Hamburg Commercial Bank

Ansatz der HCOB zu Datenschutz und Informationssicherheit

Dieses Dokument bietet eine umfassende Übersicht über den Ansatz der HCOB in Bezug auf Datenschutz und Informationssicherheit. Es beschreibt die verschiedenen Konzepte und Richtlinien, die entwickelt wurden, um die wesentlichen Auswirkungen und Risiken in diesen Bereichen zu steuern. Diese Ansätze sind in der schriftlich fixierten Ordnung der HCOB verankert und dienen als Leitfaden für den sicheren und verantwortungsvollen Umgang mit Daten.

Digitale Kompetenz

Digitalisierung und Innovation gehören zu den wichtigsten Erfolgsfaktoren der Bank. So hat die HCOB in den letzten Jahren eine umfassende IT-Transformation vorgenommen und ist von Onsite-Systemen auf cloudbasierte Lösungen umgestiegen. Damit kann die Bank ihre Prozesse optimieren, Kosten minimieren und sich im digitalen Zeitalter zukunftsorientiert aufstellen.

IT- und Datensicherheit

Die Sicherstellung des Datenschutz und der Informationssicherheit ist für die HCOB wesentlich, um Kund:innendaten sowie den Ruf der HCOB zu schützen und damit die Geschäftstätigkeit zu gewährleisten. Wichtige Vorgaben für IT-bezogene Aktivitäten der Mitarbeitenden umfassen die Richtlinien und Regelungen zum Datenschutz, das Managementsystem für Informationssicherheit (ISMS) mitsamt der Informationssicherheitsrichtlinie sowie die IT-Prozesse inkl. der Prozesse und Regelungen zum IT-Sicherheitsmanagement und zum Identity & Access Control Management. So gibt es spezifische technische Maßnahmen, wie u.a. den Einsatz von Data Loss Prevention, Phishingfilter und Verschlüsselungstechniken, um ein hohes Maß an Datenschutz und Informationssicherheit zu erreichen. Die Anforderungen an die Informationssicherheit der HCOB gelten auch und insbesondere für externe Dienstleister (Third Parties), die sich auf die Einhaltung der IT- und Datensicherheit verpflichten müssen und entsprechend hinsichtlich deren Einhaltung einem regelmäßigen Monitoring unterliegen.

Organisation der Informationssicherheit

Im Rahmen der Informationssicherheit, hat die HCOB eine Sicherheitsorganisation eingerichtet, die die gesetzlichen und aufsichtsrechtlichen Anforderungen erfüllt und die ISO 27001 (internationaler Standard für Informationssicherheitsmanagement) als führenden Sicherheitsstandard anwendet. Zudem wurde ein Information Security Officer ernannt. Dieser berichtet in seiner Funktion direkt an den Risiko-Vorstand, um die Unabhängigkeit dieser Funktion gemäß den aufsichtsrechtlichen Anforderungen zu gewährleisten. Er berichtet darüber hinaus dem Gesamtvorstand regelmäßig (mindestens vierteljährlich) bzw. anlassbezogen über den Stand der Informationssicherheit in der Bank.

Managementsystem für Informationssicherheit (ISMS)

Das ISMS ist ein Schlüsselelement der Informationssicherheit in der Organisation. Grundlegende Anforderungen an die Informationssicherheit, die u. a. Teile der MaRisk, der bankaufsichtsrechtlichen Anforderungen an die IT (BAIT) und der ISO 27001 umfassen und ab Januar 2025 insbesondere auf DORA (Digital Operational Resilience Act) ausgerichtet sein werden, sind in der Informationssicherheitsrichtlinie definiert, die Teil der schriftlich fixierten Ordnung ist. Um festzustellen, ob diese Anforderungen ordnungsgemäß definiert und wirksam umgesetzt wurden, werden regelmäßig risikoorientierte Assessments und Kontrollen der Informationssicherheit geplant und durchgeführt. Diese Assessments und Kontrollen werden intern sowie bei dritten Parteien (z.B. externen Geschäftspartner:innen) durchgeführt. Festgestellte Mängel werden bewertet und entsprechende Abhilfemaßnahmen mit den zuständigen Abteilungen bzw. Partner:innen vereinbart.

Datenschutz

Die Verantwortung für den Datenschutz liegt beim Vorstand, der eine Datenschutzorganisation eingerichtet hat, um die Einhaltung der Datenschutzvorschriften umzusetzen und zu gewährleisten. Hierbei beachtet die HCOB nicht nur die datenschutzkonforme Verarbeitung, sondern auch die möglichst zügige Löschung nicht mehr benötigter Daten. Ein wichtiger Bestandteil der Datenschutzorganisation ist der betriebliche Datenschutzbeauftragte (DSB), der entsprechende Aufgaben unabhängig und nach eigenem Ermessen wahrnimmt und direkt dem Vorstand unterstellt ist. Der DSB überwacht die Einhaltung der Datenschutzbestimmungen, insbesondere der europäischen Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) sowie anderer Datenschutzbestimmungen und branchenspezifischer Anforderungen. Zu den Aufgaben gehört zudem neben dem Identifizieren möglicher Schwachstellen, dass der DSB beratend tätig ist und die HCOB, ihre Mitarbeitenden sowie Dienstleister:innen, die im Auftrag der Bank personenbezogene Daten verarbeiten, über Ansatzpunkte für Änderungen oder Verbesserungen informiert. Daten werden stets nur für die vereinbarten Geschäftszwecke verarbeitet und sofern erforderlich weitergegeben. Neue Anforderungen, die sich aus Gesetzesänderungen oder Gerichtsurteilen ergeben, werden unverzüglich umgesetzt und in den betroffenen Prozessen angewendet.

Risikomanagement hinsichtlich externer Dienstleister im Bereich IT

Die HCOB verwaltet und überwacht ihre externen IT-Dienstleister streng, da die IT- und Datensicherheit ein wichtiger Bestandteil des Bankgeschäfts ist und streng reguliert wird. Drittanbieter werden auf der Grundlage einer umfassenden Due Diligence Prüfung ausgewählt, die sich auf ihre Fachkompetenz und Glaubwürdigkeit (Integrität) in ihrem jeweiligen Tätigkeitsbereich konzentriert. Zu diesem Zweck verfügt die HCOB über umfassende Richtlinien in Form von Fragebögen zur Überprüfung externer Dienstleister, die als Teil des Vertragsprozesses erforderlich sind. Diese detaillierten (und anbietergruppenspezifischen) Fragebögen befassen sich intensiv mit den Aufgaben und Verantwortlichkeiten des Dienstleisters, insbesondere mit Fragen zur Gewährleistung der Daten- und Informationssicherheit. Mögliche weitere Unteraufträge des Drittanbieters sind genehmigungspflichtig und unterliegen den gleichen Richtlinien und Anforderungen. Die strukturierten Fragebögen und Listen sind (je nach zu beauftragender Dienstleistung) in Gruppen zusammengefasst: Hardware- und Softwarespezifikationen; Richtlinien zur Gewährleistung der Sicherheit der Datenverarbeitung (inkl. Passwortmanagement & Malware-Sicherheit) und Datenspeicherung (Archive, inkl. Anerkennung rechtlicher Rahmenbedingungen & Anforderungen) bis hin zu; Verantwortlichkeiten aller an Projekten beteiligten externen Mitarbeiter. Der Inhalt des Fragebogens basiert, abgeleitet aus der ISO 27001, auf der Informationssicherheitsrichtlinie. Die Einhaltung der Anforderungen wird regelmäßig überprüft und Verstöße werden sanktioniert. Die oben genannten Richtlinien decken alle Aktivitäten der HCOB mit externen IT- und Datenmanagement-Dienstleistern ab.

Sensibilisierung der Mitarbeiter:innen

Eine weitere wichtige Aufgabe der Informationssicherheit sind kontinuierliche Maßnahmen zur Sensibilisierung der Mitarbeitenden der HCOB für die Risiken von Cyberangriffen und Verstößen gegen die Schutzziele der Bank. Zu diesem Zweck nehmen alle Mitarbeiter:innen u.a. regelmäßig verpflichtend an Online-Schulungen zur Informationssicherheit und zum Datenschutz teil. Zudem werden die Mitarbeitenden mit gezielten Maßnahmen über aktuelle Bedrohungen und entsprechende Handlungsoptionen aufgeklärt, etwa die Auswirkungen von leichtsinnigem Verhalten.