EMEA
TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN
(TOMs)

Versionsänderung/Überprüfungshistorie

Freigabe /Version	Datum	Autor(en)	Revision Details
1.0	25.05.2018	Gerhard Smischek	Originaldokument
2.0	01.02.2021	Mateusz Leszczynski	Auf neues Vorlagenformat umgestellt. Umstellung der Versionierung auf eine gemeinsame Nomenklatur. Umstellung auf das Konzept von ISO/IEC 27001:2013 und Exela ISO 27001-Zertifizierungsprogramm. EMEA-weit erweitert.
2.1	19.05.2021	Bernhard Hofmann	Deutsche Nachbearbeitung
2.2	20.05.2021	Oleg Simanic	Freigabe
3.0	21.07.2021	Mateusz Leszczynski	Aktualisierung des territorialen Geltungsbereichs: 2 geschlossene Betriebsstätten entfernt, 1 neu zertifizierte Betriebsstätte hinzugefügt; Freigabe

Präambel

Exela Technologies (im Folgenden als "Exela" bezeichnet) ist ein führendes Unternehmen im Bereich der Geschäftsprozessautomatisierung (BPA), das eine globale Präsenz und firmeneigene Technologien einsetzt, um Lösungen für die digitale Transformation anzubieten, die die Qualität, Produktivität und die Erfahrung der Endbenutzer verbessern. Das Geschäft von Exela, das in den Anwendungsbereich dieses Dokuments fällt, ist Design, Entwicklung, Implementierung und Support von Dokumentenmanagement & Bildverarbeitung, Datenerfassung, Workflow-Lösungen, Software-Support-Services und Managed Services einschließlich Druck, Post & Versand.

Exela beabsichtigt, die Sicherheit der personenbezogenen Daten in Übereinstimmung mit der GDPR und UK-GDPR zu gewährleisten und stellt sicher, dass die Daten des Kunden auf sichere Weise verarbeitet werden. Das folgende Dokument stellt geeignete technische und organisatorische Maßnahmen vor, deren Schutzniveau den Risiken der Verarbeitungstätigkeiten von Exela angemessen sind. Das Informationssicherheitsmanagement beschreibt Kontrollen, die eine Organisation implementieren muss, um sicherzustellen, dass sie die Vertraulichkeit, Verfügbarkeit und Integrität von Daten vor Bedrohungen und Schwachstellen sinnvoll schützt.

Bei den getroffenen Maßnahmen handeln es sich um solche, die ein dem Risiko angemessenes Schutzniveau in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne der GDPR und UK-GDPR berücksichtigt worden. Zur Orientierung wird auf die Konzepte der ISO/IEC 27001:2013 "Informationssicherheitsmanagementsysteme" Anhang A verwiesen.

Regionaler Geltungsbereich

Die folgenden TOMs gelten für die Region EMEA und beziehen sich auf die unten aufgeführten ISO/IEC 27001:2013-zertifizierten Exela-Standorte:

1. Exela Technologies, Baronsmede House, 20 the Avenue, Egham, TW20 9AB, Vereinigtes Königreich;
2. Exela Technologies, Sandringham House, Sandringham Avenue, Harlow Business Park, Harlow CM19 5QS, Vereinigtes Königreich;
3. Exela Technologies, Barclays House, 1 Wimborne Road, Poole BH15 2BB, Vereinigtes Königreich;
4. Exela Technologies, Moulton House, 10 Pond Wood Close, Moulton Park, Northampton NN3 6DF, Vereinigtes Königreich;
5. Exela Technologies, 8 Beckett Way, Park West, Nangor Road, Dublin 12, Irland;
6. Exela Technologies, Vastberga Alle 36A, Hagersten, Stockholm 120 23, Schweden;
7. Exela Technologies, Eskilstunavagen 34, Strangnas 645 34, Schweden;
8. Exela Technologies, Gripengrand 4, Froson 838 80, Schweden;
9. Exela Technologies, Eskilstunavagen 34, Strangnas 645 34, Schweden;
10. Exela Technologies, Nedre Rommen 5C, Oslo 0988, Norwegen;
11. Exela Technologies, Plauener Str. 163-165, Berlin 13053, Deutschland;
12. Exela Technologies, Hübnerstrasse 3, Augsburg 86150, Deutschland;
13. Exela Technologies (GmbH), Monzastrasse 4c, Langen 63225, Deutschland;
14. Exela Technologies, Grudziądzka 46-48, Toruń 87-100, Polen;
15. Exela Technologies, 1 Rue de la Mare Blanche, Noisiel 77186, Frankreich;
16. Exela Technologies, 14 Rue des Landelles, Cesson Sevigne, Ille-et-Vilaine 35510, Frankreich;

17. Exela Technologies, ZAC des Foliouses, Rue de Monts d'Or, Miribel les Echets 01700, Frankreich;
18. Exela Technologies, Uraniumweg 15, 3812 RJ Amersfoort, Holland
19. Exela Technologies (ETH), Monzastrasse 4c, Langen 63225, Deutschland;

Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit von Verarbeitungssystemen und Diensten

I.Physische und räumliche Sicherheit

Relevante ISO-Regelungen: A.11.1.1 Physischer Sicherheitsumfang; A.11.1.2 Physische Zugangskontrollen; A.11.1.3 Sicherung von Büros, Räumen und Anlagen; A.11.1.4 Schutz vor externen und umweltbedingten Bedrohungen; A.11.1.5 Arbeiten in sicheren Bereichen

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Alle relevanten Türen und/oder Fenster sind durch Kontrollmechanismen (z. B. Schlösser, Riegel, Alarme, Ausweisleser, Magnetkarten) in geeigneter Weise gegen unbefugten Zutritt gesichert;

☒ Wo erforderlich, sind zusätzliche Barrieren und Abgrenzungen zur Kontrolle des physischen Zugangs zwischen Bereichen im selben Gebäude vorhanden (z. B. für Serverräume);

☒ Der Zugang zu den Standorten und Gebäuden ist nur für autorisiertes Personal möglich;

☒ Zugriffsrechte werden auf einer "Need-to-know"-Basis gewährt und regelmäßig überprüft, aktualisiert und bei Bedarf widerrufen;

☒ Das Datum und die Uhrzeit des Eintritts und des Austritts von Besuchern werden aufgezeichnet, und alle Besucher werden von einem Exela-Mitarbeiter beaufsichtigt, es sei denn, ihr Zutritt wurde zuvor genehmigt;

☒ Foto-, Video-, Audio- oder andere Aufnahmegeräte, wie z. B. Kameras in mobilen Geräten, sind nicht erlaubt, es sei denn, ihre Verwendung wurde zuvor genehmigt;

☒ Der physische Schutz gegen Naturkatastrophen, böswillige Angriffe oder Unfälle wird in Übereinstimmung mit nationalen, regionalen oder internationalen Standards ausgelegt und angewendet.

II.Zugriffskontrollen

Relevante ISO-Regelungen: A.9.1.1 Zugangskontrollpolitik; A.9.1.2 Zugang zu Netzwerken und Netzwerkdiensten; A.9.2.2 Bereitstellung von Benutzerzugängen; A.9.2.4 Verwaltung von geheimen Authentifizierungsinformationen der Benutzer; A.9.4.2 Sichere Anmeldeverfahren; A.9.4.3 Passwortverwaltungssystem; A.12.4.1 Ereignisprotokollierung; A.12.4.3 Administrator- und Bedienerprotokolle;

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Die Zugriffskontrollpolitik wird festgelegt, dokumentiert und regelmäßig überprüft. Sie umfasst u. a.: Trennung der Zugriffskontrollrollen (z. B. Zugriffsanfrage), Anforderungen an die formale Autorisierung und regelmäßige Überprüfung der Zugriffsanfragen;

☒ Managementkontrollen und Verfahren zum Schutz des Zugangs zu Netzwerkverbindungen und Netzwerkdiensten, sowie Mittel, die für den Zugang zu Netzwerken und Netzwerkdiensten verwendet werden (z. B. Verwendung von VPN)-sind vorhanden;

☒ Need-to-know- und Need-to-Use-Prinzipien werden eingehalten;

☒ Prozesse für die Vergabe oder den Entzug von Zugriffsrechten und Benutzer-IDs sind vorhanden und beinhalten unter anderem: Sicherstellung, dass Zugriffsrechte nicht aktiviert werden (z. B. durch Dienstanbieter), bevor die Autorisierungsverfahren abgeschlossen sind. Darüber hinaus führt Exela eine zentrale Aufzeichnung der Zugriffsrechte, die einer Benutzer-ID für den Zugriff auf Informationssysteme und -dienste gewährt wurden;

☒ Geheime Authentifizierungsinformationen werden durch einen formalen Verwaltungsprozess kontrolliert;

☒ Wo es die Zugriffskontrollpolitik erfordert, muss der Zugriff auf Systeme und Anwendungen durch ein sicheres Anmeldeverfahren kontrolliert werden;

☒ Passwortverwaltungssysteme sind interaktiv und stellen die Qualität der Passwörter sicher (z. B. werden die Benutzer gezwungen, ihr Passwort in regelmäßigen Abständen zu ändern, und eine Regel gibt vor, Passwörter bei der Eingabe nicht auf dem Bildschirm anzuzeigen).

☒ Ereignisprotokolle, die Benutzeraktivitäten, Ausnahmen, Störungen und Informationssicherheitsereignisse aufzeichnen, werden geführt und bei Bedarf überprüft.

III. Vermögenswertverwaltung und Datenmanagement

Relevante ISO-Regelungen: A.8.1.1 Inventarisierung von Assets; A.8.2.1 Klassifizierung von Informationen; A.8.2.2 Kennzeichnung von Informationen; A.8.3.1 Management von Wechselmedien; A.12.2.1 Kontrollen gegen Malware; A.12.3.1 Informationssicherung;

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Exela identifiziert Vermögenswerte und deren Eigentümer im Lebenszyklus von Informationen, dokumentiert deren Bedeutung und erstellt ein Inventarverzeichnis davon, welches regelmäßig gepflegt wird;

☒ Klassifizierungen und zugehörige Schutzkontrollen für Informationen umfassen geschäftliche sowie gesetzliche Anforderungen für die gemeinsame Nutzung oder Einschränkung von Informationen. Das Schutzniveau wird durch die Analyse von Vertraulichkeit, Integrität und Verfügbarkeit sowie aller anderen Anforderungen an die betrachteten Informationen bewertet. Die Eigentümer von Informationswerten sind für deren Klassifizierung verantwortlich;

☒ Ein geeigneter Satz von Regeln für die Kennzeichnung von Informationen wird in Übereinstimmung mit dem innerhalb von Exela angenommenen Informationsklassifizierungsschema entwickelt und umgesetzt. Die Mitarbeiter sind mit den Kennzeichnungsverfahren vertraut;

☒ Verfahren für die Verwaltung von Wechseldatenträgern gemäß dem Klassifizierungsschema sind implementiert (z. B. werden alle Datenträger in einer sicheren Umgebung gemäß den Herstellerangaben aufbewahrt);

☒ Erkennungs-, Präventions- und Wiederherstellungskontrollen zum Schutz vor Malware werden in Kombination mit einer angemessenen Sensibilisierung der Benutzer implementiert;

☒ Sicherungskopien von Informationen, Software und Systemimages werden regelmäßig gemäß einer vereinbarten Sicherungsrichtlinie getestet;

☒ Die Backups werden an einem entfernten Ort gespeichert, mit ausreichender Entfernung, um bei einer Katastrophe am Hauptstandort nicht beschädigt zu werden.

IV. Kommunikation

Relevante ISO-Regelungen: A.13.1.1 Netzwerk-Kontrollen; A.13.1.3 Segregation in Netzwerken; A.13.2.2 Vereinbarungen zur Informationsübertragung; A.13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Netzwerke werden verwaltet und kontrolliert, um Daten in Systemen und Anwendungen zu schützen (z. B. wird die Verbindung von Systemen zum Netzwerk eingeschränkt und authentifiziert, es werden spezielle Kontrollen eingerichtet, um die Vertraulichkeit und Integrität von Daten zu gewährleisten);

☒ Gruppen von Informationsdiensten, Anwendern und Informationssystemen sind in Netzwerken voneinander getrennt. Der Zugriff wird am Perimeter über ein Gateway (z. B. Firewall) kontrolliert;

☒ Übertragungsvereinbarungen sind vorhanden;

☒ Geheimhaltungsvereinbarungen, die den Schutzbedarf von Exela widerspiegeln, werden identifiziert, regelmäßig überprüft und dokumentiert.

V.Compliance

Relevante ISO-Regelungen: A.18.1.1 Identifikation von anwendbaren Gesetzen und vertraglichen Anforderungen; A.18.1.3 Schutz von Aufzeichnungen; A.18.1.4 Privatsphäre und Schutz von persönlich identifizierbaren Informationen

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Alle relevanten gesetzlichen, behördlichen und vertraglichen Anforderungen sind identifiziert, dokumentiert und auf dem neuesten Stand. Die spezifischen Kontrollen und individuellen Verantwortlichkeiten zur Erfüllung dieser Anforderungen sind ebenfalls definiert und dokumentiert;

☒ Alle Daten werden vor Verlust, Zerstörung, Verfälschung, unbefugtem Zugriff und unbefugter Freigabe in Übereinstimmung mit den gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen geschützt;

☒ Die Privatsphäre und der Schutz personenbezogener Daten werden wie in den einschlägigen Gesetzen und Vorschriften gefordert sichergestellt, wo diese anwendbar sind, insbesondere einschließlich GDPR und UK-GDPR.

Die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls zeitnah wiederherzustellen

I. Störfall-Management

Relevante ISO-Regelungen: A.16.1.2 Meldung von Informationssicherheitsereignissen; A.16.1.3 Meldung von Informationssicherheitsschwächen; A.16.1.4 Bewertung von und Entscheidung über Informationssicherheitsereignisse; A.16.1.5 Reaktion auf Informationssicherheitsvorfälle; A.16.1.7 Sammlung von Beweisen

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Relevante Verfahren und Prozesse zur Sicherstellung einer schnellen, effektiven und ordnungsgemäßen Reaktion auf Informationssicherheitsvorfälle sind implementiert und werden regelmäßig überprüft. Die Klassifizierung und Priorisierung von Vorfällen ist definiert;

☒ Alle Mitarbeiter sind sich ihrer Verantwortung bewusst, Informationssicherheitsvorfälle zu melden und ihnen ist die Existenz von Verfahren zur Meldung und der Kontaktstelle, an die die Vorfälle gemeldet werden sollen, bekannt;

☒ Sammlung, Erfassung und Sicherung von Beweisen in Übereinstimmung mit verschiedenen Medientypen, Geräten und in Abhängigkeiten des Status von Geräten sind definiert.

II. Kontinuitätsmanagement

Relevante ISO-Regelungen: A.12.3.1 Informationssicherung; A.17.1.1 Planung der Kontinuität der Informationssicherheit; A.17.1.2 Implementierung der Kontinuität der Informationssicherheit; A.17.2.1 Verfügbarkeit von Einrichtungen zur Informationsverarbeitung.

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Anforderungen an die Informationssicherheit und die Kontinuität des Informationssicherheitsmanagements in widrigen Situationen (z. B. während einer Krise oder Katastrophe) sind definiert;

☒ Prozesse, Verfahren und Kontrollen sind eingerichtet, dokumentiert, implementiert und werden aufrechterhalten, um das erforderliche Maß an Kontinuität für die Informationssicherheit während einer ungünstigen Situation zu gewährleisten;

☒ Die Kontinuität des Informationssicherheitsmanagements wird u. a. dadurch überprüft, dass die Funktionalität der Prozesse, Verfahren und Kontrollen zur Kontinuität der Informationssicherheit geübt und getestet wird, um sicherzustellen, dass sie mit den Zielen der Kontinuität der Informationssicherheit übereinstimmen;

☒ Wo anwendbar, sollten redundante Informationssysteme getestet werden, um sicherzustellen, dass der Failover von einer Komponente zu einer anderen Komponente wie vorgesehen funktioniert;

☒ Die Sicherungsmedien werden regelmäßig getestet, um sicherzustellen, dass sie im Notfall zuverlässig eingesetzt werden können.

Beurteilung und Bewertung der Wirksamkeit von technischen und organisatorischen Maßnahmen

I. Bewertungen

Relevante ISO-Regelungen: A.18.2.1 Unabhängige Überprüfung der Informationssicherheit; A.18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards; A.18.2.3 Technische Überprüfung der Einhaltung

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Kontrollen, Ziele, Richtlinien, Prozesse und Verfahren werden in geplanten Abständen und/oder bei wesentlichen Änderungen unabhängig voneinander überprüft.

☒ Wir führen zusätzliche Maßnahmen durch, wenn eine Nichteinhaltung festgestellt wird (z. B. Ermittlung der Ursachen für die Nichteinhaltung; Bewertung des Handlungsbedarfs zur Erreichung der Konformität; Umsetzung geeigneter Korrekturmaßnahmen; Überprüfung der ergriffenen Korrekturmaßnahmen zur Überprüfung ihrer Wirksamkeit und Ermittlung von Mängeln oder Schwachstellen);

☒ Technische Compliance-Reviews beinhalten die Überprüfung der operativen Systeme, um sicherzustellen, dass die Hardware- und Software-Kontrollen korrekt implementiert wurden.

Pseudonymisierung und Verschlüsselung von personenbezogenen Daten

Relevante ISO-Regelungen:

A.10.1.1 Richtlinie zum Einsatz kryptographischer Kontrollen; A.10.1.2 Schlüsselverwaltung; A.14.3.1 Schutz von Testdaten; A.18.1.5 Regelung kryptographischer Kontrollen

Exela hat geforderte Maßnahmen umgesetzt, das sind unter anderem:

☒ Richtlinie zum Einsatz kryptografischer Kontrollen zum Schutz von Informationen ist entwickelt und umgesetzt;

☒ Auf der Grundlage einer Risikobewertung wird das erforderliche Schutzniveau unter Berücksichtigung der Art, Stärke und Qualität des erforderlichen Verschlüsselungsalgorithmus ermittelt;

☒ Richtlinien für die Verwendung, den Schutz und die Lebensdauer von kryptografischen Schlüsseln sind entwickelt und implementiert. Kryptografische Algorithmen, Schlüssellängen und Verwendungspraktiken sollten entsprechend der Best Practice ausgewählt werden;

☒ Alle kryptografischen Schlüssel sollten vor Veränderung und Verlust geschützt werden. Darüber hinaus müssen geheime und private Schlüssel vor unbefugter Nutzung sowie Offenlegung geschützt werden. Geräte, die zur Erzeugung, Speicherung und Archivierung von Schlüsseln verwendet werden, sind physisch geschützt;

☒ Alle Testdaten werden sorgfältig ausgewählt, geschützt und kontrolliert;

☒ Die kryptografischen Kontrollen stehen im Einklang mit allen relevanten Vereinbarungen, Gesetzen und Vorschriften.