Wüstenrot Gruppe
Datenschutz und Cybersecurity

1. Einleitung

In einer zunehmend digitalisierten Welt sind der Schutz personenbezogener Daten und die Sicherung unserer Informations- und Kommunikationstechnologie (IKT)-Infrastruktur von größter Bedeutung. Als Allfinanzdienstleister für Österreich legt die Wüstenrot höchsten Wert auf die Sicherheit und den Datenschutz unserer Kunden und Partner. Dieses Dokument gibt einen Überblick über die strategischen Maßnahmen und Programme, die implementiert wurden, um den höchsten Standards in den Bereichen Datenschutz und Cybersicherheit gerecht zu werden. Dabei verfolgen wir die grundlegenden Schutzziele der Informationssicherheit: Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

1.1. Gesetzliche Rahmenbedingungen:

Neben der EU-Datenschutz-Grundverordnung (DSGVO – Verordnung (EU) 2016/679) und dem Datenschutzgesetz (DSG) gibt es weitere Gesetze, die datenschutzrechtliche Bestimmungen enthalten. Für die Wüstenrot Gruppe sind dies beispielsweise:

- Datenschutzgesetz (DSG)
- Bankwesengesetz (§ 38 BWG)
- Versicherungsvertragsgesetz (§§ 11a ff VersVG)
- Gesundheitstelematikgesetz (GTelG)
- Telekommunikationsgesetz (TKG 2003)

2. Datenschutz

Das Datenschutz- und Sicherheitskonzept der Wüstenrot Gruppe basiert auf klar definierten Richtlinien zur Erfassung, Nutzung, Weitergabe und Speicherung von Benutzerdaten. Wir verarbeiten personenbezogene Daten ausschließlich im erlaubten Umfang und stellen sicher, dass diese Daten nur für die angegebenen Zwecke erhoben und verarbeitet werden. Die Wüstenrot Gruppe erfasst und verarbeitet Daten auf rechtmäßige und transparente Weise, was auch die Einholung entsprechender Einwilligungen erfasst, sofern diese für die Verarbeitung erforderlich sind. Datenübertragungen an Dritte sind streng reguliert und werden nur im notwendigen Umfang durchgeführt.

2.1. Rechte des Betroffenen Auskunftsrecht (Art. 15 DSGVO)

Jeder Betroffene hat das Recht, Auskunft über die zu seiner Person verarbeiteten Daten zu erhalten. Auskunftsbegehren werden auch dann beantwortet, wenn keine Daten über den Betroffenen verarbeitet werden ("Negativauskunft").

2.2. Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung (Art. 16, 17, 18 DSGVO)

Jeder Betroffene hat das Recht, die Löschung bzw. die Richtigstellung bzw. Einschränkung unrichtiger bzw. zu Unrecht verarbeiteter Daten zu verlangen. Jeder dieser Anträge wird zeitnahe bearbeitet und beantwortet.

2.3. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Das Recht auf Datenübertragbarkeit ermöglicht der betroffenen Person, „ihre“ Daten zu erhalten sowie für ihre eigenen Zwecke und für verschiedene Dienste wiederzuverwenden.

Dieses Recht ist nicht an eine Vertragsbeendigung gebunden. Es kann auch in einem aufrechten Vertragsverhältnis geltend gemacht werden.

2.4. Widerspruchsrecht (Art. 21 DSGVO)

Wenn die Verarbeitung personenbezogener Daten auf dem berechtigten Interesse der Wüstenrot Gruppe beruht, hat der Betroffene das Recht, der Verarbeitung zu widersprechen.

2.5. Recht des Kunden auf Information (Art. 13, 14 DSGVO)

Art 13 und 14 DSGVO sieht einen umfangreichen Katalog proaktiver Benachrichtigungen durch den Verantwortlichen vor.

Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person zum Zeitpunkt der Erhebung der Daten mitgeteilt werden. Wenn die Erhebung nicht bei der betroffenen Person erfolgt ist, muss der Verantwortliche diese Informationen innerhalb einer angemessenen Frist erteilen.

3. Cybersecurity-Programm

Die Sicherheit unserer IKT-Systeme und Geschäftsdaten hat für uns oberste Priorität. Unser umfassendes Cybersecurity-Programm umfasst regelmäßige externe und interne Sicherheitsüberprüfungen, einschließlich Vulnerabilitätstests und Penetrationstests, um potenzielle Schwachstellen frühzeitig zu erkennen und zu beheben.

Operative Maßnahmen zur kontinuierlichen Überwachung und schnellen Reaktion auf IKT-Vorfälle und Cyberangriffe sind fest in unseren Betriebsabläufen verankert. Zudem investieren wir kontinuierlich in die Schulung unserer Mitarbeiter im Bereich Cybersicherheit, um ein hohes Bewusstsein und fundierte Kenntnisse im Umgang mit Sicherheitsrisiken zu gewährleisten. Unsere Governance-Strukturen zur Verwaltung der Cybersicherheit stellen sicher, dass alle Maßnahmen koordiniert und effektiv umgesetzt werden, um den Schutz unserer IT-Infrastruktur nachhaltig zu sichern.

Der Chief Information Security Officer (CISO) erstellt mindestens einmal jährlich einen Bericht über die aktuelle Bedrohungslage der Wüstenrot Gruppe und informiert direkt die höchste Managementebene.

3.1. Bedrohungslage

Aufgrund der zunehmenden Digitalisierung vergrößern sich die Angriffsflächen auf jede Art von IKT-Systemen. Die Abhängigkeit von IKT-Systemen nimmt immer mehr zu, weshalb es auch für Cyberkriminelle immer interessanter wird, daraus Kapital zu schlagen. Der CISO der Wüstenrot Gruppe und sein Team überwachen kontinuierlich die Cyber-Bedrohungslage, die auf die Unternehmensgruppe einwirken können. Dadurch kann rasch auf geänderte Bedrohungen reagiert werden. Für die kontinuierliche Beobachtung werden unter anderem

- der ENISA Threat Landscape Report,
- Threat Intelligence des SOC-Dienstleisters,
- Informationen der CISA& aus MITRE ATT&CK,
- Veränderungen in den behördlichen Empfehlungen und Richtlinien von FMA, EBA, EIOPA, NIST und BSI sowie weiteren Behörden und
- relevante Studien, Statistiken und Einschätzungen von namhaften Sicherheitsexperten, Beratungsunternehmen und Marktforschungsinstituten

herangezogen.

3.2. Maßnahmen bei Eintritt eines Cyber-Vorfalls

Cyber Vorfälle stellen IKT-Vorfäll iSd DORA dar. Diese werden im Rahmen standardisierter Prozesse behandelt. Kennzahlen

4. Datenschutz Programm

Unser Datenschutzprogramm ist darauf ausgelegt, den höchsten Standards der regulatorischen Anforderungen zu entsprechen. Regelmäßige Schulungen unserer Mitarbeiter im Bereich Datenschutz stellen sicher, dass alle Beteiligten über aktuelle Bestimmungen und bewährte Praktiken informiert sind. Betroffene Personen haben jederzeit die Möglichkeit, auf ihre Konten zuzugreifen und personenbezogene Informationen zu überprüfen oder Änderungen vorzunehmen. Governance-Strukturen für das Datenschutzmanagement gewährleisten eine effektive Steuerung und Überwachung aller Datenschutzmaßnahmen. Zudem führen wir regelmäßige Datenschutzrisikobewertungen und Audits durch, um potenzielle Risiken frühzeitig zu identifizieren und zu minimieren. Klare und zugängliche Mechanismen ermöglichen es betroffenen Personen, Bedenken hinsichtlich des Datenschutzes unkompliziert zu äußern. Abschließend sorgen unsere Vorkehrungen zur Weitergabe von Risikoinformationen dafür, dass relevante Daten sicher und transparent an die zuständigen Stellen weitergeleitet werden.

5. Business Continuity Management (BCM)

Im Business Continuity Management wird einerseits der Aufbau und die Befähigung der Notfall- und Krisenmanagement Organisation und andererseits eine angemessene Absicherung der kritischen Geschäftsprozesse sichergestellt.

Der Aufbau und die Befähigung der Notfall- und Krisenmanagementorganisation beinhaltet alle Aspekte, um einen funktionierenden Krisenstab zu etablieren, welcher auch im Not- und Krisenfall erreichbar und handlungsfähig ist. Die Wüstenrot Gruppe Österreich kann so auf Schadensereignisse reagieren, unabhängig davon, ob bereits Notfallpläne für die Fortführung von Geschäftsprozessen vorliegen. Im BCM Notfall- und Krisenhandbuch sind alle Aspekte der Notfall- und Krisenbewältigung definiert.

Die implementierte Business Impact Analyse (BIA) und BCM-Risikoanalyse dienen zur angemessenen Absicherung der zeitkritischen Geschäftsprozesse. Diese werden jährlich durchgeführt und hinsichtlich deren Auswirkungen auf das Unternehmen bewertet. Darauf basierend werden zeitkritische Geschäftsprozesse gegen ungeplante Unterbrechungen mittels Notfallplänen (Geschäftsfortführungsplänen) abgesichert und beim Eintreten eines Ereignisses Maßnahmenchecklisten herangezogen, um den operationalen Normalbetrieb rasch wiederherzustellen.

Die Überprüfung des BCMs erfolgt in diversen internen BCM-Schulungen und BCM-Krisenübungen, um einerseits sicherzustellen, dass die Krisenteammitglieder ihre Aufgaben, Pflichten und den Einsatz der Alarmierungs- und der Krisenbewältigungssoftware kennen und anwenden können und andererseits anhand von Übungen zu überprüfen, ob die beschriebenen Strukturen, Notfallpläne und insbesondere die reaktiven Maßnahmen, nicht nur theoretisch, sondern auch praktisch wirksam sind.

Das BCM-Rahmenwerk der Wüstenrot Gruppe umfasst folgende Punkte:

1. Im Zuge der BCM-Risikoanalyse identifizieren und analysieren wir relevante Risikoszenarien für die Wüstenrot Gruppe und bewerten diese hinsichtlich ihrer Eintrittswahrscheinlichkeit und Auswirkungen auf das Unternehmen.

2. Die Wüstenrot Gruppe konzentriert sich auf die geschäftskritischen Prozesse und deren Ressourcen. Die Ressourcen der Geschäftsprozesse werden im Rahmen der Business Impact Analyse (BIA) erhoben. Dabei werden die Zusammenhänge zwischen den geschäftskritischen Prozessen, der notwendigen IT, den kritischen Dienstleistern und anderen Ressourcen identifiziert.

3. Im Rahmen der Notfall- und Wiederanlaufplanung werden szenario-spezifische Maßnahmenchecklisten gemeinsam mit dem jeweiligen Risikoeigner erstellt und Geschäftsfortführungspläne für die Fachbereiche der kritischen Geschäftsprozesse erarbeitet.

4. Im Falle einer Krise (Krisenbewältigung) wird softwaregestützt (Alarmierungs- und Krisenbewältigungssoftware) die Krise bewältigt und die erarbeiteten Unterlagen (Maßnahmenchecklisten, Notfallpläne) zur Unterstützung herangezogen.

6. Schlusswort

Unsere Verpflichtung zu Datenschutz und Cybersicherheit ist ein zentraler Bestandteil unserer Unternehmensphilosophie. Wir setzen alles daran, die höchsten Standards zu erfüllen und kontinuierlich zu verbessern, um das Vertrauen unserer Kunden und Partner nachhaltig zu sichern. Die Wüstenrot ist stolz darauf, ihren Kunden und Partnern ein hohes Maß an Sicherheit und Datenschutz bieten zu können. Durch die kontinuierliche Weiterentwicklung und Anpassung unserer Programme stellen wir sicher, dass wir den regulatorischen Anforderungen stets entsprechen.