Anlage Informationssicherheit, 11/2021

1. Informationssicherheitsmanagement

Der AUFTRAGNEHMER ist verpflichtet, ein Informationssicherheitsmanagement zu betreiben und die von ihm gegenüber dem AUFTRAGGEBER zu erbringenden Leistungen in sein Informationssicherheitsmanagement einzubeziehen. Dies umfasst insbesondere Informationen des AUFTRAGGEBERS, die der AUFTRAGNEHMER verarbeitet oder speichert, informationsverarbeitende Systeme, die der AUFTRAGNEHMER für den AUFTRAGGEBER betreibt, sowie Informationen und informationsverarbeitende Systeme des AUFTRAGNEHMERS, die für die Leistungserbringung gegenüber dem AUFTRAGGEBER erforderlich sind.

Bei der Ausgestaltung und kontinuierlichen Weiterentwicklung des Informationssicherheitsmanagements beachtet der AUFTRAGNEHMER den Stand der Technik sowie aktuelle Risiken für die Informationssicherheit und orientiert sich an gängigen Standards wie bspw. dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder der ISO/IEC 2700X der International Organization for Standardization.

2. Maßnahmen zum Schutz der Informationssicherheit

Im Rahmen seines Informationssicherheitsmanagements trifft der AUFTRAGNEHMER ge-eignete Maßnahmen, um ein dem Risiko für die Informationssicherheit angemessenes Schutzniveau bezüglich der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität mit Hinblick auf die Leistungserbringung für den AUFTRAGGEBER zu gewährleisten. Dabei sind die Eintrittswahrscheinlichkeit und mögliche Schadenshöhe aus einer Verletzung der Informationssicherheit zu berücksichtigen. Der AUFTRAGNEHMER wird die Maßnahmen entsprechend dem technischen Fortschritt und dem Bekanntwerden neuer Risiken für die Informationssicherheit stetig weiterentwickeln. Der AUFTRAGGEBER kann jederzeit eine aktuelle Beschreibung der vom AUFTRAGNEHMER konkret getroffenen Maßnahmen anfordern. Der AUFTRAGNEHMER wird diese Beschreibung dem AUFTRAGGEBER kostenfrei zur Verfügung stellen.

3. Bereitstellung von Informationen

Der AUFTRAGNEHMER wird dem AUFTRAGGEBER mindestens einmal jährlich durch geeignete Nachweise belegen, dass er ein Informationssicherheitsmanagement und wirksame Maßnahmen zum Schutz der Informationssicherheit gemäß dieser Vereinbarung implementiert hat. Der AUFTRAGNEHMER stellt die Nachweise dem AUFTRAGGEBER kostenfrei zur Verfügung. Als Nachweise können beispielsweise Richtlinien, Arbeitsanweisungen, Prüfberichte oder Zertifikate dienen.

Wird eine Maßnahme des AUFTRAGNEHMERS zum Schutz der Informationssicherheit verletzt und führt dies zu einem Risiko für die Leistungserbringung gegenüber dem AUFTRAG-GEBER, hat der AUFTRAGNEHMER den AUFTRAGGEBER unaufgefordert und unverzüglich zu benachrichtigen und Schritte zur Beseitigung der Verletzung in einer der jeweiligen Verletzung angemessenen Form und Frist zu ergreifen.

Der AUFTRAGNEHMER wird den AUFTRAGGEBER zudem unverzüglich über Beanstandungen mit Relevanz für die Informationssicherheit durch eine Aufsichtsbehörde, eine Revision oder in sonstigen Prüfberichten benachrichtigen, sofern diese die Leistungserbringung für den AUFTRAGGEBER betreffen.

4. Ermöglichung von Kontrollen (Prüfrechte)

Falls die von dem AUFTRAGNEHMER vorgelegten Nachweise zu seinem Informationssicherheitsmanagement oder zu den Maßnahmen zum Schutz der Informationssicherheit nicht geeignet sind oder der AUFTRAGGEBER Anlass hat, die Wirksamkeit der Maßnahmen zu prüfen, so sind der AUFTRAGGEBER oder von ihm benannte Prüfer berechtigt, im erforderlichen Umfang vor Ort oder remote Prüfungen beim AUFTRAGNEHMER durchzuführen. Die Prüfungen erfolgen nach vorheriger Abstimmung mit dem AUFTRAGNEHMER zu seinen üblichen Geschäftszeiten ohne Störung des Betriebsablaufs. Dem AUFTRAGGEBER

bzw. den von ihm benannten Prüfern ist dabei eine Einsichtnahme in die Dokumentationen von Maßnahmen zu ermöglichen und uneingeschränkter Zugang zu allen Informationen zu gewähren, die für die Erfüllung ihrer Aufgaben erforderlich sind. Hierzu zählen ein Zutritts-, Zugangs- und Einsichtsrecht zu den relevanten Gebäuden und Räumen, Unterlagen, Daten und Systemen sowie ein Recht gegenüber Mitarbeitern des AUFTRAGNEHMERS, notwendige Auskünfte einzuholen und Unterlagen anzufordern. Der AUFTRAGNEHMER hat das Recht, die Kontrollen zu beaufsichtigen. Er ist dem AUFTRAGGEBER gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

5. Subunternehmer

Der AUFTRAGNEHMER ist nur dann berechtigt, einen Subunternehmer mit von ihm für den AUFTRAGGEBER zu erbringenden Leistungen zu beauftragen, wenn sichergestellt ist, dass der Subunternehmer bei der Erbringung der betreffenden Leistungen ebenfalls gleichwertige Maßnahmen zum Schutz der Informationssicherheit einhält. Außerdem muss der Subunternehmer vertraglich derart in vollem Umfang in die Pflichten des AUFTRAGNEHMERS eintreten, dass der AUFTRAGGEBER seine in dieser Vereinbarung genannten Rechte nötigenfalls unmittelbar gegenüber dem Subunternehmer geltend machen kann.

Der AUFTRAGGEBER ist vor der Beauftragung eines Subunternehmers zu informieren. Der AUFTRAGGEBER hat das Recht, solch einer Beauftragung aus wichtigen Gründen zu widersprechen. Als wichtiger Grund gilt insbesondere, wenn begründete Bedenken bestehen, dass kein angemessenes Schutzniveau der Informationssicherheit mit Hinblick auf die Leistungs-erbringung für den AUFTRAGGEBER gegeben ist.

6. Unverzügliche Meldung und Informationspflichten bei Informationssicherheitsvorfällen

Als Informationssicherheitsvorfall wird jedes Ereignis bezeichnet, das eine Verletzung eines der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität oder Authentizität von Informationen oder informationsverarbeitenden Systemen darstellt oder bei dem eine solche Verletzung nicht ausgeschlossen werden kann. Der AUFTRAGNEHMER muss alle Informationssicherheitsvorfälle, die die Leistungserbringung gegenüber dem AUFTRAGGEBER betreffen, erkennen und behandeln können. Der AUFTRAGGEBER ist über diese Informationssicherheitsvorfälle zu informieren. Die Meldung an den AUFTRAGGEBER muss unverzüglich erfolgen, nachdem dem AUFTRAGNEHMER der Informationssicherheitsvorfall bekannt wurde.

Jeder Informationssicherheitsvorfall, der die Leistungserbringung gegenüber dem AUFTRAGGEBER betrifft, ist vom AUFTRAGNEHMER zu dokumentieren. Die Dokumentation und Meldung eines Informationssicherheitsvorfalls enthält mindestens folgende Informationen:

1. eine Beschreibung der Art des Vorfalls und der betroffenen Informationen;
2. den Namen und die Kontaktdaten des Informationssicherheitsbeauftragten oder eines anderen verantwortlichen Ansprechpartners;
3. eine Beschreibung der voraussichtlichen Folgen für den AUFTRAGGEBER;
4. eine Beschreibung der ergriffenen oder beabsichtigten Schritte zur Behebung des Informationssicherheitsvorfalls und der Schritte zur Beseitigung seiner nachteiligen Auswirkungen.

Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Erfüllung der ihm bei einem Informationssicherheitsvorfall obliegenden Pflichten und erteilt ihm die in diesem Zusammenhang erforderlichen weiteren Informationen.

7. Kommunikation

Der AUFTRAGNEHMER richtet Informationen und Meldungen zur Informationssicherheit an das Informationssicherheitsmanagement des AUFTRAGGEBERS unter der E-Mail-Adresse: informationssicherheit@teambank.de

Bei unmittelbarer Gefährdung des AUFTRAGGEBERS, ist der Manager on Duty des AUFTRAGGEBERS unter der Rufnummer +49 (0) 911 5390 1100 zu kontaktieren.

Der AUFTRAGNEHMER ist verpflichtet, Ansprechpartner zur Informationssicherheit zu benennen.