Anlage 1

Diese Anlage zu den Technisch-organisatorischen Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO ist vom Verantwortlichen (Art. 30 Abs.1 lit g) wie auch vom Auftragsverarbeiter (Art. 30 Abs. 2 lit d) zwingend entsprechend seiner innerbetrieblichen Organisation auszufüllen. Wo zutreffend, können Referenzen auf die zur Verfügung gestellten Dokumente/Zertifikate (Ziffer 12 dieser Anlage) angegeben werden. Die innerbetriebliche Organisation ist vom Verantwortlichen/Auftragsverarbeiter so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dies beinhaltet insbesondere:

1. Zutrittskontrolle zu Räumlichkeiten und Einrichtungen, in denen Daten verarbeitet werden

Technische bzw. organisatorische Maßnahmen, nach dem jeweiligen Stand der Technik, zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Die Herausgabe von Schlüsseln passiert kontrolliert und wir entsprechend dokumentiert. Zu jeder Schlüsselübergabe gibt es ein Protokoll. Zentrale und nicht vergebene Schlüssel werden sicher verwahrt.
- Der Eingang zum Gebäude und der Eingang zu den Büroräumen sind permanent verschlossen. Eingangsbereiche und Fenster sind außerhalb der Geschäftszeiten fest verschlossen.
- Während der Geschäftszeiten ist der Empfang besetzt und dient zusätzlich als Zutrittskontrolle.
- Die Eingangstür lässt sich nur von außen mit einem Schlüssel oder per Schalter vom Empfang zu öffnen.
- Alle Zugänge werden außerhalb der Geschäftszeiten durch eine Überwachungseinrichtung (Videokameras) überwacht.
- Besucher, Gäste und Schulungsteilnehmer können sich nur im Trainingsbereich frei bewegen. Der Zutritt zu den Büroräumen ist nur mit Amagno Personal gestattet. Der Zutritt zum Rechenzentrum ist diesem Personenkreis untersagt.
- Die Anwendungsserver stehen in einem abgeschlossenen Raum, zu dem nur die IT-Administratoren Zutritt haben.
- Das Rechenzentrum befindet sich außerhalb des Gebäudes. Der Zutritt ist nur einen bestimmten Personenkreis gestattet. Jeder Zutritt wird protokolliert.

2. Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Jeder Mitarbeiter hat einen personalisierten Account, mit dem er sich an seinem persönlichen Rechner anmelden kann.
- Alle Systeme werden immer auf dem aktuellsten Stand gehalten um die bestmögliche Sicherheit zu gewährleisten.
- Die Zugangsrechte zu den Systemen sind individuell eingerichtet.
- Die Anzahl der Administratoren ist auf das Minimum begrenzt.
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung (Timeout)/Bildschirmsperrung)
- Das Netzwerk von Amagno ist gegen externe Zugriffe durch eine Firewall abgeschirmt.
- Es besteht auf allen Systemen ein Virenschutz
- Die Fernwartungszugänge zu den Servern und externe Zugriffe von Endgeräten außerhalb des Netzwerkes sind über eine VPN Verbindung abgesichert.
- Es werden nur temporäre Passwörter vergeben, die der Benutzer ändern muss. Die Passwörter können nicht durch den Administrator eingesehen werden.

3. Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Der Zugriff auf die Notebooks, Desktoprechner und Server erfolgt ausschließlich über personalisierte Authentifizierung. Die Berechtigungen (Profile, Rollen, Transaktionen und Objekte Bsp.: Begrenzung Zugriff auf Ordner) sind nach dem „need to know“ Prinzip eingerichtet)
- Amagno setzt entsprechende Passwortregeln (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts) ein.
- Die Zugänge werden nach entsprechender Anzahl von Fehlersuchen gesperrt.
- Die Benutzerkonten von ausgeschiedenen Mitarbeitern werden sofort nach dem Verlassen des Unternehmens deaktiviert.
- Nicht mehr benötigte Daten werden ordnungsgemäß gelöscht und vernichtet.
- Bei Amagno gibt es kein „Account-Sharing“ (mehrere Personen nutzen einen Account) / eindeutige „Benutzer-ID“ (Benutzer-Zuordnung)

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln (Elektronische Übertragung, Datentransport, Übermittlungskontrolle, usw.), um einen Verlust, eine Veränderung oder eine unbefugte Veröffentlichung zu verhindern.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Personenbezogene Daten im Online Verfahren ausschließlich über eine VPN-Verbindung bzw. über eine SSL/TLS verschlüsselte Verbindung übertragen
- In begründeten Ausnahmefällen können Daten nach Rücksprache und mit der Genehmigung des Auftraggebers in einer passwortgeschützten Datei oder verschlüsselten E-Mail versandt werden. Das Passwort für die Datei wird dem Empfänger über einen anderen Weg mittgeteilt
- Personenbezogene Daten werden nicht auf Datenträgern weitergegeben.

- Es wird mit allen Auftragsverarbeitern eine Vereinbarung zur Auftragsverarbeitung geschlossen.
- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.
- Das interne W-LAN ist über WPA2 gesichert, zudem gibt es ein WPA2 gesichertes Gäste W-LAN

5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten derart, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen; Art. 32.I.a) DSGVO; Art. 25.I DSGVO)

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

Da personenbezogene Daten in den genutzten Anwendungen der Amagno ursächlich entstehen und diese im Rahmen der Bearbeitung unerlässlich sind, die als erste zu pseudonymisieren wären, würde eine Pseudonymisierung in diesen Anwendungen zu nicht tragbaren Behinderungen der Sachbearbeitung und mangelhaftem Antwortzeitverhalten führen und wird deshalb nicht durchgeführt.

6. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- In den von Amagno genutzten Systemen, in denen personenbezogene Daten verarbeitet werden, kann jederzeit überprüft werden, wann und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden. Dies kann auch nachträglich überprüft werden, da alle Änderungen protokolliert werden.
- Alle Dokumente werden in einem Dokumentenmanagementsystem aufbewahrt, welches DSGVO und GOBD konform ist.

7. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Eine Datenverarbeitung durch Dritte (vergleiche Artikel 28 DSGVO) ist gemäß den Anweisungen des Auftraggebers/Datenexporteurs erlaubt. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber/Datenexporteur und Auftragnehmer/Datenimporteur:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Es liegt in der Verantwortung der Führungskräfte von Amagno, dass personenbezogene Daten nur entsprechend der Weisung der Auftraggeber und nach den geltenden Rechtsvorschriften, in den Geschäftsprozessen verarbeitet werden.
- Es bestehen eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten.
- Alle Lieferanten und Unterauftragnehmer werden sorgfältig ausgewählt.
- Nach Beendigung des Vertragsverhältnisses werden alle nicht mehr benötigten Daten gelöscht.

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

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Alle Daten werden regelmäßige nach einem Datensicherungen/Backup-Verfahren online gesichert, um eine größtmögliche Verfügbarkeit zu gewährleisten.
- Die Integrität (Integrativity) der IT-Systeme wird durch entsprechende Maßnahmen sichergestellt.
- Um einen Datenverlust durch einen Stromausfall zu verhindern, werden Unterbrechungsfreie Stromversorgungen (USV) eingesetzt.
- Alle Server sind gegen Angriffe durch entsprechend Maßnahmen (Virenschutz / Firewall) gesichert.

9. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

- Die unterschiedlichen Anwendungen sind voneinander getrennt. Die Verwaltung innerhalb der Systeme stellt sicher, dass nur Berechtigte Zugriff haben.
- Funktionstrennung (Produktion / Test)
- Logische Trennung von Daten

10. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32.I. d) DSGVO; Art. 25.I DSGVO)

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen:

Datenschutz-Management

- Datenschutz ist Aufgabe des gesamten Unternehmens.
- Die IT-Sicherheit muss stets auf dem aktuellen Stand der Technik sein.
- Es werden datenschutzfreundliche Technologien eingesetzt, wenn es möglich und wirtschaftlich ist.
- Regelmäßige Sensibilisierung und Schulung der Mitarbeiter.
- Festlegen von Zuständigkeiten.
- Weisungen von Kunden im Rahmen einer Auftragsverarbeitung werden kundenbezogen dokumentiert.
- Ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert.

Incident-Response-Management:

- Es bestehen interne Prozesse und Handlungsanweisungen zum Datenschutz, die bei Bedarf erweitert oder ergänzt werden.

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

- In den verwendeten Systemen wird stets die höchste Schutzstufe bei der Erstellung neuer Benutzer verwendet. Neue Benutzer haben keine Rechte in den Systemen. Diese werden erst mit der Zuordnung der Rolle zugeteilt.