Anlage 1: Allgemeine TOMs

Allgemeine technische und organisatorische Maßnahmen (TOMs) der Q-FOX® Gruppe

Stand: September 2026

Revision: September 2026

Inhaltsverzeichnis

Präambel

Die nachfolgend beschriebenen allgemeinen „technischen und organisatorischen Maßnahmen" gelten grundsätzlich für die gesamte Q-FOX® Gruppe[1] und werden deshalb hier zentral beschrieben.

Rechtliche Grundlagen

Art. 32 DSGVO

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: (...)"

Art. 28 DSGVO

„Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet (...)"

Umsetzung der Anforderungen aus Art. 28 und 32 DSGVO

Unter Berücksichtigung der Anforderungen der Datenschutz-Grundverordnung stellen wir sicher, dass sämtliche Verarbeitungsprozesse personenbezogener Daten ein angemessenes Schutzniveau gewährleisten. Grundlage hierfür sind insbesondere die Vorgaben aus Art. 28 DSGVO sowie Art. 32 DSGVO, die wir in unseren technischen und organisatorischen Maßnahmen konsequent umsetzen.

Wir wählen und beauftragen ausschließlich solche Auftragsverarbeiter, die nachweislich hinreichende Garantien für Datenschutz und Datensicherheit bieten. Dies umfasst insbesondere die Fähigkeit, geeignete technische und organisatorische Maßnahmen umzusetzen, um eine Verarbeitung im Einklang mit den gesetzlichen Anforderungen sicherzustellen und die Rechte der betroffenen Personen zu schützen.

Gleichzeitig orientieren wir uns bei der Ausgestaltung unserer Sicherheitsmaßnahmen am Stand der Technik, den Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung. Zudem berücksichtigen wir die Eintrittswahrscheinlichkeit und Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen.

Unsere technischen und organisatorischen Maßnahmen werden regelmäßig überprüft, weiterentwickelt und an neue rechtliche, technische und organisatorische Anforderungen angepasst. Ziel ist es, jederzeit ein dem Risiko angemessenes, wirksames und nachvollziehbares Schutzniveau für alle verarbeiteten personenbezogenen Daten sicherzustellen.

1 Sofern in diesem Dokument von Q-FOX® Gruppe die Rede ist, so bezeichnet dies die NOVELLUS Holding AG und alle angehörigen Töchter und Beteiligungen.

Zertifizierungen

Die Q-FOX® Gruppe verfügt über die hier genannten Zertifizierungen, welche die Wirksamkeit der implementierten technischen und organisatorischen Maßnahmen belegen und regelmäßig extern auditiert werden.

TÜVRheinland®
CERTIFIED

Management System
ISO/IEC 27001:2022
ISO/IEC 27017:2015
ISO/IEC 27018:2019

www.tuv.com
ID 9000005059

Rechenzentren

https://www.badencloud.de/rechenzentren/

Die Rechenzentren der Q-FOX® Gruppe bieten höchste Sicherheit, regionale Verfügbarkeit und zertifizierte Infrastruktur für sensible Unternehmensdaten. Sie sind TÜV-geprüft nach DIN EN 50600 Stufe 3 und speichern Daten ausschließlich in Deutschland. Redundante A/B-Stromversorgung, hocheffiziente Kühlung, N_2-Löschanlage und rollenbasierte Zutrittskontrollen schützen vor Ausfällen und unbefugtem Zugang. Die Standorte Lahr und Appenweier sind mehrfach redundant vernetzt und über Glasfaser direkt an DE-CIX und EU-CIX angebunden. Unternehmen profitieren von Colocation, Hosting und Managed Services in einer stabilen, regional verankerten IT-Infrastruktur.

☒ TÜV-geprüft nach DIN EN 50600 Teil 1, 2 und 3 inkl. Verfügbarkeitsklasse 3

☒ Regionaler Öko-Strom, niedriger PUE-Faktor < 1,3

☒ N+1 Redundanz

☒ ISO 27001-konform

☒ Blitzschutz nach DIN EN 62305-5

☒ F90-klassifizierte Schutzräume

☒ 24/7 Video-Überwachung und Sicherheitsdienst

Security Operations Center (SOC)

Unser Security Operations Center (SOC) bildet die zentrale Einheit zur Überwachung und Steuerung der IT-Sicherheitslage. Es kombiniert spezialisierte Fachkräfte, etablierte Prozesse und moderne Technologien, um sicherheitsrelevante Ereignisse kontinuierlich zu analysieren und frühzeitig auf Bedrohungen zu reagieren. Das SOC sammelt und korreliert Daten aus Systemen, Netzwerken und Anwendungen, um potenzielle Risiken zu identifizieren und deren Auswirkungen zu bewerten.

Bei sicherheitsrelevanten Vorfällen führt das SOC koordinierte Maßnahmen zur Eindämmung, Behebung und Wiederherstellung durch, um Betriebsunterbrechungen zu minimieren und Schäden zu verhindern. Durch die permanente Überwachung wird eine 24/7-Reaktionsfähigkeit gewährleistet, die es ermöglicht, Angriffe bereits in frühen Phasen zu erkennen.

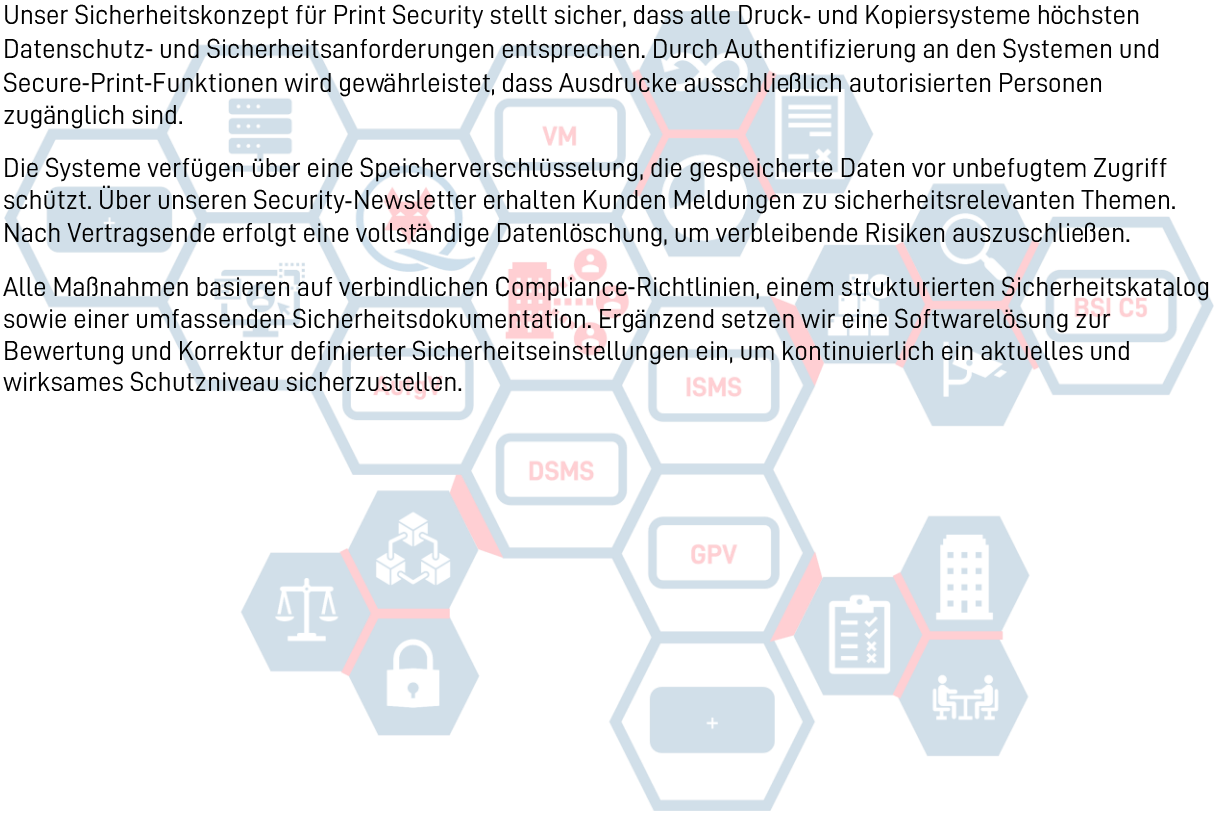
Ziel unseres SOC ist es, die IT-Sicherheitsresilienz kontinuierlich zu stärken, Bedrohungen proaktiv zu managen und ein dauerhaft hohes Schutzniveau für Ihre Systeme und Daten sicherzustellen.

Sicherheitskonzept für Print Security

Unser Sicherheitskonzept für Print Security stellt sicher, dass alle Druck- und Kopiersysteme höchsten Datenschutz- und Sicherheitsanforderungen entsprechen. Durch Authentifizierung an den Systemen und Secure-Print-Funktionen wird gewährleistet, dass Ausdrucke ausschließlich autorisierten Personen zugänglich sind.

Die Systeme verfügen über eine Speicherverschlüsselung, die gespeicherte Daten vor unbefugtem Zugriff schützt. Über unseren Security-Newsletter erhalten Kunden Meldungen zu sicherheitsrelevanten Themen. Nach Vertragsende erfolgt eine vollständige Datenlöschung, um verbleibende Risiken auszuschließen.

Alle Maßnahmen basieren auf verbindlichen Compliance-Richtlinien, einem strukturierten Sicherheitskatalog sowie einer umfassenden Sicherheitsdokumentation. Ergänzend setzen wir eine Softwarelösung zur Bewertung und Korrektur definierter Sicherheitseinstellungen ein, um kontinuierlich ein aktuelles und wirksames Schutzniveau sicherzustellen.



Vertraulichkeit gem. Art. 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. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Gebäudeart: Wirtschaftsgebäude, Massivbau	☒ Schlüsselregelung / Liste
☒ Umfriedung	☒ Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen sowie Regelung der Ausnahmefälle
☒ Überwachung des Gebäudes / Geländes außerhalb der Betriebsstunden	☒ Empfang / Rezeption
☒ Alarmanlage	☒ Besucherbuch (RZ) / Protokoll der Besucher
☒ Bewegungsmelder	☒ Mitarbeiter- / Besucherausweise
☒ Automatisches Zugangskontrollsystem	☒ Tragepflicht von MA-Ausweisen
☒ Biometrische Vereinzelung (**Rechenzentrum**)	☒ Besucher in Begleitung durch Mitarbeiter auf dem Campus / akkreditierte Mitarbeiter für RZ-Zutritt
☒ Chipkarten / Transpondersystem	☒ Zertifikate oder Prüfberichte, die die physische Sicherheit der betroffenen Räumlichkeiten belegen: Verfügbarkeitsklasse 3 basierend auf DIN EN 50600 DIN EN50600 Teil 1 bis 3
☒ Manuelles Schließsystem	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Sicherheitsschlösser	☒ Aufzeichnung / Dokumentation der Anwesenheitszeit von Personen in den Sicherheitsbereichen der Stufe 2 und 3 erstellt: Personenvereinzelung und individuelle Zutrittskontrolle beim Zutritt ab RZ-Geländezugang (3 Sicherheitsbereiche - Gelände, Gebäude, RZ); Besucher-Anmeldung / -Registrierung für alle Gebäude der Q-FOX® Gruppe; Ausweispflicht auf allen Geländen
☒ Server in abschließbaren und abgeschlossenen Räumen bzw. Schränke	☒ Einteilung in Sicherheitszonen / Sperrbereiche (z.B. für Server, Archiv, etc...)
☒ Türen mit Knauf Außenseite	
☒ Videoüberwachung im Rechenzentrum	

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. 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).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz welcher Betriebssysteme: Marktüblich bzw. Auswahl gem. Verwendungszweck	☒ Verwalten von Benutzerberechtigungen
☒ Angemessene Authentisierungsverfahren für jedes informationsverarbeitende System	☒ Verbindliches Verfahren zur Zugangsberechtigungsvergabe
☒ Selbstständige Möglichkeit zur Passwortänderung durch den Benutzer	☒ Nicht mehr benötigte Berechtigungen werden zeitnah entzogen
☒ Login mit Benutzername + Passwort	☒ Erstellen von Benutzerprofilen (an AD gekoppelt)
☒ Nach einem zentral festgelegten, vom Benutzer nicht änderbaren Zeitraum einer Leerlaufverbindung erfolgt eine erneute Authentisierung	☒ Zentrale Passwortvergabe
☒ Login mit biometrischen Daten	☒ Richtlinie „Sicheres Passwort"
☒ Anti-Viren-Software Server	☒ Richtlinie „Löschen / Vernichten"
☒ Anti-Virus-Software Clients	☒ Richtlinie „Clean Desk / Clear Screen"
☒ Zugriffsberechtigung wird vom Auftraggeber individuell ausgelöst	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Firewall Server	☒ Mobile Device Policy
☒ Firewall Clients	☒ Schulung der MA hinsichtlich der Vergabe von sicheren Kennwörtern
☒ Intrusion Detection Systeme	☒ Regelmäßige Kontrolle der Gültigkeit der Berechtigungen
☒ Mobile Device Management	
☒ Einsatz VPN bei Remote-Zugriffen	
☒ Verschlüsselung von Datenträgern	
☒ Verschlüsselung Smartphones	
☒ Alle wesentlichen Administrationstätigkeiten und Transaktionen werden protokolliert	
☒ Alle protokollierten Ereignisse werden zentral gesammelt und archiviert. Protokolle sind vor Manipulation geschützt.	
☒ Automatische Desktopsperre/Bildschirmschoner	
☒ Verschlüsselung von Notebooks / Tablet	

☒ Kontosperrung bei wiederholter Fehleingabe der Zugangsdaten	
☒ Funktions-Accounts	
☒ Single Sign-On	
☒ Externer Remotezugriff (z.B. VPN) inkl. Zwei-Faktor-Authentifizierung	
☒ Lokal verschlossene Schränke	
☒ **Security Operations Center (SOC):** SOC-Prozesse verhindern oder erkennen Datenabflüsse. ▪ Erkennung unautorisierter Zugriffe ▪ Monitoring ungewöhnlicher Datenübertragungen	

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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Akten Schredder (mind. Stufe 3, cross cut)	☒ Einsatz Rollen/Berechtigungskonzepte
☒ Externer Aktenvernichter (DIN 32757)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☒ Kontrolle der Aktivitäten der Systemadministratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten.	☒ Tresor für Sicherungsbänder
☒ Netzwerkmanagement (z.B. VLANs)	☒ Verwaltung Benutzerrechte durch Administratoren.
☒ Trennung von Test- und Produktionsbetrieb (auch bei Schulungen)	☒ Jeder Administrator arbeitet mit seinem eigenen Account
☒ Protokollierung des Zugriffs auf bestimmte sensible Ressourcen	☒ Sichere Aufbewahrung von Datenträgern
☒ Absicherung der Räume, in denen Datenträger aufbewahrt werden (Datenträgerarchiv)	☒ Ordnungsgemäße Vernichtung von Datenträgern (ISO/IEC 21964)
☒ Differenzierte Berechtigungen (z.B. für Lesen, Löschen, Ändern): Im Rahmen der vom Kunden gewünschten Leistungen	☒ Protokollierung der Vernichtung

☒ Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem: Im Rahmen der vom Kunden gewünschten Leistungen	☒ Für jedes informationsverarbeitende System ist ein definiertes Verfahren mit definierten Verantwortlichkeiten zur Vergabe, Veränderung und den Entzug von privilegierten Rechten vorhanden
☒ Zugriff von Benutzern und Wartungspersonal auf Informationen, Applikationen und Dienste beschränkt: Im Rahmen der vom Kunden gewünschten Leistungen	
☒ Mandantentrennung der Systeme und Datenträger für verschiedene Auftraggeber: Trennung je System, Datenträger, oder innerhalb der Applikation	
☒ Einsatz von „Superuser" und es erfolgt ein Monitoring bzw. regelmäßige Kontrollen von Aktivitäten, die mithilfe dieser Benutzerkonten durchgeführt werden	
☒ Funktionelle/personelle Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch): Im Rahmen der vom Kunden gewünschten Leistungen.	

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Klare innerbetriebliche Vorgaben für die Datenerhebung und -verarbeitung
	☒ Falls Tests durchgeführt werden, werden diese nicht aus Originaldaten gewonnen oder diese zuvor anonymisiert

Verschlüsselung

Technische Maßnahme, die eine unbefugte Offenlegung oder Zugang zu personenbezogenen Daten verhindern

Technische Maßnahmen	Organisatorische Maßnahmen
☒ **Verschlüsselung von** ▪ Datenträger ▪ Übermittlung / E-Mail ▪ Datenbanken ▪ Anbindung extern (VPN)	☒ Klare innerbetriebliche Vorgaben für den Einsatz von Verschlüsselung (Richtlinie zur Kryptografie)
☒ Verschlüsselung auf Datenträger (ggf. in verschlossenen Behältern) oder über VPN-Verbindung (risikogerechte Verschlüsselung auf Daten- oder Protokoll-Ebene)	
Eine sichere Passwortverwaltung gewährleistet den Schutz sensibler Daten und Zugänge durch den Einsatz aktueller Verschlüsselungsverfahren nach dem Stand der Technik. Passwörter werden verschlüsselt gespeichert und vor unbefugtem Zugriff geschützt. Der Zugriff auf Passwörter und Benutzerkonten erfolgt über klar definierte Berechtigungs- und Rollenmodelle, sodass nur autorisierte Personen Zugriff erhalten. Regelmäßige Sicherheitsupdates, Mehr-Faktor-Authentifizierung und kontinuierliche Überprüfungen der Sicherheitsmaßnahmen tragen zusätzlich zur Risikominimierung bei. Die eingesetzten Lösungen sind auf aktuelle Sicherheitsanforderungen ausgelegt und werden fortlaufend an technische Entwicklungen angepasst, um Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten Zugangsdaten sicherzustellen.	

Integrität (Art. 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ E-Mail-Verschlüsselung (Transportverschlüsselung)	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen und Zulässigkeit
☒ E-Mail-Anhänge-Verschlüsselung (Inhaltsverschlüsselung)	☒ Dokumentation und Kontrolle (Zeiten, Rückmeldung, Vollständigkeits-/Richtigkeitsprüfung, Protokollierung, Datenträger-Begleitzettel, Lieferschein / Empfangsbestätigung)
☒ Einsatz von VPN	☒ Festlegung der Übermittlungswege, der Übertragungsart und der Datenempfänger, sowie was zu beachten ist und wie im Falle von Fehlern (z.B. Datenträgerverlust) vorzugehen ist
☒ WLAN-Verschlüsselung	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen

☒ Verschlüsselung auf Datenträger (ggf. in verschlossenen Behältern) oder über VPN-Verbindung (risikogerechte Verschlüsselung auf Daten- oder Protokoll-Ebene)	☒ Persönliche Übergabe mit Protokoll
☒ Bereitstellung über verschlüsselte Verbindungen wie SFTP, HTTPS	☒ Fachgerechte Entsorgung von nicht mehr benötigten klassifizierten Dokumenten gem. den aktuellen Anforderungen des Datenschutzes (z.B. DIN-Standard, geeignete Tools)
☒ Nutzung von Signaturverfahren	☒ Löschprotokolle werden geführt und gemäß Vertrag revisionssicher archiviert
☒ Zugriff auf personenbezogene Daten über das Internet mit angemessenen Schutzmaßnahmen (gesonderte Authentifizierung, kontrollierter Zugriff über Firewall, ...)	☒ Regelung zur datenschutzgerechten Vernichtung von Daten bzw. Datenträgern
☒ Speichermedien (Bsp. in Notebook, Drucker, etc...) werden vor ihrer Wiederverwendung sicher gelöscht, so dass eine Wiederherstellung der Informationen nicht möglich ist	☒ Verbot der Nutzung privater Datenträger am Arbeitsplatz
☒ Verwendung der elektronischen Signatur	

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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☒ Einsatz des „Prinzips der minimalen Rechte“	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☒ Protokollierung der Administratorentätigkeiten (Anlegen von Benutzern, Ändern von Benutzerrechten)	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
☒ Security Operations Center (SOC): Das SOC erkennt Manipulationsversuche und unautorisierte Änderungen. ▪ Log-Analyse zur Erkennung von Datenmanipulation ▪ Alarmierung bei verdächtigen Konfigurationsänderungen ▪ Erkennung kompromittierter Accounts ▪ Korrelation von Login-Anomalien	

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Automatische Feuerlöschanlage im Rechenzentrum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Regelmäßig Penetrationstest	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☒ Getrennte Partitionen für Betriebssysteme und Daten der Serversysteme
☒ RAID-System / Festplattenspiegelung	☒ Geregelter Zutritt zum Serverraum
☒ Videoüberwachung Serverraum	☒ Schriftliche Festlegungen für die Aufbewahrungsdauer von Daten
☒ Regelmäßig Lasttests bei Systemänderungen	☒ Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Wer darf wann auf wessen Anforderung Backup-Daten einspielen)
☒ In Hochwassergebieten: Serverräume über der Wassergrenze	Statusinformationen zu den BADEN CLOUD® Diensten: https://www.badencloud-status.de/
☒ Erfolgen regelmäßige Updates	☒ Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (Notfallplan)
☒ Verwendung ausreichender Virenschutzprogramme	
☒ Auslagerung der Datenkopie	
☒ Überspannungsfilter	
☒ Einsatz von Sicherheitssoftware (Virenscanner/Malware-Protection, Firewalls, SPAM-Filter, Verschlüsselungsprogramme)	

☒ Security Operations Center (SOC):

Das SOC überwacht Systeme, erkennt Angriffe frühzeitig und reagiert, bevor Ausfälle entstehen. Typische Aspekte:

- 24/7 Monitoring kritischer Systeme
- DDoS-Erkennung
- Incident Response zur schnellen Wiederherstellung
- Isolierung kompromittierter Systeme
- Dokumentation von Sicherheitsvorfällen

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen, die eine rasche Wiederherstellung bei einem physischen oder technischen Zwischenfall gewährleisten

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Regelmäßige Restores der Backups werden durchgeführt (DASI-Check)	☒ Backup & Recovery-Konzept (ausformuliert)
	☒ Backups werden im Tresor gelagert
	☒ Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (Notfallplan)
	☒ Definierte Vertreterregelung

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

Datenschutz-Management

Maßnahmen, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrens -weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	☒ Bestellter Datenschutzbeauftragter Herr Dr. Rainer Harwardt ORGATEAM Unternehmensberatung GmbH +49 (7805) 918-2553 rainer.harwardt@orgateam.org
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Bestellter Informationssicherheitsbeauftragter Herr Eric Kummer NOVELLUS Integrierte Dienste GmbH +49 (7805) 918-2555 eric.kummer@novellus.de
	☒ Zentrales Compliance-Postfach compliance@qfox.de
	☒ Zentrales Datenschutz-Postfach datenschutz@novellus.de

	☒ Interner Datenschutz- und Informationssicherheitskoordinator Herr Michael Bernhardt NOVELLUS Integrierte Dienste GmbH +49 (7805) 918-1031 michael.bernhardt@novellus.de
	☒ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter (Mindestens jährlich)
	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	☒ Die Verantwortlichkeiten sind geregelt
	☒ Die Schutzbedarfsermittlung hat stattgefunden
	☒ Eine Risikoermittlung hat stattgefunden
	☒ Gegenmaßnahmen bei der Risikoermittlung wurden definiert.
	☒ Interne Datenschutz- und Informationssicherheitsaudits
	☒ Gemeinsame verbindliche Datenschutzleitlinie, sowie Datenschutzkonzept innerhalb der Q-FOX® Gruppe

☒ Software-Lösungen für Datenschutz- und Informationssicherheitsmanagement im Einsatz

Zur Unterstützung des Datenschutz- und Informationssicherheitsmanagements werden innerhalb der Unternehmensgruppe spezialisierte Software-Lösungen eingesetzt. Das Datenschutz-Management-System (DSMS) bildet sämtliche datenschutzrelevanten Prozesse gemäß DSGVO ab und orientiert sich am kontinuierlichen PDCA-Zyklus (Plan, Do, Check, Act). Die Lösung unterstützt unter anderem die Verwaltung von Datenschutzbeauftragten, Verarbeitungstätigkeiten, Auftragsverarbeitungen, Datenschutz-Folgenabschätzungen, Betroffenenrechten, Datenschutzverletzungen sowie Schulungs- und Nachweispflichten. Ergänzend werden Informationssicherheitsprozesse, Risikobewertungen, Maßnahmenmanagement, Audits und Dokumentationen zentral verwaltet. Durch standardisierte Workflows, revisionssichere Dokumentation und regelmäßige Überprüfungen wird die Einhaltung gesetzlicher Anforderungen sowie anerkannter Standards und des aktuellen Stands der Technik unterstützt und nachweisbar sichergestellt.

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB ☒ ISK/DSK ☒ ISB in Sicherheitsvorfälle und Datenpannen
☒ Beweissicherung (Eingrenzung des Zugangs zum kompromittierten System)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

	☒ Dokumentation Schadensverlauf, Geschehnisse und Umstände

☒ Security Operations Center (SOC):

Das SOC überwacht Systeme, erkennt Angriffe frühzeitig und reagiert, bevor Ausfälle entstehen. Typische Aspekte:

- 24/7 Monitoring kritischer Systeme
- DDoS-Erkennung
- Incident Response zur schnellen Wiederherstellung
- Isolierung kompromittierter Systeme

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Einhaltung der Grundsätze der DSGVO - Rechtmäßigkeit - Datenminimierung und Zweckbindung - Speicherbegrenzung - Richtigkeit, Integrität, Vertraulichkeit und Verfügbarkeit
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☒ Risikoermittlung und bei Bedarf durchführen einer Datenschutz-Folgenabschätzung

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen
☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln
☒ Vorherige Prüfung der Auftragnehmer hinsichtlich eines Transfer Impakt Assessments (TIA)
☒ Schriftliche Weisungen an den Auftragnehmer
☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☒ Regelung zum Einsatz weiterer Subunternehmer
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
☒ Führung eines aktuellen Verarbeitungsverzeichnis gem. Art. 30 DSGVO

☒ Regelmäßige Auskunft bez. aktuellen Testaten hinsichtlich Einhaltung des Datenschutzes beim Auftragnehmer (Nachweise zur Einhaltung der TOMs)

NOVELLUS Holding AG
Im Ettenbach 13a
77767 Appenweier-Urloffen

Tel.: +49 7805 918 -0
Fax: +49 7805 918 -200

info@qfox.de
www.qfox.de