Verpflichtung zur Lieferantenkontrolle (Supplier Control Obligation, SCO)

Management Kontrollvorgaben –

Informationen, Cyber- und physische Sicherheit, Technologie, Wiederherstellungsplanung, Datenschutz, Datenmanagement und EUDA

MC 1.0 – Governance und Verantwortlichkeit

Der Lieferant muss über ein etabliertes und durchgängiges Branchenstandardsystem für Informationstechnologie, IT-Sicherheit, physische Sicherheit, Wiederherstellungsplanung, Datenmanagement und Governance für die Verwaltung personenbezogener Daten (Datenschutz) (NIST, ISO/IEC 27001, COBIT, BS10012, SSAE 18, ITIL) oder ähnliche Standardrahmenkonzepte nach bewährten Branchenverfahren verfügen, um sicherzustellen, dass die Sicherheitsvorkehrungen oder Gegenmaßnahmen ihrer Prozesse, Technologien und physischen Umgebung als wirksam gelten. Ein gut strukturiertes, unternehmensweites Governance-Programm muss sicherstellen, dass die Kernkonzepte Verfügbarkeit, Integrität und Vertraulichkeit durch angemessene Kontrollen unterstützt werden. Die Kontrollen müssen so konzipiert sein, dass die Risiken des Verlusts, der Unterbrechung oder der Korruption von Informationen gemindert oder verringert werden; der Lieferant muss sicherstellen, dass die Anforderungskontrollen von Barclays wirksam angewendet werden und funktionieren, um die Services zu schützen, die Barclays erbracht werden.

Es muss ein Governance-Rahmenkonzept entwickelt werden, das administrative, technische und physische Sicherheitsvorkehrungen zum Schutz von Ressourcen und Informationen/Daten vor versehentlichem und/oder vorsätzlichem Verlust oder ebensolcher Offenlegung, Veränderung oder Vernichtung, Diebstahl, unangemessener Nutzung oder Missbrauch sowie unberechtigtem Zugriff, unberechtigter Nutzung oder Offenlegung umfasst.

Das Governance- und Verantwortlichkeitsprogramm muss unter anderem folgende Schwerpunkte enthalten:

- Richtlinien für Governance – Ein Satz von Richtlinien für Governance muss definiert, vom Management genehmigt, veröffentlicht, den Mitarbeitern des Lieferanten und den relevanten Parteien mitgeteilt und gepflegt werden.
    - Richtlinien, Verfahren, Standardprogramme, mit denen die umzusetzenden Richtlinien und -standards effektiv erstellt und implementiert werden können sowie ihre Wirksamkeit kontinuierlich gemessen werden kann.
    - Ein umfassendes Governance-Programm mit klarer Führungsstruktur und Kontrolle auf Managementebene, um eine Kultur von Verantwortung und Awareness zu schaffen.
    - Eine kontinuierliche Kommunikation genehmigter Richtlinien und Verfahren im gesamten Unternehmen.
    - Anpassung von Richtlinien und Praktiken, Datensicherheit durch Design und andere Kontrollen an gesetzliche Anforderungen, um sicherzustellen, dass Richtlinien und Prozesse wirksam implementiert werden
- Überprüfung und Überwachung von Governance-Richtlinien und -Mechanismen sowie Kontrollen, um sicherzustellen, dass Richtlinien und Prozesse wirksam implementiert werden
- Die Richtlinien für alle Domänenbereiche sind in geplanten Intervallen oder bei erheblichen Änderungen zu überprüfen, um ihre fortwährende Eignung, Hinlänglichkeit und Wirksamkeit zu gewährleisten.
    - Sicherstellung, dass Richtlinien und Verfahren/Standards routinemäßig überprüft werden (mindestens einmal jährlich oder zu einem Zeitpunkt, an dem wesentliche Änderungen vorgenommen werden, je nachdem, welcher Zeitpunkt früher eintritt).
- Rollen und Verantwortlichkeiten – Verantwortlichkeiten sind zu definieren und zuzuweisen.

  - Verantwortung und Zuständigkeit der einzelnen Mitarbeiter für Informationsressourcen
  - Ernennung erfahrener und entsprechend qualifizierter Personen, mit denen Barclays in Bezug auf physische Sicherheit und Gebäudesicherheit, Informations- und Cyber-Sicherheit sowie Verwaltung personenbezogener Daten (Datenschutz) zusammenarbeiten kann, und Sicherstellung, dass Richtlinien und Praktiken, Datenschutz durch Design und andere Kontrollen wirksam implementiert und überwacht werden.
  - Der Lieferant muss die Rollen und Verantwortlichkeiten des Personals koordinieren und aufeinander abstimmen, das die Effektivität von Kontrollen mit internen und Unterauftragnehmern/Unterauftragsverarbeitern implementiert, verwaltet und überwacht.
- Der Lieferant muss eine sichere Infrastruktur und ein Kontrollrahmenkonzept einrichten, um die Organisation vor etwaigen Bedrohungen zu schützen (einschließlich Cyber-Sicherheit).
- Unabhängige Prüfung und Bewertung – Der Ansatz des Lieferanten für die Verwaltung und Durchführung des Informationssicherheitsarchitekturprogramms (d. h. Kontrollziele, Kontrollen, Richtlinien, Prozesse und Verfahren für die Informationssicherheit) ist in geplanten Abständen oder bei erheblichen Änderungen unabhängig zu überprüfen.
  - Mindestens einmal jährlich müssen unabhängige Prüfungen und Beurteilungen durchgeführt werden, um sicherzustellen, dass das Unternehmen eventuelle Nichtkonformitäten mit etablierten Richtlinien, Standards, Verfahren und Compliance-Verpflichtungen behebt.
  - Informationssysteme werden mindestens jährlich auf die fortgesetzte Übereinstimmung mit den Informationssicherheitsrichtlinien und -standards des Unternehmens überprüft.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Eine Informationssicherheitsrichtlinie für Cloud-Computing sollte als themenspezifische Richtlinie des Cloud-Service-Kunden definiert werden. Die Informationssicherheitsrichtlinien des Cloud-Service-Kunden für Cloud-Computing sollten mit den akzeptablen Sicherheitsrisiken des Unternehmens für seine Informationen und andere Ressourcen vereinbar sein. Bei der Definition der Informationssicherheitsrichtlinie für Cloud-Computing sollte der Cloud-Service-Kunde Folgendes berücksichtigen:

- Die in der Cloud-Computing-Umgebung gespeicherten Informationen können dem Zugriff und der Verwaltung des Cloud-Dienstanbieters unterliegen.
- Ressourcen, z. B. Anwendungsprogramme, können in der Cloud-Computing-Umgebung verwaltet werden.
- Prozesse können auf einem mehrmandantenfähigen, virtualisierten Cloud-Service ausgeführt werden.
- Die Nutzer von Cloud-Diensten und der Kontext, in dem sie den Cloud-Dienst nutzen.
- Die Cloud-Service-Administratoren mit privilegiertem Zugriff auf den Cloud-Service-Kunden.
- Die geografischen Standorte der Organisation des Cloud-Serviceproviders und die Länder, in denen der Cloud-Serviceprovider die Daten des Cloud-Service-Kunden speichern kann (einschließlich temporärer Speicherung).

Die entsprechende Sicherheitsrichtlinie des Cloud-Service-Kunden sollte den Cloud-Serviceprovider als einen Lieferantentyp kennzeichnen und gemäß der Sicherheitsrichtlinie verwalten. Dies sollte darauf abzielen, Risiken zu mindern, die durch den Zugriff und die Verwaltung der Daten von Cloud-Service-Kunden im Zusammenhang mit Cloud-Serviceprovider entstehen.

Der Cloud-Service-Kunde sollte die relevanten Gesetze und Vorschriften der Länder berücksichtigen, die für den Cloud-Serviceprovider gelten, zusätzlich zu denen, die für den Cloud-Service-Kunden gelten. Der Cloud-Service-Kunde muss den Nachweis dafür einholen, dass der Cloud-Serviceprovider die relevanten Vorschriften und Standards erfüllt, die für das Geschäft des Cloud-Service-Kunden erforderlich sind. Die von externen Prüfern ausgestellten Bescheinigungen/Zertifikate können auch als ein solcher Nachweis dienen.

Darüber hinaus muss der Lieferant Barclays schnellstmöglich schriftlich informieren, wenn der Lieferant Gegenstand einer Fusion, einer Übernahme oder eines sonstige Eigentümerwechsels wird.

MC 2.0 – Risikomanagement

Der Lieferant muss ein Programm zum Risikomanagement aufstellen, mit dem Risiken innerhalb der vom Lieferanten kontrollierten Umgebung effektiv beurteilt, gemindert und überwacht werden können.

Das Risikomanagementprogramm muss unter anderem folgende Schwerpunkte enthalten:

- Der Lieferant muss über ein Risikomanagement-Rahmenkonzept verfügen (z. B. Informations-, Cyber-, physische, Technologie-, Daten- und Wiederherstellungsplanung). Das Rahmenkonzept muss von der zuständigen stelle (z. B. dem Vorstand oder einem seiner Ausschüsse) genehmigt werden. Dieses muss in die allgemeine Geschäftsstrategie und das Rahmenkonzept zum Risikomanagement eingebunden werden.
- Angepasst an den Risikorahmen, müssen mindestens ein Mal pro Jahr oder in festgelegten Intervallen formelle Risikobewertungen unter Anwendung eines risikobasierten Ansatzes durchgeführt oder auf ereignisgesteuerter Basis ausgelöst werden, z. B. in Reaktion auf einen Zwischenfall oder die daraus resultierenden Erkenntnisse (und in Verbindung mit sämtlichen Änderungen an Informationssystemen oder physischen Gebäuden oder Räumen), um mithilfe qualitativer und quantitativer Methoden die Wahrscheinlichkeit und die Auswirkungen aller ermittelten Risiken zu bestimmen. Die Wahrscheinlichkeit und die Auswirkungen in Zusammenhang mit inhärenten und verbleibenden Risiken müssen unabhängig und unter Berücksichtigung aller Risikokategorien (z. B. Audit-Ergebnisse, Gefahren- und Schwachstellenanalyse und Einhaltung gesetzlicher Vorschriften) ermittelt werden.
- Legt Risikokriterien fest und pflegt sie. Zu ihnen zählen:
  - die Kriterien für die Risikoakzeptanz und
  - Kriterien für die Durchführung von Risikobewertungen,
- Identifiziert die Risiken:

- Anwendung des Risikobewertungsprozesses, um Risiken zu identifizieren, die mit dem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Rahmen des Risiko-Rahmenkonzepts verbunden sind, und
- Identifizieren der Risikoverantwortlichen,

- Analysiert die Risiken:
  - Beurteilung der potenziellen Konsequenzen, die sich ergeben würden, wenn die Risiken erkannt würden,
  - Beurteilung der realistischen Wahrscheinlichkeit des Auftretens der identifizierten Risiken, und
  - Bestimmen der Risikostufen
- Bewertet die Risiken:
  - Vergleichen der Ergebnisse der Risikoanalyse mit den festgelegten Risikokriterien, und
  - Priorisieren der analysierten Risiken für die Risikobehandlung
- Risikobehandlung:
  - Auswahl geeigneter Optionen zur Risikobehandlung unter Berücksichtigung der Ergebnisse der Risikobeurteilung,
  - Bestimmung aller Kontrollen, die zur Implementierung der gewählten Risikobehandlungsoption(en) erforderlich sind,
  - Erstellung einer Anwendungserklärung, die die erforderlichen Kontrollen und Rechtfertigungen für Einschlüsse enthält, unabhängig davon, ob diese implementiert sind oder nicht, und
  - Durch Priorisierung der Risiken und Implementierung von Gegenmaßnahmen muss der Lieferant gewährleisten, dass die ermittelten Risiken innerhalb der Umgebung minimiert oder eliminiert werden. Der Lieferant sollte die Gegenmaßnahmen kontinuierlich überwachen, damit sie wirksam sind.
- Der Lieferant muss mindestens eine jährliche Risikobewertung in Bezug auf Informations-, Cyber-, physische Sicherheits-, Datenschutz- und Wiederherstellungsplanung durchführen. Abhängig von den spezifischen Umgebungen mit aktuellen und aufkommenden Bedrohungen muss der Lieferant eine häufigere Frequenz in Betracht ziehen.
  - Überprüfung der für den Betrieb der Barclays (einschließlich Rechenzentren) erbrachten Prozesse/Services wichtigen Standorte mindestens jährlich
- Das Unternehmen muss dokumentierte Informationen über den Prozess der Risikobewertung für die Informationssicherheit aufbewahren.
- Bei Risikobewertungen in Verbindung mit Datensteuerungsanforderungen muss Folgendes berücksichtigt werden:
  - Kategorisierung und Schutz der Daten vor unbefugter Verwendung, Zugriff, Verlust, Zerstörung oder Fälschung.
  - Kenntnis, wo sensible Daten gespeichert sind und über welche Anwendungen, Datenbanken, Server und Netzwerkinfrastrukturen diese übermittelt werden.
  - Einhaltung der festgelegten Aufbewahrungsfristen und Entsorgungsauflagen am Lebensende.
- Der Lieferant muss eine Bewertung der Auswirkungen auf den Datenschutz und der Folgeauswirkungen solcher Datenschutzrisiken auf den Geschäftsbetrieb des Unternehmens einschließlich Mission, Funktionen, andere Prioritäten des Risikomanagements (z. B. Compliance, Finanzen), Reputation, Belegschaft und Unternehmenskultur durchführen

- Der Lieferant muss die organisatorische Governance-Struktur entwickeln und implementieren, um ein fortlaufendes Verständnis der Prioritäten des Risikomanagements der Organisation auf der Grundlage des Datenschutzrisikos zu ermöglichen.

Der Lieferant muss Barclays informieren, falls er Risikobereiche nicht mindern bzw. verringern kann, die sich erheblich auf die für Barclays erbrachten Dienste auswirken könnten. Solche Fälle müssen Barclays umgehend gemeldet werden, damit Barclays alle aufsichtsbehördlichen Berichtspflichten erfüllen kann, und in jedem Fall innerhalb von 10 Arbeitstagen nach der Entdeckung.

MC 3.0 – Rollen und Verantwortlichkeiten

Der Lieferant hat sicherzustellen, dass alle seine Mitarbeiter wie auch unter anderem seine Auftragnehmer, Unterauftragnehmer und Unterauftragsverarbeiter, die an der Erbringung von Dienstleistungen für Barclays beteiligt sind, die Kontrollvorgaben von Barclays kennen und einhalten. Der Lieferant muss sicherstellen, dass ein geeignetes Team von Spezialisten und/oder Personen mit entsprechenden und sachgerechten Fähigkeiten, definierten Rollen und Verantwortlichkeiten zur Unterstützung und/oder Verwaltung der Kontrollvorgaben von Barclays eingesetzt wird, um effektiv zum Schutz der Barclays Services zu wirken.

Zur wirksamen Unterstützung der Kontrollvorgaben von Barclays muss der Lieferant Rollen und Verantwortlichkeiten definieren und kommunizieren. Diese Rollen und Verantwortlichkeiten müssen regelmäßig (mindestens alle 12 Monate) und nach jeder wesentlichen Änderung am Betriebsmodell oder Geschäft des Lieferanten überprüft werden.

Es liegt in der Verantwortung des Lieferanten, sicherzustellen, dass seine Mitarbeiter, Auftragnehmer, Unterauftragnehmer/Unterauftragsverarbeiter mit den Kontrollvorgaben dieses Standards und der zugehörigen Richtlinien und Standards vertraut sind und diese einhalten. Der Lieferant muss eine Ansprechstelle benennen, die sich bei einer Eskalation aufgrund einer Nichteinhaltung von Kontrollvorgaben in Verbindung setzt. Spezifische vertragliche Anforderungen sind schriftlich an die Unterauftragnehmer/Unterauftragsverarbeiter des Lieferanten zu übergeben.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Der Cloud-Service-Kunde sollte sich mit dem Cloud-Serviceprovider auf eine angemessene Zuweisung von Rollen und Verantwortlichkeiten für die Informationssicherheit einigen und bestätigen, dass er seine zugewiesenen Rollen und Verantwortlichkeiten erfüllen kann. Die Rollen und Verantwortlichkeiten beider Parteien sollten in einer Vereinbarung festgelegt werden. Der Cloud-Service-Kunde sollte seine Beziehung zur Kundensupport- und Betreuungsfunktion des Cloud-Serviceproviders identifizieren und verwalten.

Der Cloud-Service-Kunde sollte seine bestehenden Richtlinien und Verfahren entsprechend seiner Nutzung von Cloud-Diensten definieren oder erweitern und seine Cloud-Service-Benutzer über ihre Rollen und Verantwortlichkeiten bei der Nutzung des Cloud-Dienstes informieren.

MC 4.0 - Weiterbildung und Awareness

Der Lieferant muss für alle Mitarbeiter des Lieferanten, einschließlich Auftragnehmer, kurzfristige Mitarbeiter und Berater, kontinuierlich ein Schulungsprogramm zu Awareness durchführen. Alle Personen mit Zugriff auf Barclays-Daten/-Informationen oder andere physische Ressourcen müssen angemessen geschult und regelmäßig auf den neuesten Awareness-Stand der organisatorischen Richtlinien, Prozesse und Verfahren gebracht werden, die sich auf ihre berufliche Funktion innerhalb des Unternehmens beziehen. Schulungen und Awareness müssen die Mitarbeiter des Lieferanten auf die sichere Wahrnehmung ihrer Aufgaben vorbereiten. Die Unterlagen des durchgeführten Programms müssen in einer geeigneten Lernmanagementplattform oder durch einen manuellen Prozess aufgezeichnet werden.

Der Lieferant muss sicherstellen, dass alle Mitarbeiter des Lieferanten eine obligatorische Weiterbildungs- und Awareness-Schulung absolvieren. Dazu gehören Cyber-Sicherheit, physische Sicherheit, Wiederherstellungsplanung, Verwaltung personenbezogener Daten (Datenschutz), Datenmanagement, IT-Service-Management, EUDA und Schutz von Barclays-Daten innerhalb eines Monats nach dem Eintritt in das Unternehmen und/oder nach Eintritt in den Service für Barclays. Neben der jährlichen Aktualisierung der Schulung muss der Lieferant sicherstellen, dass Tests durchgeführt werden, um dafür zu sorgen, dass die Mitarbeiter des Lieferanten die Schulung und die Bildung von Awarenesss verstehen. Alle Schulungen müssen für alle Mitarbeiter des Lieferanten aufgezeichnet und gepflegt werden, die an den Barclays-Services arbeiten, und Barclays auf Verlangen zur Einsichtnahme vorgelegt werden.

Der Lieferant muss sicherstellen, dass sein Schulungsprogramm zur Sensibilisierung folgende Cyber-Sicherheitsthemen umfasst: Social Engineering und Insider-Bedrohung. Es wird empfohlen, dass der Lieferant Simulationstests für Social-Engineering-Angriffe mit Techniken wie Phishing-Simulationstests für alle Mitarbeiter auf Unternehmensebene durchführt und diese kontinuierlich überwacht, um sich zu vergewissern, dass die Bedrohung durch solche Risiken klar verstanden wird und identifizierte Probleme gemindert werden.

Gruppen mit hohem Risiko, wie z.B. Personen mit Zugang zu privilegierten Systemen, mit Zugang zu hochriskanten oder kritischen Bereichen oder in sensiblen Geschäftsfunktionen (einschließlich privilegierter Benutzer wie Entwickler und Support, leitende Angestellte, Informationssicherheitspersonal und externe Stakeholder), müssen entsprechend ihrer Rollen und Verantwortlichkeiten Schulungen zu Informationssicherheit und Awareness für die Situation der physischen Sicherheit erhalten.

Alle Mitarbeiter der physischen Sicherheit (unabhängig davon, ob sie vom Lieferanten, einem Eigentümer oder einem externen Lieferanten angestellt sind) müssen über einen akkreditierten, lizenzierten Dienstleister in Übereinstimmung mit den lokalen Gesetzen beauftragt oder vertraglich beauftragt werden und, sofern dies gesetzlich vorgeschrieben ist, eine persönliche Lizenz zur Durchführung von Sicherheitsaufgaben halten. Mitarbeiter der physischen Sicherheit müssen ihrer Rolle und Verantwortung entsprechende

Sicherheitsschulungen erhalten. Alle Schulungen müssen dokumentiert werden, für das gesamte Sicherheitspersonal muss ein Schulungsprotokoll geführt und auf Verlangen Barclays zur Einsichtnahme vorgelegt werden.

Der Lieferant muss sicherstellen, dass Mitarbeiter seiner Drittanbietern, die mit der Datenverarbeitung befasst sind, in Awareness des Datenschutzes geschult sind, um ihre datenschutzbezogenen Aufgaben und Verantwortlichkeiten im Einklang mit den entsprechenden Richtlinien, Prozessen, Verfahren, Vereinbarungen und Datenschutzwerten des Unternehmens wirksam zu erfüllen. Alle Schulungen müssen dokumentiert, für das gesamte Personal muss ein Schulungsprotokoll geführt und auf Verlangen Barclays zur Einsichtnahme vorgelegt werden.

Der Lieferant muss die Mitarbeiter schulen, um ihre Aufgaben im Datenmanagement (Management kritischer Datenelemente oder von Drittanbietern verwalteter Anwendungen) wirksam zu erfüllen.

Der EUDA-Eigentümer des Lieferanten muss die Mitarbeiter des Lieferanten mit EUDA-Verantwortlichkeiten identifizieren und sicherstellen, dass sie mindestens einmal pro Jahr eine rollengerechte Weiterbildungs- und Awareness-Schulung absolvieren und Belege als Nachweis für die Einhaltung der Kontrollmaßnahmen aufbewahren.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Der Cloud-Service-Kunde sollte zu Awarenessprogrammen, Weiterbildungs- und Schulungsprogrammen für Business Manager von Cloud-Diensten, Cloud-Service-Administratoren, Cloud-Service-Integratoren und Cloud-Service-Benutzer, einschließlich relevanter Mitarbeiter und Auftragnehmer, folgende Punkte hinzufügen:

- Standards und Verfahren für die Nutzung von Cloud-Diensten
- Risiken der Informationssicherheit in Bezug auf Cloud-Dienste und Umgang mit diesen Risiken
- Risiken der System- und Netzwerkumgebung bei der Nutzung von Cloud-Diensten
- Einschlägige rechtliche und behördliche Erwägungen.

Awareness für Informationssicherheit, Weiterbildungs- und Schulungsprogramme zu Cloud-Dienste sollten dem Management und den Vorgesetzten, auch der Geschäftseinheiten, zur Verfügung gestellt werden. Diese Bemühungen unterstützen eine effektive Koordinierung von Maßnahmen zur Informationssicherheit.

MC 5.0 – Management von Sicherheitsvorfällen

Der Lieferant muss über ein etabliertes Rahmenkonzept für das Management von Sicherheitsvorfällen verfügen, das einen Vorfall und seine zugrunde liegende Ursache wirksam handhabt, eindämmt und aus der Lieferantenumgebung entfernt bzw. mildert.

Der Lieferant muss über ein dokumentiertes Verfahren für das Vorfall- und Krisenmanagement verfügen, das unter anderem den Prozess zur Eskalation von Vorfällen/Krisen an Barclays beinhaltet. Der Lieferant muss Sorge dafür tragen, dass Teams und Prozesse für das

Management von Vorfällen/Krisen mindestens einmal jährlich getestet werden, um sicherzustellen, dass der Lieferant zur wirksamen und effizienten Behandlung von Vorfällen in der Lage ist. Der Lieferant muss außerdem prüfen, ob er in der Lage ist, die betreffenden Kontakte innerhalb eines festgelegten Zeitrahmens über einen Vorfall zu informieren, und dies Barclays auf Verlangen demonstrieren.

Der Lieferant muss gewährleisten, dass schriftliche Vorfallbehandlungspläne vorliegen, in denen die Rollen der Lieferantenmitarbeiter wie auch die einzelnen Phasen von Vorfallbehandlung/Vorfallmanagement festgelegt sind:

- Verantwortlichkeiten und Verfahren – Managementverantwortlichkeiten und -verfahren müssen festgelegt werden, um eine schnelle, effektive und geordnete Reaktion auf Vorfälle zu gewährleisten.
- Meldung von Vorfallereignissen – Vorfallereignisse müssen so schnell wie möglich über geeignete Managementkanäle gemeldet werden; die Meldemechanismen müssen für alle Mitarbeiter und Auftragnehmer des Lieferanten einfach und zugänglich sein.
- Bewertung von Vorfallereignissen – Vorfallereignisse müssen bewertet werden, um die sachgerechte Wichtigkeit, Klassifizierung und Reaktion zu bestimmen.
    - Klassifizierung von Vorfällen: Festlegung einer Skala für die Klassifizierung von Vorfällen sowie Entscheidung, ob das Ereignis als Vorfall klassifiziert werden muss. Die Klassifizierung und Priorisierung von Vorfällen kann dabei helfen, die Auswirkungen und das Ausmaß eines Vorfalls zu identifizieren.
- Reaktion auf Vorfälle – Auf Vorfälle muss in Übereinstimmung mit den dokumentierten Verfahren des Managements von Vorfällen des Lieferanten reagiert werden.
    - Eindämmung des Vorfalls – Nutzung von Mitarbeiter-, Verfahrens- und Technologiekompetenzen, um einen Vorfall schnell und effektiv in der Umwelt einzudämmen.
    - Beseitigung/Minderung von Bedrohungen – Nutzung von Mitarbeiter-, Verfahrens- und Technologiekompetenzen, um eine Sicherheitsbedrohung und/oder deren Komponenten innerhalb der Umgebung schnell und effektiv zu beseitigen/zu mindern.
- Lernen aus Vorfällen – Die durch die Analyse und Lösung von Vorfällen gewonnenen Erkenntnisse sollen genutzt werden, um die Wahrscheinlichkeit oder Auswirkungen zukünftiger Vorfälle zu verringern.
- Beweisaufnahme – Der Lieferant hat Verfahren zur Identifizierung, Sammlung, Erfassung und Aufbewahrung von Informationen zu definieren und anzuwenden, die als Beweismittel dienen können.

Nach dem Vorfall – Nach einer Störung des Dienstes ist Barclays innerhalb von **vier Kalenderwochen** nach Wiederherstellung des Dienstes in den normalen Betriebszustand ein **Vorfallbericht** vorzulegen. Der Bericht muss mindestens eine Überprüfung folgender Punkte enthalten:

- Ereignisse im Umfeld der Situation
- Handhabung des Vorfalls bzw. der Krise
- Analyse der Grundursachen des Vorfalls bzw. der Krise

- Einstufung des Vorfalls bzw. der Krise vom Lieferanten oder von Barclays als „Risikoereignis“ (d. h. als in ausreichendem Maße erheblich angesehen wird, dass er bzw. sie gemäß den geltenden Richtlinien, die dem Lieferanten bekannt sind, an die relevanten Stakeholder gemeldet/eskaliert werden sollte)
- ob der Vorfall bzw. die Krise ein Verhaltenrisiko („Conduct Risk“) darstellt (wenn beispielsweise der Lieferant direkten Umgang mit Kunden von Barclays hat)
- jegliche dem Lieferanten bekannte Beschwerden von Barclays-Kunden
- kontinuierliche Verbesserung, um einem erneuten Auftreten vorzubeugen
- Der Lieferant muss versuchen, die Behandlungsmaßnahmen möglichst zu optimieren, indem er Erkenntnisse aus aktuellen und früheren Feststellungen/Behandlungsmaßnahmen einfließen lässt.

Kommunikation – Der Lieferant muss eine Ansprechstelle für eventuelle Sicherheitsvorfälle benennen, die bei Vorfällen/Krisen mit Barclays zusammenarbeitet. Der Lieferant muss Barclays die Kontaktdaten der Person(en) und alle eventuellen Änderungen samt außerhalb der Geschäftszeiten erreichbaren Kontaktpersonen und Telefonnummern mitteilen.

Die Angaben müssen Folgendes beinhalten: - Name, Verantwortlichkeiten innerhalb des Unternehmens, Funktion, E-Mail-Adresse und Telefonnummer

Wenn der Lieferant zu irgendeinem Zeitpunkt bestätigt, dass ein Vorfall Auswirkungen auf Barclays Services, Barclays-Systemen oder Barclays-Daten hat, muss er Barclays unverzüglich, jedoch nicht später als 2 Stunden nach dem Vorfall benachrichtigen.

Sobald der Lieferant Kenntnis von einem Cyber-Vorfall erlangt, auch durch Hinweis eines Barclays-Unternehmens, hat der Lieferant unverzüglich, in keinem Fall jedoch später als nach geltendem Recht erforderlich oder, wenn keine solche Vorgabe besteht, innerhalb von 48 Stunden nach dem ersten Bekanntwerden des Cyber-Vorfalls, Barclays durch E-Mail an gcsojoc@barclays.com **zu benachrichtigen**, und alle relevanten Informationen zu liefern, insbesondere, soweit möglich, (a) die Kategorien und die annähernde Anzahl der betroffenen Barclays-Datensätze und, falls zutreffend, die Kategorien und die annähernde Anzahl der betroffenen Personen, (b) die Auswirkungen und wahrscheinlichen Folgen des Cyber-Vorfalls für Barclays und gegebenenfalls die entsprechenden betroffenen Personen, und (c) die vom Lieferanten ergriffenen oder zu ergreifenden Korrektur- und Schadensbegrenzungsmaßnahmen.

Im Falle eines tatsächlichen, vermuteten oder behaupteten Diebstahls, einer solchen unbefugten Nutzung oder Offenlegung geschützter personenbezogener Daten aufgrund eines Versagens der Sicherheitsgarantien des Lieferanten (oder der Mitarbeiter des Lieferanten) oder des unbefugten Zugriffs auf geschützte personenbezogene Daten vom oder über den Lieferanten (oder Mitarbeiter des Lieferanten), Verlust, Beschädigung oder Vernichtung geschützter personenbezogener Daten im Besitz oder unter Kontrolle eines Lieferantenpersonals oder einer sonstigen unbefugten Verarbeitung geschützter personenbezogener Daten hat der Lieferant Barclays so schnell wie möglich, in jedem Fall innerhalb von 24 Stunden nach Bekanntwerden des entsprechenden Ereignisses, Barclays durch E-Mail an gcsojoc@barclays.com

zu benachrichtigen und Barclays in Bezug auf ein solches Ereignis umfassende Zusammenarbeit und Unterstützung zu leisten, samt Lieferung aller relevanten Angaben wie Daten, Zeit, Ort, Art des Vorfalls, Auswirkungen, Status und ergriffene Maßnahmen zur Risikominderung.

Wenn ein Unterauftragnehmer/Unterauftragsverarbeiter zur Erbringung des Dienstes eingesetzt wird, in welchem er Daten/Informationen oder Ressourcen von Barclays hält oder verarbeitet, muss der Lieferant die Zustimmung von Barclays einholen. Der Lieferant muss eine vertragliche Beziehung zu den Unterauftragnehmern/Unterauftragsverarbeitern haben und sicherstellen, dass die Unterauftragnehmer/Unterauftragsverarbeiter mit einem ähnlichen Standard-Rahmenkonzept gemäß den besten Branchenverfahren akkreditiert sind, das die von ihnen verarbeiteten und/oder gespeicherten Barclays-Daten/Informationen wirksam schützt. Bei einem Vorfall mit einem Unterauftragnehmer/Unterauftragsverarbeiter muss sichergestellt werden, dass die oben genannte Meldung des Vorfalls befolgt werden muss.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Der Cloud-Service-Kunde sollte die Zuweisung der Verantwortlichkeiten für das Management von Vorfällen überprüfen und sicherstellen, dass er die Anforderungen des Cloud-Service-Kunden erfüllt. Der Cloud-Service-Kunde sollte vom Cloud-Serviceprovider Informationen über folgende Mechanismen verlangen:
– Meldung eines vom Cloud-Service-Kunden festgestellten Vorfalls/Ereignisses an den Cloud-Serviceprovider
– Eingang von Meldungen eines vom Cloud-Serviceprovider festgestellten Vorfalls/Ereignisses beim Cloud-Service-Kunden
– Nachverfolgung des Status eines gemeldeten Informationssicherheitsereignisses durch den Cloud-Service-Kunden.

MC 6.0 – IT-Ressourcenmanagement (Hardware und Software)

Der Lieferant muss ein effektives Programm zum Ressourcenmanagement während des gesamten Lebenszyklus eingerichtet haben und betreiben. Das Ressourcenmanagement muss den Lebenszyklus der Ressourcen steuern – von der Beschaffung bis hin zur Außerbetriebnahme und/oder sicheren Entsorgung – und so über alle Ressourcenklassen in der Umgebung hinweg für Transparenz und Sicherheit sorgen.

Der Lieferant muss eine vollständige, zutreffende und aktuelle Bestandsliste aller geschäftskritischen Ressourcen führen, die sich an sämtlichen Standorten bzw. Regionen befinden, an denen Dienste für Barclays erbracht werden, darunter auch Barclays-Ausrüstung, die in den Räumlichkeiten des Lieferanten bzw. eines Unterauftragsnehmers/Unterauftragverarbeiters des Lieferanten gehostet oder von Barclays zur Verfügung gestellt wird, und sicherstellen, dass diese mindestens einmal jährlich überprüft wird, um zu validieren, dass die Bestandsliste der Informationsressourcen aktuell, vollständig und zutreffend ist. Auf Verlangen wird er Barclays die Ergebnisse vorlegen.

Der Prozess zum Ressourcenmanagement muss folgende Bereiche abdecken:

- Ressourcenbestand – Mit Informationen und Informationsverarbeitungseinrichtungen in Verbindung stehende Ressourcen sind zu identifizieren, eine Bestandsaufnahme dieser Ressourcen ist zu erstellen und zu pflegen.
    - Der Lieferant muss eine zutreffende und aktuelle Bestandsliste aller Hardware-Ressourcen pflegen, mit deren Hilfe Informationen gespeichert oder verarbeitet werden können.
    - Der Lieferant muss über einen zutreffenden und aktuellen Bestand an Informationsressourcen für Barclays-Geräte verfügen, die beim Lieferanten gehostet werden, und/oder Barclays-IT-Anlagen, die dem Lieferanten zur Verfügung gestellt wurden.
    - Lieferanten mit Tier-1-, Tier-2- oder Tier-3-Spezifikation müssen aktuelle, vollständige und zutreffende Ressourcen-Bestandslisten führen (einschließlich Desktop-PCs, Laptops, Netzwerk-Ausstattung, RSA-Token oder von Barclays zur Verfügung gestellte Ressourcen).
    - Der Lieferant muss in jährlichen Abständen eine Abstimmung aller Ressourcen von Barclays (Hardware und Software) durchführen und Barclays (Chief Security Office/ECAM-Team) die Ergebnisse vorlegen.
    - Durchführung einer aktuellen Bestandsaufnahme aller zur Verfügung gestellten, autorisierten Softwareprodukte, die für die Erbringung des Barclays-Services erforderlich sind, und Befolgung der Bedingungen der jeweiligen Lizenzen.
    - Der Bestand der Ressourcen des Cloud-Service-Kunden muss Informationen und zugehörige Ressourcen enthalten, die in der Cloud-Computing-Umgebung gespeichert sind. In den Bestandsaufzeichnungen muss angegeben sein, wo die Ressourcen gepflegt werden, z. B. Benennung des Cloud-Services.
- Eigentum an Ressourcen – die im Bestand geführten Ressourcen müssen sich im Eigentum befinden.
    - Informationsressourcen sind je nach Klassifizierung, Bedeutung und Geschäftswert geschützt.
- Akzeptable Nutzung von Ressourcen – Regeln für die akzeptable Nutzung von Informationen und von Ressourcen, die mit Einrichtungen zu Informationen und Informationsverarbeitung verbunden sind, müssen identifiziert, dokumentiert und implementiert werden.
    - Sicherstellung, dass nicht-autorisierte Ressourcen aus dem Netzwerk entfernt werden.
    - Der Lieferant muss sicherstellen, dass effektive und effiziente Verfahren implementiert werden, um nicht unterstützte Technologien zu reduzieren sowie Lebensende, Außerbetriebnahme und Sichere Entsorgung von Ressourcen und Daten zu managen und so das Risiko einer Datenkompromittierung zu minimieren.
    - Kennzeichnung nicht unterstützter Software und Hardware im Bestandsverwaltungssystem als nicht unterstützt.
- Rückgabe von Ressourcen – Alle Mitarbeiter des Lieferanten und Unterauftragnehmers/Unterauftragsverarbeiters (im Umfang der Dienstleistungen an Barclays) müssen alle Ressourcen des Lieferanten, die sich in ihrem Besitz befinden, nach Beendigung ihres Arbeitsverhältnisses, Auftrags oder Vertrags zurückgeben.
    - „Gestohlene oder verlorene“ Barclays-Ressourcen müssen ordnungsgemäß untersucht und Barclays gemäß der Kontrolle des Vorfallmanagements gemeldet werden.
    - Falls „Gestohlene oder verlorene“ Lieferantenressourcen Barclays-Informationen enthalten, müssen diese der Vorfallmanagement-Kontrolle entsprechend Barclays gemeldet werden.

Der Lieferant muss Barclays bekannte Änderungen seiner direkten oder indirekten Fähigkeit zum Support für IT-Ressourcen, die zum Erbringen von Diensten für Barclays verwendet werden, sofort anzeigen, unter anderem wenn Produkte Sicherheitsschwachstellen aufweisen, und er muss für die rechtzeitige Aufrüstung oder Aussonderung dieser IT-Ressourcen sorgen.

Transport von Barclays-Ressourcen - Der Lieferant stellt sicher, dass sämtliche Ressourcen und Daten von Barclays sicher transportiert und angemessene Kontrollen durchgeführt werden, die im Verhältnis zum Wert der zu befördernden Ressourcen und Daten (in Hinblick auf sowohl finanzielle Verluste als auch Rufschädigungen) sowie zur Auswirkung der Bedrohungsumgebung stehen, in die sie transportiert werden.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Der Ressourcenbestand des Cloud-Service-Kunden sollte Informationen und zugehörige Ressourcen ausweisen, die in der Cloud-Computing-Umgebung gespeichert sind. In den Bestandsaufzeichnungen sollte angegeben sein, wo die Ressourcen gepflegt werden, z. B. Benennung des Cloud-Services.

Die Installation kommerziell lizenzierter Software in einem Cloud-Service kann eine Verletzung der Lizenzbedingungen für die Software verursachen. Der Cloud-Service-Kunde sollte über ein Verfahren zur Identifizierung Cloud-spezifischer Lizenzanforderungen verfügen, bevor er die Installation von lizenzierter Software in einem Cloud-Service zulässt. Besondere Aufmerksamkeit sollte den Fällen gelten, in denen der Cloud-Service flexibel und skalierbar ist und die Software auf einer größeren Anzahl von Systemen oder Prozessorkernen ausgeführt werden kann, als laut Lizenzbedingungen zulässig ist.

MC 7.0 – Sichere Entsorgung/Vernichtung von physischen Ressourcen und Datenremanenz von elektronischen Informationen

Sichere Vernichtung oder Löschung von Barclays-Informationsressourcen, einschließlich der für den Service verwendeten Bilder, die in physischer und/oder elektronischer Form gespeichert sind, müssen auf eine zweckgerechte sichere Methode durchgeführt werden und sicherstellen, dass Barclays-Daten nicht wiederherstellbar sind.

Der Lieferant muss Verfahren mit unterstützenden Geschäftsprozessen und technischen Maßnahmen zur sicheren Entsorgung unter Verwendung geeigneter Sanitierungsverfahren einrichten, wie unter anderem das Löschen, Entfernen und Vernichten von Barclays-Daten von allen Speichermedien, wodurch Barclays-Daten durch bekannte computerforensische Mittel nicht wiederherstellbar werden.

Die auf Datenträgern gespeicherten Barclays-Daten müssen gelöscht werden, um die Daten in einen nicht wiederherstellbaren Zustand zu bringen; dazu sind geeignete Datenlöschtechniken wie Secure Wipe, Purging, Data Clearing oder Asset Destruction oder softwarebasierte Methoden zum Überschreiben der Daten zu verwenden oder das Branchenstandard-Rahmenkonzept zur Datenentsorgung (NIST) anzuwenden. Alle Geräte (Informationsressourcen) müssen am Ende ihrer Lebensdauer und/oder Betriebsdauer (fehlerhaft, aufgrund von

stillgelegten oder nicht mehr benötigten Services außer Betrieb genommen, in einem Test oder Proof of Concept verwendet, Datenlöschdienste können für wiederverwendbare Geräte genutzt werden usw.) entsorgt werden.

Die Entsorgungsvorgaben gelten für Unterauftragnehmer/Unterauftragsverarbeiter des Lieferanten, die zur Erbringung der Barclays-Services eingesetzt werden.

Entsorgung von Dokumenten in Papierform muss mit einem Aktenvernichter nach mindestens P4 DIN 66399 erfolgen (einschließlich Zahlungskartendaten). Alternativ können sie gemäß BS EN 15713:2009 verbrannt werden.

Für Barclays müssen Belege für die Datenvernichtung aufbewahrt werden, die einen Prüfpfad, Nachweise und eine Rückverfolgung ermöglichen und Folgendes beinhalten müssen:

- Nachweis über die Vernichtung und/oder Entsorgung (einschließlich Datum und Methode)
- Systemprüfprotokolle für die Löschung.
- Bescheinigungen über die Datenvernichtung.
- Ausführende Stelle der Vernichtung (einschließlich etwaiger Partner, Dritter oder Auftragnehmer)
- Es muss ein Vernichtungs- und Überprüfungsbericht erstellt werden, um den Erfolg oder das Scheitern eines Vernichtungs-/Löschvorgangs zu bestätigen (d.h. ein Überschreibungsprozess muss eine Aufstellung liefern, die alle Sektoren detailliert aufführt, die nicht gelöscht werden konnten).

Bei Verlassen des Barclys-Services muss der Lieferant dafür sorgen, dass die Daten von Barclays nach Benachrichtigung und Genehmigung durch Barclays sicher vernichtet werden.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Der Cloud-Service-Kunde sollte eine Bestätigung verlangen, dass der Cloud-Serviceprovider über Richtlinien und Verfahren zur sicheren Entsorgung oder Wiederverwendung von Ressourcen verfügt. Der Cloud-Service-Kunde sollte eine dokumentierte Beschreibung des Prozesses zur Beendigung des Services verlangen, die die Rückgabe und Entfernung der Ressourcen des Cloud-Service-Kunden enthält, gefolgt von der Löschung aller Kopien dieser Ressourcen aus den Systemen des Cloud-Serviceproviders. In der Beschreibung sollten alle Ressourcen aufgeführt und der Zeitplan für die Beendigung des Services dokumentiert werden, der zeitnah erfolgen sollte.

MC 8.0 – Informationsklassifizierung und Datenverarbeitung

Der Lieferant muss über ein etabliertes und angemessenes Rahmenkonzept/Programm zur Informationsklassifizierung und Datenhandhabung (angepasst an bewährten Praktiken der Branche und/oder die Anforderungen von Barclays) verfügen, das folgende Komponenten abdeckt:

- Klassifizierung von Informationen – Informationen sind hinsichtlich ihrer Wichtigkeit und Sensibilität in Bezug auf unberechtigte Offenlegung oder Änderung zu klassifizieren.
- Kennzeichnung von Informationen – Ein geeignetes Set von Verfahren zur Kennzeichnung von Informationen ist gemäß dem vom Lieferanten angenommenen Informationsklassifikationsschema zu entwickeln und umzusetzen.
- Umgang mit Ressourcen – Verfahren für den Umgang mit Ressourcen sind gemäß dem vom Lieferanten angenommenen Klassifizierungsschema für Informationen zu entwickeln und umzusetzen.
- Sicherstellung, dass alle Mitarbeiter mit den Kennzeichnungs- und Handhabungsanforderungen des Lieferanten/von Barclays vertraut sind und wissen, wie die korrekte Informationsklassifizierung richtig anzuwenden ist.

Der Lieferant muss sich auf das Barclays-Kennzeichnungsschema für Informationen und die Anforderungen an die Handhabung (Anhang A, Tabellle A1 und A2 oder ein alternatives Schema berufen, um zu gewährleisten, dass sämtliche von ihm verwahrten und/oder verarbeiteten Barclays-Informationen gesichert und geschützt werden. Diese Anforderung gilt für sämtliche im Auftrag von Barclays verwahrten oder verarbeiteten Barclays-Informationsressourcen einschließlich der Unterauftragnehmer/Unterauftragsverarbeiter.

Leitfaden für Cloud-Service-Kunden (Lieferant)

Der Cloud-Service-Kunde sollte Informationen und zugehörige Ressourcen, die in der Cloud-Computing-Umgebung gepflegt werden, entsprechend den vom Cloud-Service-Kunden verabschiedeten Kennzeichnungsverfahren kennzeichnen. Gegebenenfalls können vom Cloud-Serviceprovider zur Verfügung gestellte Funktionen, die die Kennzeichnung unterstützen, übernommen werden.

Inspektionsrecht

Zur Überprüfung der Erfüllung der Vertragspflichten des Lieferanten gegenüber Barclays muss der Lieferant Barclays erlauben, nachdem Barclays dies mindestens zehn (10) Geschäftstage zuvor schriftlich angekündigt hat, eine Sicherheitsüberprüfung jedes Standorts oder jeder Technologie vorzunehmen, der bzw. die vom Lieferanten oder von dessen Unterauftragnehmer/Unterauftragsverarbeiter dazu genutzt wird, die in den Diensten verwendeten Lieferantensysteme zu entwickeln, zu testen, zu verbessern, zu pflegen oder zu betreiben. Der Lieferant muss Barclays zudem erlauben, mindestens ein Mal pro Jahr oder unmittelbar nach einem Sicherheitsvorfall eine Inspektion durchzuführen.

Zu jeder von Barclays bei einer Inspektion identifizierten Nichtkonformität von Kontrollen muss Barclays eine Risikobewertung durchführen und einen Zeitrahmen für Abstellmaßnahmen vorgeben. Anschließend muss der Lieferant etwaige verlangte Abstellmaßnahmen innerhalb dieses Zeitrahmens ausführen.

Der Lieferant muss Barclays in Bezug auf die Inspektion und die bei der Inspektion vorgelegten Unterlagen in angemessener Weise unterstützen. Die Dokumentation muss ausgefüllt und umgehend an Barclays zurückgesendet werden. Der Lieferant muss Barclays außerdem mit einem Beurteilungs-Fragesteller sowie mit den im Zuge einer Sicherheitsrisikoüberprüfung verlangten Nachweisen unterstützen.

Anhang A: Barclays-Kennzeichnungsschema für Informationen, Anforderungen an die Handhabung von Daten

Tabelle A1: Barclays-Kennzeichnungsschema für Informationen

Kennzeichnung	Definition	Beispiele
Geheim	Informationen müssen als **Geheim** kategorisiert werden, wenn ihre unbefugte Offenlegung negative Auswirkungen auf Barclays haben würde, mit der Einschätzung im Rahmen des Enterprise Risk Management Rahmenkonzept (ERMF) als „Kritisch" - „Critical" (finanziell oder nicht finanziell). Diese Informationen sind auf eine spezifische Zielgruppe beschränkt und dürfen ohne Erlaubnis des Urhebers nicht weiterverbreitet werden. Auf ausdrückliche Genehmigung des Verantwortlichen für die Informationen können zur Zielgruppe auch externe Empfänger gehören.	• Informationen über mögliche Firmenzusammenschlüsse oder -übernahmen • Informationen zur strategischen Planung – das Geschäft und die Organisation betreffend. • Bestimmte Informationen über die Sicherheitskonfiguration. • Bestimmte Befunde und Berichte einer Betriebsprüfung. • Vorstandsprotokolle. • Angaben zur Authentifizierung oder Identifizierung und Verifizierung (ID&V) – Kunden/Klienten und Kollegen. • Große Mengen an Informationen über Karteninhaber. • Gewinnprognosen oder Jahresbilanzen (vor deren Veröffentlichung) • Im Rahmen einer formellen Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) behandelte Punkte.
Eingeschränkt - Intern	Informationen müssen als **Eingeschränkt – Intern** kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern nur um authentifizierte Mitarbeiter von Barclays und Managed Service Providers (MSPs) von Barclays mit einem bestehenden aktiven Vertrag handelt und sie auf eine spezifische Zielgruppe beschränkt sind. Eine unbefugte Offenlegung würde negative Auswirkungen auf Barclays haben, mit der Einschätzung im Rahmen des ERMF als „Bedeutend" - „Major" oder „Begrenzt" - „Limited" (finanziell oder nicht finanziell).	• Strategien und Budgets • Leistungsbeurteilungen • Vergütung und personenbezogene Daten von Mitarbeitern. • Schwachstellenbewertungen

	Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	
Eingeschränkt – Extern	Informationen müssen als **Eingeschränkt – Extern** kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern um authentifizierte Mitarbeiter von Barclays und MSPs von Barclays mit einem bestehenden aktiven Vertrag handelt und sie auf eine spezifische Zielgruppe oder auf vom Verantwortlichen für die Informationen genehmigte externe Personen beschränkt sind. Eine unbefugte Offenlegung würde negative Auswirkungen auf Barclays haben, mit der Einschätzung im Rahmen des ERMF als „Bedeutend" - „Major" oder „Begrenzt" - „Limited" (finanziell oder nicht finanziell). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Neue Produktpläne • Klientenverträge • Rechtsgültige Verträge • Für die externe Versendung vorgesehene Kunden-/Klienteninformationen individueller Art bzw. geringen Umfangs. • Kunden-/Klientenmitteilungen. • Angebotsunterlagen für Neuemissionen (z. B. Emissions-, Verkaufsprospekt). • Abschließende Forschungsdokumente. • Nicht zu Barclays gehörige wesentliche nicht öffentliche Informationen (Material Non-Public Information; MNPI). • Sämtliche Forschungsberichte • Bestimmtes Marketingmaterial • Marktkommentare • Befunde und Berichte einer Betriebsprüfung
Uneingeschränkt	Informationen müssen als Uneingeschränkt kategorisiert werden, wenn sie entweder für die allgemeine Verbreitung bestimmt sind oder wenn sie im Falle ihrer Verbreitung keine negativen Auswirkungen auf die Organisation haben würden.	• Marketingmaterial • Veröffentlichungen • Öffentliche Ankündigungen • Stellenausschreibungen • Informationen ohne Auswirkungen auf Barclays

Tabelle A2: Barclays-Kennzeichnungsschema für Informationen – Anforderungen an die Handhabung von Daten

*** Informationen über Systemsicherheitskonfigurationen, Ergebnisse von Betriebsprüfungen und personenbezogene Datensätze können, je nach den Auswirkungen ihrer unbefugten Offenlegung auf das Geschäft, als „Eingeschränkt – Intern“ oder „Geheim“ eingestuft werden.

Phase des Lebenszyklus	Geheim	Eingeschränkt – Intern	Eingeschränkt – Extern
Erstellen und Einführen	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.	• Ressourcen müssen einem Verantwortlichen für die Informationen zugewiesen sein.
Speichern	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Elektronische Ressourcen in Speichermedien müssen durch Verschlüsselung oder zweckgerechte Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht. • Alle zum Schutz der Daten, der Identität und/oder Reputation von Barclays verwendeten privaten Schlüssel müssen durch zertifizierte HSMs (Hardware Security Modules), d. h. FIPS 140-2 Level 3 oder höher, geschützt sein.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen abgelegt werden (einschließlich öffentlicher Bereiche innerhalb der Räumlichkeiten, in die Besucher ohne Überwachung gelangen könnten). • Informationen dürfen nicht in öffentlichen Bereichen innerhalb von Räumlichkeiten gelassen werden, in die Besucher ohne Überwachung gelangen könnten.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Elektronische Ressourcen in Speichermedien müssen durch Verschlüsselung oder zweckgerechte Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht.
Zugriff und Verwendung	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten bearbeitet oder unbeaufsichtigt gelassen werden, an denen unbefugte Personen sie einsehen oder auf sie zugreifen könnten. Ressourcen können bearbeitet werden, wenn zweckgerechte Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Für den Druck vorgesehene Ressourcen müssen mithilfe sicherer Druckprogramme gedruckt werden.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen außerhalb der Räumlichkeiten gelassen werden. • Ressourcen (ob physisch oder elektronisch) dürfen nicht in öffentlichen Bereichen innerhalb der Räumlichkeiten gelassen werden, in die Besucher ohne Überwachung gelangen könnten. • Falls erforderlich, müssen elektronische Ressourcen durch zweckgerechte LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.	• Ressourcen (ob physisch oder elektronisch) dürfen nicht an Orten bearbeitet oder unbeaufsichtigt gelassen werden, an denen unbefugte Personen sie einsehen oder auf sie zugreifen könnten. Ressourcen können bearbeitet werden, wenn zweckgerechte Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente).

	• Elektronische Ressourcen müssen durch zweckgerechte LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.		• Gedruckte Ressourcen müssen sofort aus dem Drucker entnommen werden. Ist dies nicht möglich, müssen sichere Druckprogramme verwendet werden. • Elektronische Ressourcen müssen durch zweckgerechte LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.
Weitergabe	• Ausgedruckte Ressourcen müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Umschläge, in denen sich ausgedruckte Ressourcen befinden, müssen an der Vorderseite eine sichtbare Informationsbeschriftung tragen und mit einem manipulationssicheren Siegel versehen werden. Vor der Verteilung müssen diese in einen unbeschrifteten zweiten Umschlag gesteckt werden. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. Elektronische Kopien mehrseitiger Dokumente müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen. • Ressourcen dürfen nur an Personen verteilt werden, denen vom Verantwortlichen für die Informationen ausdrücklich die Befugnis erteilt wurde, sie in Empfang zu nehmen.	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung erhalten. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen.	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung tragen. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Umschläge, in denen sich ausgedruckte Ressourcen befinden, müssen an der Vorderseite eine sichtbare Informationsbeschriftung tragen. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen. Elektronische Kopien mehrseitiger Dokumente müssen auf jeder Seite eine sichtbare Informationsbeschriftung tragen. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden. • Ressourcen dürfen nur an Personen verteilt werden, die beim Unternehmen angestellt oder entsprechend vertraglich verpflichtet sind oder die im Rahmen eines klar anerkannten geschäftlichen Bedarfs (z. B. Vertragsverhandlung) diese Ressourcen benötigen. • Ressourcen dürfen nur an Personen verteilt werden, die diese aus geschäftlichen Gründen benötigen.

	• Ressourcen dürfen nicht per Fax gesendet werden. • Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübermittlung außerhalb des internen Netzwerks verläuft. • Für elektronische Ressourcen muss eine Kontrollkette gepflegt werden.		• Ressourcen dürfen nicht per Fax gesendet werden, es sei denn, der Absender hat sich vergewissert, dass die Empfänger zum Abruf der Ressource bereitstehen. • Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübermittlung außerhalb des internen Netzwerks verläuft.
Archivieren und Entsorgen	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben“ des Systems und ähnlichen Ablagen gelöscht werden. • Medien, auf denen als „Geheim” eingestufte elektronische Ressourcen gespeichert wurden, müssen vor oder während der Entsorgung entsprechend bereinigt werden.	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben“ des Systems und ähnlichen Ablagen gelöscht werden.	• Ausgedruckte Ressourcen müssen von einem Entsorgungsdienst für vertrauliche Unterlagen entsorgt werden. • Kopien elektronischer Ressourcen müssen auch umgehend aus den „Papierkörben“ des Systems und ähnlichen Ablagen gelöscht werden.

Anhang B: Definitionen

Vertrauliche Informationen von Barclays sind alle Informationen, die vom Leiter des Lieferanten, vom Lieferanten oder von Mitarbeitern des Lieferanten im Zusammenhang mit diesen Allgemeinen Geschäftsbedingungen und/oder Verträgen eingeholt wurden (oder auf die einer der Genannten Zugriff hat), die sich beziehen auf frühere, gegenwärtige oder zukünftige (i) geschäftliche Aktivitäten, Produkte und/oder Entwicklungen von Barclays-Unternehmen und/oder (ii) Mitarbeiter, Kunden, Kontrahenten, Dritte/Lieferanten und/oder Auftragnehmer von Barclays-Unternehmen (mit Ausnahme von Unternehmen des Lieferanten), einschließlich des gesamten geistigen Eigentums von Barclays-Unternehmen (einschließlich gemäß eines Vertrags) oder solcher Drittanbieter/Auftragnehmer, geschützter personenbezogener Daten, dieser Allgemeinen Geschäftsbedingungen, jedes Moduls und jedes Vertrags sowie von Aufzeichnungen, die im Rahmen eines Vertrags geführt werden, und alle Informationen in Bezug auf Pläne, Preise, Methoden, Prozesse, Finanzdaten des jeweiligen Unternehmens oder der jeweiligen Person, Rechte des geistigen Eigentums, Forschung, Systeme, Programme und/oder Informationstechnologie.

Barclays-Daten sind alle Daten, Informationen, Texte, Zeichnungen und anderen Materialien, die in einem beliebigen Medium enthalten sind, einschließlich aller elektronischen, optischen, magnetischen oder materiellen Medien, die (i) dem Lieferanten im Zusammenhang mit einem Vertrag zugänglich sind, (ii) dem Lieferanten von einem Barclays-Unternehmen zur Verfügung gestellt werden, oder (iii) der Lieferant in Verbindung mit einem Vertrag, mit Ausnahme von Materialien des Lieferanten, erzeugt, erfasst, verarbeitet, speichert oder übermittelt.

Barclays-Systeme bezeichnet die elektronischen Informationssysteme, die aus einem oder mehreren von Hardware, Geräten, Software, Peripheriegeräten und Kommunikationsnetzwerken bestehen, die sich im Eigentum eines Barclays-Unternehmens befinden oder von einem solchen Unternehmen kontrolliert, betrieben und/oder genutzt werden.

Cyber-Vorfall bezeichnet jedes Ereignis, unabhängig davon, ob der Eintritt eines solchen Ereignisses tatsächlich bestätigt wurde, oder ob der Lieferant oder Barclays angemessene Gründe zur Annahme hat, dass es eingetreten ist (basierend auf einer glaubwürdigen Bedrohung, Informationen oder auf anderen Wegen), das (i) die Vertraulichkeit, Integrität oder vollständige Verfügbarkeit von Barclays-Daten oder (ii) die Vertraulichkeit, Integrität oder vollständige Verfügbarkeit und den normalen Betrieb eines Lieferantensystems oder eines Barclays-Systems gefährdet hat oder dazu führen kann.

Datenschutz-Folgenabschätzung bezeichnet eine Beurteilung der Auswirkungen der geplanten Verarbeitungsvorgänge auf den Schutz personenbezogener Daten, wie sie in den Datenschutzgesetzen vorgeschrieben ist.

Datenschutzgesetzgebung bedeutet, soweit dies für die Erfüllung der Verpflichtungen des Lieferanten aus einem Vertrag gilt: (i) die EU-Richtlinie über den Datenschutz und die elektronische Kommunikation 2002/58/EG (in ihrer jeweils geänderten oder ersetzten Fassung), (ii) die EU-Datenschutz-Grundverordnung 2016/679 (**DSGVO**), Entscheidungen und Leitlinien der Europäischen Kommission und alle nationalen Durchführungsgesetze, (iii) die britische GDPR, (iv) die Bestimmungen des Gramm–Leach–Bliley Act über nicht-öffentliche personenbezogene Daten, (V) der Health Insurance Portability and Accountability Act 1996 und (vi) alle anderen anwendbaren Gesetze, Verordnungen und aufsichtsrechtlichen Leitlinien in Bezug auf Datenschutz und Privatsphäre in (a) allen Ländern, in denen sich die jeweilige Barclays-Unternehmen befindet, die Pflichten der Lieferanten erfüllt werden, der jeweilige Betroffene seinen Sitz hat, oder geschützte personenbezogene Daten verarbeitet, gespeichert oder verwendet werden und (b) in jedem Land, von dem aus der Lieferant eine seiner Verpflichtungen aus einem Vertrag erfüllt.

Datenschutz-Kontrollpflichten sind alle Datenschutzpläne, die einen Bestandteil von Anhang 7 (Pflichten zur Kontrolle externer Lieferanten) bilden.

Betroffene Person hat die diesem Begriff in den Datenschutzgesetzen verliehene Bedeutung. Wo ein solcher Begriff durch Datenschutzgesetzgebung nicht definiert ist, bezeichnet er eine natürliche Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung einer Kennung wie einem Namen, einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Datenübermittlungsvereinbarung bezeichnet eine Datenübermittlungsvereinbarung zu den Bedingungen, die von Barclays nach vernünftigem Ermessen festgelegt werden, um sicherzustellen, dass die Übermittlung je nach Sachlage der relevanten personenbezogenen Daten aus Großbritannien, der personenbezogenen Daten aus der EU und/oder von nicht-EU/nicht-UK-personenbezogenen Daten (falls zutreffend) angemessenen Sicherheitsmaßnahmen unterliegt, wie sie in den Datenschutzgesetzen vorgeschrieben sind.

Bewährte Branchenpraxis bezeichnet in Bezug auf jede Unternehmung und unter allen Umständen die Ausübung des höchsten Grades an Geschick, Sorgfalt, Umsicht und Weitsicht, die vernünftigerweise von einem hochqualifizierten und erfahrenen Menschen erwartet werden würde, der unter denselben oder ähnlichen Umständen in der gleichen Art von Unternehmen tätig ist.

Personenbezogene Daten hat die diesem Begriff in den Datenschutzgesetzen zugewiesene Bedeutung. Sofern dieser Begriff nicht durch die Datenschutzgesetze definiert ist, bezeichnet er alle Informationen, die sich auf eine betroffene Person beziehen oder diese direkt oder indirekt identifizieren.

Verletzung personenbezogener Daten hat die diesem Begriff in den Datenschutzgesetzen zugewiesene Bedeutung Wenn dieser Begriff nicht durch die Datenschutzgesetze definiert ist, bezeichnet er jede Sicherheitsverletzung, die zu unbeabsichtigter oder widerrechtlicher Vernichtung, Verlust, Änderung, unberechtigter Offenlegung oder unberechtigtem Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete Daten führt.

Verarbeitung hat die diesem Begriff in den Datenschutzgesetzen zugewiesene Bedeutung. Sofern dieser Begriff nicht durch die Datenschutzgesetze definiert ist, bezeichnet er alle Vorgänge oder Betriebsabläufe, die mit personenbezogenen Daten durchgeführt werden, unabhängig davon, ob sie automatisch erfolgen, wie z. B. Erfassung, Aufzeichnung, Organisation, Speicherung, Anpassung oder Änderung, Abruf, Konsultation, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder anderweitige Verfügbarmachung, Angleichung oder Kombination, Sperrung, Löschung oder Vernichtung; **verarbeiten** und **verarbeitet** haben die entsprechende Bedeutung.

Unterauftragnehmer bezeichnet Dritte, die bisweilen Waren liefern und/oder Dienstleistungen erbringen in Verbindung mit: (A) der Verfügbarmachung von Produkten, Erbringung von Dienstleistungen und/oder lieferbaren Leistungen und/oder (b) die Verarbeitung oder sonstige Nutzung geschützter personenbezogener Daten gemäß einem Vertrag.

Mitarbeiter des Lieferanten/Dritten bezeichnet alle Personen und/oder Organisationen, die einen Teil der Dienstleistungen erbringen oder Produkte im Rahmen eines Vertrags liefern, samt ihren Mitarbeitern, Unterauftragnehmern und/oder Vertretern des Lieferanten oder seiner Unterauftragnehmer.

Systeme von Lieferanten/Dritten sind alle elektronischen Informationssysteme (die eines oder mehrere von Hardware, Geräte, Software, Peripheriegeräte und Kommunikationsnetzwerke umfassen können), die (oder von denen ein Teil): (i) zur Lieferung von Produkten oder Erbringung von Dienstleistungen

für ein angeschlossenes Unternehmen von Barclays im Zusammenhang mit einem Vertrag oder (ii) zur Wartung, Verwaltung, Überwachung oder unter der Kontrolle des Lieferanten oder eines Unterauftragnehmers im Zusammenhang mit einem Vertrag eingesetzt werden.

System bezeichnet jedes elektronische Informationssystem (das eines oder mehrere von Hardware, Geräte, Software, Peripheriegeräte und Kommunikationsnetze umfassen kann), das (oder ein Teil dessen) eingesetzt wird, um für ein verbundenes Unternehmen von Barclays in Verbindung mit einem Vertrag Waren zu liefern oder Dienstleistungen zu erbringen.