Anlage Informationssicherheit, 08/2024
(soweit eine Auftragsdatenverarbeitung vorliegt)

1. 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. Die Anforderungen an die Informationssicherheit betreffen somit alle Mitarbeiter, IT-Systeme und Einrichtungen des Auftragnehmers, die in eine Verarbeitung der Informationen des Auftraggebers involviert sind.

2. Informationssicherheit

2.1 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 angemessenes Schutzniveau zu gewährleisten. Dabei wird der Auftragnehmer in Bezug auf die Daten und Informationen des Auftraggebers die Schutzziele der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gemäß der angemessenen Standards der Informationssicherheit wahren. Zudem sind die Eintrittswahrscheinlichkeit und die Schwere eines aus einer möglichen Verletzung der Informationssicherheit resultierenden Risikos, sowie der Stand der Technik, angemessene Standards für Informationssicherheit (z.B. IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der international Sicherheitsstandard ISO/IEC 2700X der International Organisation for Standardization) zu berücksichtigen. Dies beinhaltet auch Maßnahmen, die darauf ausgerichtet sind, Cyberrisken angemessen zu steuern.

2.2 Informationssicherheitsstandards

2.2.1 Bei der Festlegung geeigneter technischer und organisatorischer Maßnahmen wird der Auftragnehmer ferner mindestens die Anforderungen gemäß des jeweils aktuellen Sicherheitsstandards ISO/IEC 27001 (inklusive dessen Annex A) einhalten.

2.2.2 Außerdem wird der Auftragnehmer, soweit ihm der Auftraggeber eine Schutzbedarfsfeststellung mitteilt, auf die hierbei definierten Sollvorgaben hinwirken und über eventuelle Abweichungen berichten.

2.2.3 Soweit der Auftragnehmer eine ISO 27001 Zertifizierung oder einen Kontrollgewährleistungsbericht (ISAE 3402, SOC II-Bericht) besitzt, die auch die Leistungserbringung gegenüber dem Auftraggeber abdeckt, werden diese ISO 27001 Zertifizierungen und die Kontrollgewährleistungsberichte (ISAE 3402, SOC II-Bericht) auch in Zukunft aufrechterhalten und auf Anfrage dem Auftraggeber in der jeweils aktuellen Version unentgeltlich zur Verfügung gestellt. Für den Fall, dass der Auftragnehmer die ISO 27001 Zertifizierung oder die Kontrollgewährleistungsberichte (ISAE 3402, SOC II-Bericht) in Zukunft nicht mehr fortführt, diese aberkannt wird oder die Leistungserbringung gegenüber dem Auftraggeber nicht mehr vom Scope der Zertifizierung abgedeckt sein sollte, wird der Auftragnehmer den Auftraggeber hierüber unverzüglich unter Angabe von Gründen informieren.

2.2.4 Änderungen seiner von dem Auftragnehmer zu beachtenden Informationssicherheitsstandards teilt der Auftraggeber dem Auftragnehmer mit einem Vorlauf von sechs Wochen mit.

2.3 Weiterentwicklung des Informationssicherheitsmanagements

Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen entsprechend des technischen Fortschritts und des Bekanntwerdens neuer Risiken für die Informationssicherheit stetig weiterentwickeln. Wesentliche Änderungen der technischen und organisatorischen 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.

2.4 Beachtung von Richtlinien und Arbeitsanweisungen des Auftraggebers

Soweit im Rahmen der Tätigkeiten des Auftragnehmers, die Einhaltung von Richtlinien und/oder fachlichen Arbeitsanweisungen notwendig wird, werden die entsprechenden Richtlinien/Arbeitsanweisungen unmittelbar mit dem Mitarbeiter des Auftragnehmers besprochen und die Einhaltung individuell zwischen den Vertragsparteien bestätigt. Soweit sich offene Punkte ergeben, werde diese ebenfalls individuell zwischen den Vertragsparteien.

2.5 Schulung und Sensibilisierung

Der Auftragnehmer verpflichtet sich, seine Mitarbeiter, die Geschäftsleitung und ggf. eingesetzte Unterauftragnehmer (im Folgenden „eingesetzte Mitarbeiter“) auf Basis eines Schulungs- und Sensibilisierungskonzeptes entsprechend Ihrer Aufgaben und Verantwortung regelmäßig zu Aspekten der Informationssicherheit zu schulen und zu sensibilisieren. Aktuelle Nachweise zum Inhalt der Schulungs- und Sensibilisierungsmaßnahmen sowie zur Teilnahme der eingesetzten Mitarbeiter als auch das zugrunde liegende Schulungs- und Sensibilisierungskonzept werden dem Auftraggeber auf Anfrage zur Verfügung gestellt.

2.6 Threat-Led-Penetration-Testing

Die folgenden Verpflichtungen bestehen nur für diejenigen Auftragnehmer, die zum einen den Auftraggeber bei einer kritischen oder wichtigen Funktion im Sinne des Art. 3 Ziffer 22 der Verordnung (EU) 2022/2554 vom 13.12.2022 (Digital Operational Resilience Act, „DORA“) unterstützen und zum anderen die Verpflichtung des Auftragnehmers sich aus regulatorischen und/oder gesetzlichen Vorschriften ergibt.

2.6.1 Der Auftragnehmer ist dazu verpflichtet, Maßnahmen, Tools, Leit- und Richtlinien für IKT-Sicherheit vorzuhalten, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch den Auftraggeber bieten.

2.6.2 Der Auftragnehmer ist dazu verpflichtet, sich an den in den Artikeln 26 und 27 DORA genannten „Threat-Led Penetration Testing“ (TLPT) des Auftraggebers zu beteiligen und uneingeschränkt daran mitzuwirken. Der Auftragnehmer ist 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.

2.7 Ermöglichung von uneingeschränkten Kontrollen und Zurverfügungstellung von Informationen

Auf Anfrage wird der Auftragnehmer dem Auftraggeber unentgeltlich mindestens einmal jährlich durch geeignete Nachweise belegen, dass er geeignete technische und organisatorische Maßnahmen implementiert hat, um ein dem Risiko für die Informationssicherheit angemessenes Schutzniveau zu gewährleisten. Der Auftraggeber, oder ein von ihm beauftragter Dritter, sowie die zuständigen Behörden haben die uneingeschränkten Zugangs-, Inspektions- und Auditrechte sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort. Der Auftraggeber, oder ein von ihm beauftragter Dritter, ist berechtigt, nach vorheriger Abstimmung mit dem Auftragnehmer zu seinen üblichen Geschäftszeiten ohne Störung des Betriebsablaufs diese Rechte auszuüben. Vertragliche Vereinbarungen, Umsetzungsrichtlinien oder interne Vorgaben des Auftragnehmers, die die tatsächliche Ausübung dieser Rechte behindern oder einschränken, sind unwirksam.

Auftraggeber und Auftragnehmer haben das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind.

Der Auftragnehmer verpflichtet sich zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Auftraggeber oder einem vom Auftraggeber beauftragten Dritten durchgeführt werden. Der Auftragnehmer verpflichtet sich, dem Auftraggeber Einzelheiten zu Umfang und Häufigkeit der vorgenannten Vor-Ort-Inspektionen und Audits sowie dem dabei zu befolgenden Verfahren unverzüglich mitzuteilen.

2.8 Unterauftrag

Der Auftragnehmer ist nur dann berechtigt, einen Dritten (im Folgenden „Unterauftragnehmer“) mit von ihm zu erbringenden Leistungen zu beauftragen, wenn der Auftraggeber der Weiterverlagerung zustimmt und sichergestellt ist, dass der Unterauftragnehmer bei der Erbringung der betreffenden Leistungen ebenfalls geeignete technische und organisatorische Maßnahmen implementiert hat, um ein dem Risiko für die Informationssicherheit angemessenes Schutzniveau zu gewährleisten. Außerdem muss der Unterauftragnehmer vertraglich derart in vollem Umfang in die Pflichten des Auftragnehmers eintreten, dass der Auftraggeber seine vorstehend genannten Rechte nötigenfalls unmittelbar gegenüber dem Unterauftragnehmer geltend machen kann.

Der Auftraggeber ist rechtzeitig vor der Beauftragung eines neuen Unterauftragnehmers oder bei wesentlichen Änderungen eines vorhandenen Vertrages zu informieren. Der Auftraggeber hat das Recht, einer derartigen Beauftragung oder wesentliche Änderung aus wichtigen Gründen zu widersprechen. Als wichtiger Grund gilt insbesondere, wenn begründete Bedenken bezüglich des ordnungsgemäßen Schutzes der Informationen des Auftraggebers bei der Erbringung der Leistungen durch den Unterauftragnehmer bestehen.

2.9 Unverzügliche Meldung und Informationspflichten bei Informationssicherheits-verletzungen

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 „Informationssicherheitsvorfälle“) unverzüglich (ohne schuldhaftes Zögern) nach Bekanntwerden zu melden und zu dokumentieren. Der Auftragnehmer hat zur Erkennung und Behandlung von Informationssicherheitsvorfällen angemessene Systeme, Prozesse und Verantwortlichkeiten implementiert.

Die Dokumentation und Meldung eines Informationssicherheitsvorfalls enthalten mindestens folgende Informationen:

1. eine Beschreibung der Art des Informationssicherheitsvorfalls, der betroffenen Informationen, der voraussichtlichen Folgen und der von dem Auftragnehmer ergriffenen oder beabsichtigten Maßnahmen zur Behebung des Informationssicherheitsvorfalls und der nachteiligen Auswirkungen sowie
2. den Namen und die Kontaktdaten des Informationssicherheitsbeauftragten oder eines anderen Ansprechpartners.

Der Auftragnehmer unterstützt den Auftraggeber und die zuständigen Behörden bei der Erfüllung der ihr bei einem Informationssicherheitsvorfall obliegenden Pflichten und erteilt ihr die in diesem Zusammenhang erforderlichen weiteren Informationen.

Der Auftragnehmer ist verpflichtet, dem Auftraggeber bei einem IKT-Vorfall, der mit dem für den Auftraggeber bereitgestellten IKT-Dienstleistung in Verbindung steht, unentgeltlich Unterstützung zu leisten.

Der Auftragnehmer wird für die Unterstützungsleistungen, sofern ihn an dem IKT-Vorfall kein Verschulden trifft, eine der Vergütung für die vertragliche Hauptleistung entsprechende Vergütung erhalten. Der Auftragnehmer hat den ihm entstandenen Aufwand nachzuweisen.

2.10 Kommunikation

Der Auftragnehmer richtet Informationen und Meldungen zur Informationssicherheit an das Informationssicherheitsmanagement des AUFTRAGGEBERS unter der E-Mail-Adresse: informationssicherheit@teambank.de. Der Auftragnehmer ist verpflichtet, Ansprechpartner zur Informationssicherheit auf Anforderung zu nennen.

2.11 Nachweise

Der Auftragnehmer stellt dem Auftraggeber die der Art des Umfangs entsprechenden Nachweise zur Erbringung von Sicherheitsmaßnahmen und Anforderungen auf Anfrage, mindestens jedoch einmal jährlich zur Verfügung.

Dies umfasst neben eines Kontrollgewährleistungsberichts (ISAE 3402, SOC II-Bericht oder andere geeigneten Dokumentation wie beispielsweise ISO2700x einschließlich SoA) die nachfolgenden Einzelnachweise zu entsprechenden Themen:

Thema	Möglicher Nachweis
Dataklassifizierung und -handhabung	• Zustimmung/Bestätigung zu den Standards für die Klassifizierung und Handhabung von Daten seitens der Team Bank werden verstanden und befolgt. (Dies könnte z. B. ein vereinbarter Kontrollplan oder ähnliches sein)

	• Eine spezifische Bestätigung zur Verschlüsselung von Daten im Ruhezustand und während der Übertragung.
Antimalware	• Bestätigung, dass die Infrastruktur und Server der Bank durch die Antimalware-Lösung des Lieferanten abgedeckt sind.
Logging und Überwachung	• Übersicht über überwachte und protokollierte Ereignisse • Bestätigung, dass Protokollierungsinformationen 6 Monate lang verfügbar sind und mindestens 18 Monate aufbewahrt werden, einschließlich eines robusten Backup-Konzepts. • Bestätigung, dass streng vertrauliche Daten nicht protokolliert werden. • Bestätigung, dass eine monatliche Berichterstattung über SIEM-Ergebnisse erfolgt, einschließlich Anzahl und Typ der aktiv in SIEM berichtenden Verlustquellen, Anzahl protokollierter Ereignisse, Anzahl ausgelöster Vorfälle oder Warnungen, Anzahl der gemeldeten Sicherheitsvorfälle.
Netzwerk	• Dokumentation von Netzwerk-Intrusionserkennungs- und Netzwerk-Intrusionspräventionssystemen (NIDs/NIPs) und DDoS-Kontrollen.
Benutzerzugriffsverwaltung	• Dokumentation darüber, wie Passwörter gehasht und sicher gespeichert werden. • Übersicht über Rollen und Benutzerzugriffsrechte für die TeamBank eingesetzten Systeme.