Bank:
Name
Adresse
PLZ, Ort
(nachfolgend „Auftraggeber“)

IKT-Dienstleister:
market port GmbH
Splieterstraße 27
48231 Warendorf
(nachfolgend „Auftragnehmer“)

Zusatzvereinbarung zur Informationssicherheit (gem. Art. 24, 25, 30 DORA)

1. Präambel

Die Europäische Union hat eine Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA)erlassen, welche eine finanzsektorübergreifende Regulierung insbesondere der IKT-Sicherheit vorsieht. Die Verordnung gilt ab dem 17.01.2025.

2. Geltungsbereich der Anforderungen

Die im Folgenden beschriebenen Anforderungen beziehen sich ausschließlich auf die von Seiten des Auftragnehmers zu erbringenden vertraglichen Leistungen gemäß der Leistungsbeschreibung des Hauptvertrags und/oder des Angebots. Die Anforderungen an die Informationssicherheit betreffen somit alle Mitarbeiter, Systeme der Informations- und Kommunikationstechnologie (IKT-Systeme) und Einrichtungen des Auftragnehmers, die in eine Verarbeitung der Informationen des Auftraggebers involviert sind.

Die Anforderungen gelten risikoorientiert auch für Dritte („Unterauftragnehmer“ resp. „Subunternehmer“), die der Auftragnehmer mit von ihm zu erbringenden Leistungen nach Maßgabe des „Vertragsgegenstandes bzw. Leistungspflichten market port“ (siehe Hauptvertrag und/oder des Angebots) beauftragt. Der Auftragnehmer hat die Anforderungen gegenüber seinen Unterauftragnehmern vertraglich sicherzustellen.

3. Informationssicherheitsmanagement

Der Auftragnehmer ist verpflichtet, die von ihm gegenüber dem Auftraggeber zu erbringenden Leistungen in sein Informationssicherheitsmanagement einzubeziehen. Im Rahmen seines Informationssicherheitsmanagements trifft der Auftragnehmer unter anderem geeignete technische und organisatorische Maßnahmen, um ein dem Risiko für die Informationssicherheit sowie in Bezug auf die Schutzziele Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten und Informationen des Auftraggebers angemessenes Schutzniveau - wie in den folgenden Absätzen weiter ausgeführt - zu erreichen und zu wahren.
Zudem sind die Eintrittswahrscheinlichkeit und die Schwere eines aus einer möglichen Verletzung der Informationssicherheit resultierenden Risikos, sowie der Stand der Technik, angemessene Standards, wie aktuell der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), für die Informationssicherheit zu berücksichtigen.

MARKET PORTDIGITAL
market port GmbH
Splieterstraße 27
48231 Warendorf
Germany
+49 (0) 2581 949 33 60
info@marketport.de
www.marketport.de

Dies beinhaltet auch Maßnahmen, die darauf ausgerichtet sind, Cyberrisken angemessen zu steuern. Der Auftragnehmer ist dazu verpflichtet, Maßnahmen, Tools, Leit- und Richtlinien für Informationssicherheit vorzuhalten, die ein angemessenes Maß an Sicherheit für die Erbringung der IKT-Dienstleistungen durch den Auftraggeber bieten.

4. Weiterentwicklung des Informationssicherheitsmanagements

Der Auftragnehmer wird die Maßnahmen unter Berücksichtigung des technischen Fortschritts und dem Bekanntwerden neuer Risiken für die Informationssicherheit stetig weiterentwickeln. Wesentliche Änderungen der Maßnahmen, die Einfluss auf die Integrität, Vertraulichkeit, Authentizität oder Verfügbarkeit, der im Kontext der Leistungserbringungen betroffenen Daten und Informationen haben können, wird der Auftragnehmer dem Auftraggeber mitteilen, wobei der Auftraggeber solchen Änderungen nur aus wichtigem Grund widersprechen kann. Als wichtiger Grund gilt insbesondere, wenn begründeter Anlass zu Zweifeln bezüglich des ordnungsgemäßen Schutzes der Informationen des Auftraggebers besteht. Der Auftraggeber kann jederzeit eine aktuelle Beschreibung der vom Auftragnehmer konkret getroffenen technischen und organisatorischen Maßnahmen anfordern.

5. Testen der digitalen operationalen Resilienz

Der Auftragnehmer hat ein übergreifendes Programm für das Testen der digitalen operationalen Resilienz eingesetzt. Der Auftragnehmer berichtet dem Auftraggeber jährlich über die Durchführung der Tests nach dem Programm für das Testen der digitalen operationalen Resilienz.
Sofern der Auftraggeber verpflichtet ist, ein so genanntes „Threat-Led Penetration Testing“ (TLPT) gemäß Artikel 26 und 27 DORA durchzuführen, hat der Auftragnehmer sich daran zu beteiligen und uneingeschränkt mitzuwirken.

Der Auftragnehmer ist dabei zur Wahrung der Vertraulichkeit / Geheimhaltung in Bezug auf die Rahmenbedingungen und Ergebnisses dieser TLPT verpflichtet. Auf Grundlage einer ausdrücklichen Zustimmung des Auftraggebers (Schrift- oder Textform) darf der Auftragnehmer die Ergebnisse zweckgebunden verwenden.

Die Kosten für die Ressourcen des Auftragnehmers teilen sich Auftraggeber und Auftragnehmer.

6. Pflichten zur Information bei und Behandlung von Informationssicherheitsverletzungen

Der Auftragnehmer hat Unregelmäßigkeiten in der Verarbeitung von Informationen, sowie alle sicherheitsrelevanten Vorfälle, die zu einer Verletzung mindestens eines der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität führen (nachfolgend gemeinsam „IKT-bezogener Vorfall“), wie ein nicht geplantes oder unerwartetes Ereignis oder eine Reihe solcher Ereignisse, die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigen und die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten des Auftraggebers unmittelbar oder mittelbar zu gefährden und die Informationssicherheit zu bedrohen, unverzüglich (ohne schuldhaftes Zögern) nach Bekanntwerden zu melden und zu dokumentieren. Der Auftragnehmer hat zur Erkennung und Behandlung von IKT-bezogenen Vorfällen angemessene Systeme, Prozesse und Verantwortlichkeiten implementiert.
Dabei sind die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu berücksichtigen. Der Auftragnehmer unterstützt den Auftraggeber und die zuständigen Behörden bei der Erfüllung der ihr bei einem schwerwiegenden IKT-bezogenen Vorfall obliegenden Pflichten und erteilt ihr die in diesem Zusammenhang erforderlichen weiteren Informationen.

MARKET PORTDIGITAL
market port GmbH
Splieterstraße 27
48231 Warendorf
Germany
+49 (0) 2581 949 33 60
info@marketport.de
www.marketport.de

Die Dokumentation und Meldung eines IKT-bezogenen Vorfalls enthalten mindestens folgende Informationen:

1. eine Beschreibung der Art des IKT-bezogenen Vorfalls, der betroffenen Informationen, der voraussichtlichen Folgen und der von dem Auftragnehmer ergriffenen oder beabsichtigten Maßnahmen zur Behebung der Informationssicherheitsvorfalls und der nachteiligen Auswirkungen
2. Informationen aus der Fehler- bzw. Ursachenanalyse
3. falls zutreffend den durchgeführten Notfallvorsorgemaßnahmen
4. den Namen und die Kontaktdaten des Informationssicherheitsbeauftragten oder eines anderen Ansprechpartners.

Der Auftragnehmer hat zur Erkennung und dem Management von Schwachstellen angemessene Systeme, Prozesse und Verantwortlichkeiten zu implementieren. Der Auftragnehmer hat kritische Schwachstellen zeitnah zu melden. Zudem sind Statistiken und Trends (z.B. Entwicklung der Anzahl relevanter Schwachstellen, Arten von Schwachstellen, Schließung von Schwachstellen in Abhängigkeit der Kritikalität) quartalsweise an den Auftraggeber zu melden. Hierzu vereinbaren Auftraggeber und Auftragnehmer zur Einschätzung der Schwere einer Sicherheitslücke die Einstufung das Common Vulnerability Scoring System (CVSS-Version 3).
Als kritische Schwachstellen werden Vorfälle ab dem CVSS-Wert hochkritisch angenommen. Der CVSS-Wert stellt hierbei lediglich die Basisbewertung der Schwachstelle dar und dient als Indikator zur Einschätzung der Schwere einer Sicherheitslücke (Ersteinwertung):

Einstufung		CVSS-Wert	Zeit zur Behebung
extrem kritisch		unabhängig vom CVSS-Wert	Ausnahmefall, kein Automatismus, nur nach expliziter Einwertung durch Fach- oder übergreifende Einheiten. Sofortige Behebung notwendig.
hoch kritisch		10.0 - 9.0	10 Tage
kritisch		8.9 - 7.0	30 Tage
mäßig kritisch		6.9 - 4.0	60 Tage
wenig kritisch / unkritisch		3.9 - 0.0	90 Tage oder nächstes Update

Abbildung: Einstufung von Schwachstellen nach CVSS-Wert

7. Ermöglichung von uneingeschränkten Kontrollen

In den Fällen, in welchen der Auftraggeber nach dem Hauptvertrag und/oder dem Angebots (bzw. seiner AGB oder Anlagen) das Recht hat bei Unterstützung kritischer oder wichtiger Funktionen, eigene Prüfungen durch ihre Interne Revision oder durch einen von diesem bestellten Prüfer beim Auftragnehmer durchzuführen, zählen zu den etwaig bestellten Prüfern auch das Informationssicherheitsmanagement des Auftraggebers oder dessen Beauftragter bzw. externe Informationssicherheitsprüfer des Auftraggebers.

MARKET PORTDIGITAL

market port GmbH
Splieterstraße 27
48231 Warendorf
Germany

+49 (0) 2581 949 33 60
info@marketport.de
www.marketport.de

8. Kommunikation

Der Auftragnehmer richtet Informationen, Meldungen und Fragen zur Informationssicherheit die Abteilung des Auftraggebers:

E-Mail: _____ Telefon: _____

Zentraler Ansprechpartner auf Seiten des Auftragnehmers und verantwortlich für die Koordination des Notfallmanagements auf Leitungsebene:

Name: Herr Tim Schlautmann
Fachbereich: Projektkoordination, Geschäftsführung
E-Mail: schlautmann@marektport.de
Telefon: +49 175 56 07 520

Ansprechpartner bei weiteren Auskünften:

Name: Herr Serkan Taskin, Legal Counsel, Dipl.-Jur.
Fachbereich: Datenschutzbeauftragter
E-Mail: s.taskin@keyed.de
Telefon: +49 251 21 90

Der Wechsel eines Ansprechpartners wird dem Auftraggeber unverzüglich schriftlich mitgeteilt.

9. Laufzeit

Die Zusatzvereinbarung tritt mit ihrer Unterzeichnung in Kraft und richtet sich nach der Laufzeit des Hauptvertrages und/oder dem Angebot.

10. Sonstige Vereinbarungen / salvatorische Klausel

Soweit in dieser Zusatzvereinbarung nichts Gegenteiliges geregelt ist, gelten die Bedingungen des Hauptvertrages und/oder dem Angebots unverändert fort.
Die Unwirksamkeit einer oder mehrerer Bestimmungen dieser Zusatzvereinbarung berührt die Wirksamkeit der übrigen Bestimmungen nicht. Der Auftraggeber und der Auftragnehmer verpflichten sich für diesen Fall, für die unwirksame eine Bestimmung zu vereinbaren, die dem rechtlich, wirtschaftlich und tatsächlich Gewolltem am nächsten kommt.

Unterschriften

Warendorf, den 02.12.2024 Ort, Datum:

(*Tim Schlautmann, Geschäftsführer - Auftragnehmer*) (Auftraggeber)

MARKET PORTDIGITAL
market port GmbH
Splieterstraße 27
48231 Warendorf
Germany
+49 (0) 2581 949 33 60
info@marketport.de
www.marketport.de