherungen – ausschließlich im Rechenzentrum verarbeitet werden und XPS-seitig ausschließlich Administratoren einen Zugang zur Datenbank auf dem Server und damit zu den besonders kritischen personenbezogenen Kunden- und Interessentendaten der Berater haben.

XPS praktiziert in der Softwareentwicklung, der Informationssicherheit und auch im Datenschutz einen kontinuierlichen Verbesserungsprozess („KVP“). Erkannte Schwachstellen werden analysiert, beseitigt und wenn möglich nachhaltige Verbesserungsmaßnahmen ergriffen.

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen durch:

Es ist ein IT-Notfallmanagementhandbuch mit Handlungsanweisungen und Checklisten für Notfälle und Vorsorgemaßnahmen vorhanden. Daneben haben wir mit people4.net einen kompetenten Servicepartner, der uns berät und über weitreichende Erfahrungen auch im Notfallmanagement verfügt.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Privacy By Design / Privacy By Default durch:

Datensparsamkeit

Die Anwendungen sind so konzipiert, dass für die Analysen selbst keine personenbezogenen Daten erforderlich sind. Es ist beispielsweise nicht erforderlich, dass Adressdaten, Versicherungsnummern oder andere Vertragsnummern erfasst werden. Die Anwender haben die Möglichkeit mit einem Minimum an datenschutzkritischen Informationen zu arbeiten.

Datenlöschung

Der Auftraggeber hat selbst die Möglichkeit, Kunden und Interessenten mit ihren Analysen und Berater zu löschen. XPS kann jederzeit die Daten des Auftraggebers mit sämtlichen Beratern, Kunden und Interessenten und Analysen aus dem aktiven Datenbestand löschen. Das Löschen erfolgt auf Anforderung durch den Auftraggeber. Ein automatisches Löschen erfolgt nicht.

Nach Löschung sind keine Daten des Auftraggebers mehr im aktiven Datenbestand der Anwendung. Sollte tatsächlich das Einspielen von Backup-Daten in das Produktivsystem erforderlich sein, so kann ein Abgleich zwischen den aktiven Anwendern vorher und nachher vorgenommen werden und zuvor gelöschte Anwender auch nach Einspielen des Backups wieder gelöscht werden.

4.4 Auftragskontrolle (bei Auftragsverarbeitung i.S.v. Art. 28 DS-GVO)

Regelung bei Outsourcing an Dritte durch:

Außer dem oben genannten Servicepartner people4.net, hat kein weiterer Dienstleister Zugang oder Zugriff auf Daten der Kunden und Interessenten des Auftraggebers. Mit people4.net ist ein Auftragsdatenverarbeitungsvertrag geschlossen.