Kontrollpflichten externer Lieferanten

Informations- und Cyber-Sicherheit

Für Lieferanten der Kategorie „Geringes Informations- und Cyber-Risiko“

Version 9.0, April 2019

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Steuerung, Richtlinien und Standards in Bezug auf die Informations-/Cyber-Sicherheit	Beim Lieferanten müssen Prozesse zur Steuerung von Informations-/Cyber-Risiken eingerichtet sein, mit denen das Verständnis der Technologie-Umgebung und des Zustands von Informations- und Cyber-Sicherheitskontrollen sichergestellt wird, sowie ein Sicherheitsprogramm zum Schutz des Lieferanten vor Cyber-Bedrohungen gemäß den bewährten Praktiken der Branche (unter anderem NIST, SANS, ISO27001) und den anwendbaren branchenspezifischen Anforderungen. Der Lieferant nimmt regelmäßig Risikobewertungen bezüglich der Informations-/Cyber-Sicherheit vor und implementiert entsprechende Kontrollen bzw. trifft alle erforderlichen Maßnahmen zur Minderung der erkannten Risiken. Der Lieferant muss vom Führungsstab genehmigte Richtlinien sowie Standards für das Management des Informations-/Cyber-Risikos des Lieferanten einhalten. Der Lieferant muss Funktionen und Verantwortlichkeiten für die Informations-/Cyber-Sicherheit definieren.	Wird diese Kontrolle nicht umgesetzt, gibt es bei Barclays oder bei Lieferanten von Barclays möglicherweise keine angemessene Aufsicht oder keine nachweislich vorhandene Aufsichtsfähigkeit in Sachen Informations-/Cyber-Sicherheit. Dokumentierte Richtlinien und Standards sind unverzichtbare Elemente für das Risikomanagement und die Risikosteuerung. In ihnen wird die Einschätzung des Managements zu den Kontrollen festgelegt, die erforderlich sind, um das Informations-/Cyber-Risiko zu managen.
2. Vorfallmanagementprozess	Es muss ein Vorfallbehandlungsprozess für die zeitnahe Abwicklung und regelmäßige Meldung von Vorfällen im Zusammenhang mit Informationen von Barclays und/oder von Barclays genutzten Diensten eingerichtet sein und verwaltet werden. Im Rahmen des Verfahrens der Vorfallbehandlung muss Folgendes festgelegt sein: • Sicherheitsvorfälle und Datenschutzverletzungen, die sich auf Ressourcen von Barclays und/oder auf Dienste, die für Barclays erbracht werden, ausgewirkt haben oder dagegen gerichtet waren, müssen Barclays unverzüglich gemeldet werden und es müssen Mitteilungen zum Stand der Abhilfemaßnahmen gemacht werden. • Der Lieferant muss dafür sorgen, dass die festgelegten Abhilfemaßnahmen nach einem Vorfall gemäß einem Abhilfeplan (Aktion, Zuständigkeit, Frist) ausgeführt und Barclays mitgeteilt werden.	Mit Hilfe eines Vorfallmanagement- und Vorfallbehandlungsprozesses wird sichergestellt, dass Vorfälle schnell in Grenzen gehalten werden und verhindert wird, dass sie sich ausweiten.

3. Endpunkt-Sicherheit	Der Lieferant muss sicherstellen, dass die für den Zugriff auf das Netzwerk von Barclays oder für die Verarbeitung von Daten von Barclays verwendeten Endpunkte zum Schutz vor Angriffen verstärkt werden. Hierzu zählen unter anderem die Begrenzung der Angriffsfläche durch Deaktivierung von Software/Diensten/Ports, die nicht benötigt werden, die Sicherstellung, dass alle bereitgestellten Versionen nur innerhalb der offiziellen Supportzeiträume eingesetzt werden, dass Malware-Schutz und Host-Firewall-Fähigkeiten vorhanden und angemessen konfiguriert sind und dass Kontrollen vorhanden sind, um Versuche zur Ausnutzung von Schwachstellen zu entschärfen.	Wird diese Kontrolle nicht umgesetzt, sind das Netzwerk und Endpunkte von Barclays und dem Lieferanten möglicherweise für Cyber-Angriffe anfällig.
4. Cloud-Computing	Jede Nutzung von (öffentlichen / privaten / gemeinschaftlichen / hybriden) Cloud-Computing-Diensten. Jede SaaS / PaaS / IaaS, die im Rahmen der Erbringung von Diensten für Barclays verwendet wird, muss angemessen geschützt werden. Kontrollen zum Schutz der Informationen von Barclays und des Dienstes müssen dem Risikoprofil und der Kritikalität der Informationsressource angemessen sein, um Datenleckagen und Cyber-Verletzungen zu verhindern.	Wird dieses Prinzip nicht umgesetzt, könnten unangemessen geschützte Informationsressourcen von Barclays gefährdet werden, was rechtliche und behördliche Strafmaßnahmen oder Rufschädigung zur Folge haben kann.
5. Malware-Schutz	Es müssen Anti-Malware-Kontrollen und -Tools vorhanden sein, um einen angemessenen Schutz vor gefährlicher Software wie Viren und anderen Malware-Varianten zu gewährleisten.	Anti-Malware-Lösungen sind für den Schutz der Informationsressourcen von Barclays gegen Schadcode von entscheidender Bedeutung.
6. Netzwerksicherheit	Der Lieferant muss sicherstellen, dass sämtliche vom Lieferanten oder von dessen Subunternehmen betriebenen IT-Systeme, mit denen für Barclays erbrachte Dienste unterstützt werden, vor Seitwärtsbewegungen von Bedrohungen im Netzwerk des Lieferanten (und jeglicher relevanter Subunternehmen) geschützt sind. Je nach dem (den) vom Lieferanten für Barclays erbrachten Dienst(en) sollte der Lieferant folgende Schutzmechanismen in Betracht ziehen: **Externe Verbindungen:** Alle externen Verbindungen zum Netzwerk müssen dokumentiert sein, durch eine Firewall geleitet und vor ihrer Aktivierung geprüft und genehmigt werden, um Verletzungen der Datensicherheit zu verhindern. **Drahtloszugang:**	Bei Nichtbeachtung dieses Prinzips könnten externe oder interne Netzwerke durch Angreifer unterwandert werden, die sich dadurch Zugang zum Dienst bzw. den damit verbundenen Daten verschaffen wollen.

	Jeder drahtlose Zugang zum Netzwerk muss durch Protokolle zur Autorisierung, Authentifizierung, Trennung und Verschlüsselung überwacht werden, um Sicherheitsverletzungen zu vermeiden. **Erkennung/Verhinderung von Eindringversuchen:** Tools und Systeme zur Erkennung und Verhinderung von Eindringversuchen müssen an allen relevanten Punkten des Netzwerks bereitgestellt und ausgehende Datenströme entsprechend überwacht werden, um Verletzungen der Cyber-Sicherheit wie APTs (Advanced Persistent Threats) zu erkennen. **DDoS (Distributed Denial of Service, verteilte Überlastangriffe):** Das Netzwerk und die wichtigsten Systeme müssen mit einem gestaffelten Sicherheitskonzept versehen sein, das jederzeit einen Schutz vor Dienstunterbrechungen durch Attacken aus dem Internet bietet. *Anm.: Als „Netzwerk" wird in dieser Kontrolle jedes nicht zu Barclays gehörige Netzwerk bezeichnet, für das der Lieferant verantwortlich ist, darunter auch Netzwerke von Subunternehmen des Lieferanten.*	
7. Schutz von Anwendungen	Die Software-/Anwendungsentwicklung des Lieferanten stellt sicher, dass alle grundlegenden Sicherheitsmaßnahmen in den Softwareentwicklungsprozess eingebunden sind, um Dienstunterbrechungen, Sicherheitslücken und Verletzungen der Cyber-Sicherheit zu vermeiden. Der Lieferant stellt sicher, dass bei der Systementwicklung Aufgabentrennung besteht. Dazu gehört auch, dass Systementwickler keinen Zugriff auf die Live-Umgebung erhalten, sofern nicht ein Notfall vorliegt, bei dem dieser Zugriff durch angemessene Kontrollen wie Break-Glass-Prozeduren geschützt wäre. Unter diesen Umständen müssen solche Maßnahmen protokolliert und einer Überprüfung durch unabhängige Dritte unterzogen werden. Der Lieferant muss sicherstellen, dass Quellcode auf sichere Weise ausgeführt, gespeichert und an Barclays gesendet wird.	Kontrollen zum Schutz der Anwendungsentwicklung helfen, dafür zu sorgen, dass Anwendungen beim Einsatz geschützt sind.
8. Bedrohungssimulation / Penetrationstests / IT-Sicherheitsbewertung	Der Lieferant muss unter Einbeziehung eines unabhängigen qualifizierten Sicherheitsdienstleisters eine IT-Sicherheitsbewertung / Penetrationstests durchführen, die sich auf die IT-Infrastruktur und Anwendungen im Zusammenhang mit dem (den) vom Lieferanten an Barclays erbrachten Dienst(en) beziehen.	Wird diese Kontrolle nicht umgesetzt, sind Lieferanten möglicherweise nicht in der Lage, die Cyber-Bedrohungen, mit denen sie es zu tun haben, und die Angemessenheit

	Dies muss mindestens einmal jährlich erfolgen, um Schwachstellen zu identifizieren, die ausgenutzt werden könnten, um die Vertraulichkeit der Daten von Barclays durch Cyberangriffe zu verletzen. Der Lieferant muss einen einheitlichen Mechanismus für die Erfassung, Einteilung und Behandlung identifizierter Schwachstellen zum Einsatz bringen.	und Stärke ihrer Abwehrmaßnahmen einzuschätzen.
9. Technologien des Ressourcen- und Sicherheitsschutzes	Es müssen geeignete Technologien angewendet werden, um aktuellen und aufkommenden Cyber-Bedrohungen mit einer einheitlichen Basis an Kontrollen zu begegnen, die aufrechterhalten werden, um die Zuführung, Ausführung und Ausnutzung von Angriffen sowie die Exfiltration zu verhindern. Hostsysteme und Netzwerkgeräte, die Bestandteil der Lieferantensysteme sind, müssen so konfiguriert sein, dass sie gemäß den bewährten Praktiken der Branche (z. B. NIST, SANS, ISO27001) funktionieren. Die Ressourcen oder Systeme zur Speicherung oder Verarbeitung müssen vor physischer Manipulation, Verlust, Schäden oder Beschlagnahme sowie unsachgemäßer Konfiguration oder unsachgemäßen Änderungen geschützt werden. Bei Informationsressourcen von Barclays, ob in physischer oder elektronischer Form gespeichert, muss im Falle der Vernichtung oder Löschung auf sichere und dem damit verbundenen Risiko entsprechende Art und Weise vorgegangen werden, damit sie nicht wiederherstellbar sind. Systeme müssen sicher konfiguriert sein, um unnötige Rechtsverletzungen und Verstöße zu verhindern. Zum Erkennen unerwünschter oder böswilliger Aktivitäten müssen die Systeme über Automatismen für Überwachung, Audit und Protokollierung verfügen.	Wird diese Kontrolle nicht umgesetzt, könnten Ressourcen von Barclays oder von Lieferanten zum Erbringen von Diensten für Barclays genutzte Ressourcen beeinträchtigt werden, was finanzielle Verluste, Datenverlust, Rufschädigung und Verweise von Aufsichtsbehörden nach sich ziehen kann.

10. Logische Zugriffsverwaltung (Logical Access Management (LAM))	Der Zugriff auf Informationen muss eingeschränkt sein und unter gebührender Berücksichtigung der Grundsätze des Wissensbedarfs, der Minimalberechtigung und der Aufgabentrennung erfolgen. Dem Verantwortlichen für die Informationsressource obliegt die Entscheidung darüber, wer welchen Zugriff benötigt. • Der Grundsatz des Wissensbedarfs besagt, dass Personen nur auf Informationen Zugriff haben sollten, deren Kenntnis sie zur Erfüllung der ihnen ordnungsgemäß übertragenen Aufgaben benötigen. Wenn zum Beispiel ein Mitarbeiter nur Umgang mit Kunden im Vereinigten Königreich hat, besteht bei ihm kein Wissensbedarf in Bezug auf Informationen zu Kunden in den USA. • Der Grundsatz der Minimalberechtigung besagt, dass Personen nur den Mindestumfang an Berechtigungen haben sollten, die zur Erfüllung der ihnen ordnungsgemäß übertragenen Aufgaben erforderlich sind. Wenn zum Beispiel ein Mitarbeiter die Adresse eines Kunden einsehen, diese aber nicht ändern muss, benötigt er nach dem Grundsatz der Minimalberechtigung Nur-Lese-Zugriff. Dieser sollte dem Mitarbeiter verschafft werden, Schreib-/Lese-Zugriff hingegen nicht. • Der Grundsatz der Aufgabentrennung besagt, dass zur Verhinderung von Fehlern und Betrug mindestens zwei Einzelpersonen für die separaten Bestandteile einer Aufgabenstellung verantwortlich sind. Wenn zum Beispiel ein Mitarbeiter die Erstellung eines Kontos beantragt, sollte der Antrag nicht von ihm, sondern von einem anderen genehmigt werden.	Angemessene LAM-Kontrollen helfen dabei, sicherzustellen, dass Informationsressourcen vor unangemessener Verwendung geschützt werden.

	Diese Grundsätze sollten auf der Basis des Risikos angewendet werden, unter Berücksichtigung der Vertraulichkeitseinstufung der Informationen. Jedes Konto muss einer einzelnen Person zugeordnet sein, die für sämtliche mit dem Konto durchgeführten Aktivitäten verantwortlich ist. Dies steht der Verwendung von gemeinsam genutzten Konten nicht entgegen, allerdings muss auch für jedes gemeinsam genutzte Konto eine einzelne Person verantwortlich sein. Zugriffsverwaltungsprozesse müssen gemäß den bewährten Praktiken der Branche definiert sein und mindestens Folgendes beinhalten: • Vorhandensein eines robusten Autorisierungsprozesses, bevor Konten erstellt/geändert/gelöscht werden; • regelmäßig durchgeführter Prozess zur Überprüfung des Zugriffs eines Benutzerkontos; • Kontrollen für Personen, die in eine neue Position gewechselt sind – Zugriffsmöglichkeiten innerhalb von fünf Arbeitstagen nach dem Datum des Wechsels geändert/entfernt; • Kontrollen für ausscheidende Personen – sämtliche zum Erbringen von Diensten für Barclays verwendeten logischen Zugriffsmöglichkeiten werden innerhalb von 24 Stunden nach dem Zeitpunkt des Ausscheidens entfernt, alle anderen sekundären Zugriffsmöglichkeiten werden innerhalb von sieben Tagen entfernt; und • ruhende Konten, die 60 Tage in Folge oder länger nicht verwendet wurden, müssen gesperrt werden. • Passwörter für interaktive Konten müssen mindestens alle 90 Tage geändert werden und sich von den zwölf (12) vorherigen Passwörtern unterscheiden. • Passwörter für privilegierte Konten müssen nach jedem Gebrauch, mindestens jedoch alle 90 Tage, geändert werden. • Interaktive Konten müssen spätestens nach fünf (5) fehlgeschlagenen Versuchen in Folge deaktiviert werden. Wenn der Fernzugriff auf Informationsressourcen von Barclays, die in einer vom Lieferanten verwalteten Umgebung gespeichert werden, erlaubt ist, muss eine Zwei-Faktor-Authentifizierung und Autorisierung des Endpunktes unter Berücksichtigung der Identität des Benutzers, des Gerätetyps und des Sicherheitsstatus des Gerätes (z. B. Patch-Level, Status von Anti-Malware, Mobilgerät mit vollen Administratorrechten (Root) oder ohne Root usw.) vorgenommen werden.	

11. Verhinderung von Datenleckagen	Das Risiko von Datenleckagen, bei denen Informationen im Zusammenhang mit dem (den) vom Lieferanten für Barclays erbrachten Dienst(en) durch das Netzwerk oder ein physisches Medium austreten, muss bewertet und vermindert werden. Folgende Kanäle für Datenleckagen sind zu berücksichtigen: • Unzulässige Übertragung von Informationen außerhalb des internen Netzwerks bzw. außerhalb des Netzwerks des Lieferanten. • Verlust oder Diebstahl von Informationsressourcen von Barclays, die sich auf tragbaren elektronischen Medien befinden (darunter Informationen in elektronischer Form auf Laptops, Mobilgeräten sowie tragbaren Medien); • Unsicherer Austausch von Informationen mit Dritten; und • Unangebrachtes Ausdrucken oder Kopieren von Informationen	Angemessene Kontrollen zur Verhinderung von Datenleckagen sind ein wichtiges Element der Informationssicherheit, denn sie helfen dabei, sicherzustellen, dass Informationen von Barclays nicht verloren gehen.
12. Kennzeichnungsschema für Informationen	***Gegebenenfalls**** muss der Lieferant für sämtliche im Auftrag von Barclays gehaltenen oder verarbeiteten Informationsressourcen das Barclays-Kennzeichnungsschema für Informationen und die Anforderungen an die Handhabung (Anhang B, Tabelle B1 und B2) anwenden, oder ein mit Barclays vereinbartes alternatives Schema. * *Der Ausdruck „**gegebenenfalls**“ bezieht sich auf den Nutzen der Kennzeichnung im Vergleich zu den damit verbundenen Kosten. Beispielsweise kann die Beschriftung eines Dokuments unangemessen sein, wenn diese einen Verstoß gegen etwaige Manipulationsschutzvorschriften bedeuten würde.*	Eine vollständige und genaue Bestandsliste der Informationsressourcen ist unverzichtbar, um sicherzustellen, dass die Kontrollen angemessen sind.
13. Inspektionsrecht	Zur Überprüfung der Erfüllung der Vertragspflichten des Lieferanten muss der Lieferant Barclays erlauben, nachdem Barclays dies mindestens zehn Geschäftstage zuvor schriftlich angekündigt hat, eine Sicherheitsüberprüfung jedes Standorts oder jeder Technologie vorzunehmen, der bzw. die vom Lieferanten oder von dessen Subunternehmen 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, unmittelbar nach einem Sicherheitsvorfall eine Inspektion durchzuführen. Zu jeder von Barclays bei einer Inspektion identifizierten Nichterfüllung von Kontrollen nimmt Barclays eine Risikobewertung vor und Barclays gibt einen Zeitrahmen für Abstellmaßnahmen vor. Anschließend muss der Lieferant etwaige geforderte Abstellmaßnahmen innerhalb dieses Zeitrahmens ausführen. Soweit von Barclays angefordert, leistet der Lieferant bei jeder Inspektion Unterstützung in angemessener Weise.	Sofern dies nicht vereinbart wurde, sind Lieferanten nicht in der Lage, die Einhaltung dieser Sicherheitspflichten vollumfänglich abzusichern.

Anhang A: Glossar

Definition	
APT (Advanced Persistent Threat)	Ein APT (Advanced Persistent Threat) ist ein verdeckter Computernetz-Angriff, bei dem sich eine Person oder eine Gruppe unbefugten Zugriff auf ein Netzwerk verschafft und längere Zeit unentdeckt bleibt.
Benutzerkonto	Konto ohne besondere Rechte, das einem Mitarbeiter, einem Berater, einem Auftragnehmer oder einer Zeitarbeitskraft des Lieferanten zugeteilt wurde, der bzw. die zum Zugriff auf ein System berechtigt ist.
DoS(-Angriff) (Denial of Service)	Versuch, die Verfügbarkeit einer Computerressource für ihre vorgesehenen Benutzer aufzuheben.
Gemeinsam genutztes Konto	Konto, das mehreren Mitarbeitern, Beratern, Auftragnehmern oder Zeitarbeitskräften mit Zugriffsberechtigung überlassen wird, wenn Einzelkonten aufgrund der Art des Systems, auf das zugegriffen wird, keine zur Verfügung gestellte Option sind.
Informationsressource	Alle Informationen, denen ein Wert im Hinblick auf ihre Anforderungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit beigemessen wird. Jegliche Einzelinformation oder Gruppe von Informationen, die einen Wert für die Organisation hat. Die Gruppierung erfolgt in der Regel auf hoher Ebene (von Geschäftsprozessen).
Konto	Ein Satz von Anmeldedaten (z. B. eine Benutzerkennung und ein Passwort), durch die der Zugriff auf ein IT-System mithilfe logischer Zugriffssteuerungen verwaltet wird.
Minimalberechtigung	Der Mindestumfang an Zugriffsrechten/Genehmigungen, mit denen einem Benutzer oder Konto die Erfüllung seiner geschäftlichen Funktion ermöglicht wird.
Multi-Faktor-Authentifizierung	Authentifizierung mit zwei oder mehr unterschiedlichen Authentifizierungstechniken. Ein Beispiel ist die Verwendung eines Sicherheits-Tokens. Erforderlich für eine erfolgreiche Authentifizierung ist dabei etwas, das sich im Besitz der betreffenden Einzelperson befindet (d. h. das Sicherheits-Token), und etwas, das dem Benutzer bekannt ist (d. h. die Sicherheits-Token-PIN).
Privilegiertes Konto	Ein Konto, das ein höheres Maß an Kontrolle über ein spezifisches IT-System bietet. Solche Konten werden in der Regel für Systemwartung, Sicherheitsverwaltung oder Konfigurationsänderungen an einem IT-System verwendet. Beispiele sind „Administrator“, „Stammverzeichnis“, Unix-Konten mit uid=0, Supportkonten, Sicherheitsadministratorkonten, Systemadministratorkonten und lokale Administratorkonten.
Schadcode	Software, die in der Absicht erstellt wurde, die Sicherheitsrichtlinien eines IT-Systems, eines IT-Geräts oder einer IT-Anwendung zu umgehen. Beispiele sind Computerviren, Trojaner und Würmer.
System	Ein System im Kontext dieses Dokuments sind Personen, Verfahren, IT-Geräte und Software. Die Elemente dieses zusammengesetzten Gebildes werden zusammen in der vorgesehenen Betriebs- oder Support-Umgebung verwendet, um eine bestimmte Aufgabe zu verrichten oder einem bestimmten Zweck gerecht zu werden, Support zu leisten oder eine Einsatzanforderung zu erfüllen.
Vernichtung/ Löschung	Das Überschreiben, Auslöschen oder physische Zerstören von Informationen auf eine solche Art und Weise, dass sie nicht wiederherstellbar sind.

Anhang B: Barclays-Kennzeichnungsschema für Informationen

Tabelle B1: 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 Framework (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 potenzielle Firmenzusammenschlüsse oder -übernahmen. • Informationen zur strategischen Planung – das Geschäft und die Organisation betreffend. • Bestimmte Konfigurationen der Informationssicherheit. • 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 Jahresergebnisse (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). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Strategien und Budgets. • Leistungsbeurteilungen. • Vergütung und personenbezogene Daten von Mitarbeitern. • Schwachstellenbewertungen. • Befunde und Berichte einer Betriebsprüfung.
Eingeschränkt – Extern	Informationen müssen als Eingeschränkt – Extern kategorisiert werden, wenn es sich bei den voraussichtlichen Empfängern um authentifizierte	• Neue Produktpläne. • Klientenverträge.

	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.	• 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.
Uneingeschränkt	Informationen, die entweder für die allgemeine Verbreitung bestimmt sind oder die im Falle ihrer Verbreitung keine Auswirkungen auf die Organisation haben würden.	• Marketingmaterial. • Veröffentlichungen. • Öffentliche Bekanntgaben. • Stellenausschreibungen. • Informationen ohne Auswirkungen auf Barclays.

Tabelle B2: Barclays-Kennzeichnungsschema für Informationen – Anforderungen an die Handhabung

*** 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	Eingeschränkt – Intern	Eingeschränkt – Extern	Geheim
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 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 geeignete Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht.	• 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 geeignete 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.
Zugriff und Verwendung	• 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 geeignete 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 geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Gedruckte Ressourcen müssen sofort aus dem Drucker entnommen werden. Ist dies nicht möglich, müssen sichere Druckprogramme verwendet werden. • Elektronische Ressourcen müssen durch geeignete 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 geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Für den Druck vorgesehene Ressourcen müssen mithilfe sicherer Druckprogramme gedruckt werden. • Elektronische Ressourcen müssen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.
Weitergabe	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung erhalten. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein. • Elektronische Ressourcen müssen eine deutliche Informationsbeschriftung tragen.	• Ausgedruckte Ressourcen müssen eine sichtbare Informationsbeschriftung tragen. Die Beschriftung muss mindestens auf der Vorderseite zu lesen sein.	• Ausgedruckte Ressourcen 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.	• 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, 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 Datenübertragung außerhalb des internen Netzwerks verläuft.	• 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. • Ressourcen dürfen nicht per Fax gesendet werden. • Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübertragung außerhalb des internen Netzwerks verläuft. • Für elektronische Ressourcen muss eine Kontrollkette geführt werden.

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.	• 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. • Medien, auf denen als „Geheim” eingestufte elektronische Ressourcen gespeichert wurden, müssen vor oder während der Entsorgung entsprechend bereinigt werden.

Bankgeheimnis

Zusätzliche Kontrollen nur für Länder mit Bankgeheimnis (Schweiz/Monaco)

Kontrollbereich / Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Funktionen und Verantwortlichkeiten	Der Lieferant muss Funktionen und Verantwortlichkeiten für die Handhabung von Daten, durch die Kunden identifiziert werden (Client Identifying Data, nachfolgend CID genannt), definieren und kommunizieren. Der Lieferant muss nach jeder am Betriebsmodell (oder Geschäft) des Lieferanten vorgenommenen Änderung oder mindestens einmal im Jahr die Dokumente überprüfen, in denen die Funktionen und Verantwortlichkeiten für CID näher beschrieben sind, und er muss sie in dem betreffenden Land mit Bankgeheimnis verteilen. Wesentliche Funktionen sind unter anderem ein leitender Angestellter, der für den Schutz und die Aufsicht über sämtliche mit CID zusammenhängenden Aktivitäten zuständig ist (Definition von CID ist Anhang A zu entnehmen).	Durch die klare Definition von Funktionen und Verantwortlichkeiten wird die Umsetzung des Vertragsanhangs „Kontrollpflichten externer Lieferanten“ unterstützt.
2. Berichterstattung über Verstöße im Zusammenhang mit CID	Um sicherzustellen, dass Verstöße mit Auswirkungen auf CID gemeldet und verwaltet werden, müssen dokumentierte Kontrollmechanismen und Prozesse vorhanden sein. Der Lieferant muss auf jede Nichteinhaltung der (in Tabelle C2 definierten) Anforderungen an die Handhabung reagieren und die Nichteinhaltung muss dem entsprechenden Land mit Bankgeheimnis sofort (spätestens innerhalb von 24 Stunden) gemeldet werden. Es muss ein Vorfallbehandlungsprozess für die zeitnahe Abwicklung und regelmäßige Meldung von Ereignissen, die CID betreffen, eingerichtet werden. Der Lieferant muss dafür sorgen, dass die festgelegten Abhilfemaßnahmen nach einem Vorfall gemäß einem Abhilfeplan (Aktion, Zuständigkeit, Frist) ausgeführt und mit dem entsprechenden Land mit Bankgeheimnis abgesprochen und vereinbart werden.	Mit Hilfe eines Vorfallbehandlungsprozesses wird sichergestellt, dass Vorfälle schnell eingedämmt werden und verhindert wird, dass sie sich ausweiten. Jede Nichteinhaltung mit Auswirkungen auf CID könnte Barclays schwere Rufschädigungen zufügen sowie Geldbußen und den Verlust der Banklizenz in der Schweiz oder in Monaco nach sich ziehen.

3. Weiterbildung und Awareness	Mitarbeiter des Lieferanten, die Zugriff auf CID haben und/oder diese handhaben, müssen nach jeder neuen Änderung der Vorschriften oder mindestens einmal im Jahr eine Schulung* absolvieren, bei der die Anforderungen des Bankgeheimnisses an CID umgesetzt werden. Der Lieferant muss dafür sorgen, dass alle neuen Mitarbeiter des Lieferanten (die Zugriff auf CID haben und/oder diese handhaben) innerhalb eines angemessenen Zeitraums (ca. 3 Monate) eine Schulung absolvieren, mit der sichergestellt wird, dass sie sich über ihre Verantwortlichkeiten in Bezug auf CID im Klaren sind. Der Lieferant muss den Überblick darüber behalten, welche Mitarbeiter die Schulung absolviert haben. * Länder mit Bankgeheimnis geben noch Anleitungen zu den erwarteten Inhalten der Schulung.	Durch Weiterbildung und Awareness werden alle anderen Kontrollen im Rahmen dieses Vertragsanhangs unterstützt.
4. Kennzeichnungsschema für Informationen	***Gegebenenfalls**** muss der Lieferant für sämtliche im Auftrag des betreffenden Landes mit Bankgeheimnis gehaltenen oder verarbeiteten Informationsressourcen das Barclays-Kennzeichnungsschema für Informationen (Tabelle C1 von Anhang C) anwenden, oder ein mit dem Land mit Bankgeheimnis vereinbartes alternatives Schema. Die Anforderungen an die Handhabung bei CID-Daten sind in Tabelle C2 von Anhang C festgelegt. * *Der Ausdruck „**gegebenenfalls**“ bezieht sich auf den Nutzen der Kennzeichnung im Vergleich zu den damit verbundenen Kosten. Beispielsweise kann die Beschriftung eines Dokuments unangemessen sein, wenn diese einen Verstoß gegen etwaige Manipulationsschutzvorschriften bedeuten würde.*	Eine vollständige und genaue Bestandsliste der Informationsressourcen ist unverzichtbar, um sicherzustellen, dass die Kontrollen angemessen sind.
5. Cloud-Computing / externe Speicherung	Jede Nutzung von Cloud-Computing und/oder externer Speicherung von CID (auf Servern außerhalb des Landes mit Bankgeheimnis oder außerhalb der Infrastruktur des Lieferanten), die im Rahmen des Dienstes für das betreffende Land verwendet werden, bedarf der Genehmigung durch die entsprechenden relevanten lokalen Teams (einschließlich des Chief Security Office, der Abteilung Compliance und der Rechtsabteilung); und damit CID im Hinblick auf ihr hohes Risikoprofil ausreichend geschützt sind, müssen Kontrollen im Einklang mit den Vorschriften im betreffenden Land mit Bankgeheimnis umgesetzt werden.	Wird dieses Prinzip nicht umgesetzt, könnten unangemessen geschützte Kundendaten (CID) gefährdet werden, was rechtliche und behördliche Strafmaßnahmen oder Rufschädigung zur Folge haben kann.

** Daten, durch die Kunden identifiziert werden, sind spezielle Daten auf Grund der in der Schweiz und in Monaco gültigen Gesetze zum Bankgeheimnis. Deshalb verstehen sich die Kontrollen, die hier aufgeführt sind, als Ergänzung zu den oben aufgeführten Kontrollen.

Ausdruck	Definition
CID	Daten, durch die Kunden identifiziert werden (Client Identifying Data)
CIS	Cyber-Sicherheit und Informationssicherheit
Mitarbeiter des Lieferanten	Jegliche dem Lieferanten als festangestellte(r) Mitarbeiter(in) direkt zuzuordnende Einzelperson, oder jegliche Einzelperson, die dem Lieferanten zeitlich begrenzt Leistungen erbringt (z. B. Berater(in))
Ressource	Jegliche Einzelinformation oder Gruppe von Informationen, die einen Wert für die Organisation hat
System	Ein System im Kontext dieses Dokuments sind Personen, Verfahren, IT-Geräte und Software. Die Elemente dieses zusammengesetzten Gebildes werden zusammen in der vorgesehenen Betriebs- oder Support-Umgebung verwendet, um eine bestimmte Aufgabe zu verrichten oder einem bestimmten Zweck gerecht zu werden, Support zu leisten oder eine Einsatzanforderung zu erfüllen.
Benutzer	Konto ohne besondere Rechte, das einem Mitarbeiter, einem Berater, einem Auftragnehmer oder einer Zeitarbeitskraft des Lieferanten zugeteilt wurde, der bzw. die zum Zugriff auf ein im Eigentum von Barclays befindliches System berechtigt ist.

Anhang B: DEFINITION VON DATEN, DURCH DIE KUNDEN IDENTIFIZIERT WERDEN (CLIENT IDENTIFYING DATA, CID)

Direkte CID (DCID) lassen sich definieren als (im Eigentum des Kunden befindliche) eindeutige Kennungen, die es in der vorhandenen Form und auf sich allein gestellt ermöglichen, einen Kunden zu identifizieren, ohne dass auf Daten in Bankanwendungen von Barclays zugegriffen wird. Dies muss unzweideutig sein, keine Auslegungssache, und mögliche Beispiele hierfür sind Informationen wie der Vorname, der Nachname, der Firmenname, die Unterschrift, die Kennung in sozialen Netzwerken usw. Direkte CID sind Kundendaten, die sich weder im Eigentum der Bank befinden noch von ihr erstellt wurden.

Indirekte CID (ICID) werden in drei Stufen unterteilt

- **ICID der Stufe L1** lassen sich definieren als (im Eigentum der Bank befindliche) eindeutige Kennungen, die es ermöglichen, einen Kunden eindeutig zu identifizieren, falls Zugriff auf Bankanwendungen oder sonstige **Anwendungen Dritter** gewährt wird. Die Kennung muss unzweideutig sein, keine Auslegungssache, und mögliche Beispiele hierfür sind Kennungen wie die Kontonummer, die IBAN, Kreditkartennummer usw.

- **ICID der Stufe L2** lassen sich definieren als (im Eigentum des Kunden befindliche) Informationen, die in Kombination mit einer anderen Information auf die Identität eines Kunden schließen lassen würden. Zwar lassen sich diese Informationen auf sich allein gestellt nicht zur Identifizierung eines Kunden verwenden, sie können aber mit anderen Informationen verwendet werden, um einen Kunden zu identifizieren. ICID der Stufe L2 müssen ebenso streng wie DCID geschützt und verwaltet werden.

- **ICID der Stufe L3** lassen sich definieren als (im Eigentum der Bank befindliche) eindeutige, aber anonymisierte Kennungen, die es ermöglichen, einen Kunden zu identifizieren, wenn Zugriff auf Bankanwendungen gewährt wird. Der Unterschied zu ICID der Stufe L1 besteht in der Kategorisierung der Informationen als Eingeschränkt – Extern und nicht als Bankgeheimnis, sie unterliegen also nicht den gleichen Kontrollen.

Eine Übersicht zur Methode der Kategorisierung ist der Abbildung 1, Entscheidungsbaum für CID, zu entnehmen.

Direkte CID und ICID der Stufe L1 dürfen nicht an Personen außerhalb der Bank weitergegeben werden und bei ihnen muss jederzeit der Grundsatz des Wissensbedarfs beachtet werden. ICID der Stufe L2 dürfen je nach Wissensbedarf weitergegeben werden, ihre Weitergabe darf jedoch nicht in Verbindung mit jeglichen anderen Bestandteilen von CID erfolgen. Durch die Weitergabe mehrerer Bestandteile von CID besteht die Möglichkeit, dass eine „toxische Kombination“ entsteht und die Identität eines Kunden so potenziell offenbart wird. Eine toxische Kombination definieren wir ausgehend von mindestens zwei ICID der Stufe L2. ICID der Stufe L3 dürfen weitergegeben werden, da sie nicht als Informationen auf der Stufe des Bankgeheimnisses kategorisiert sind, es sei denn, die wiederholte Verwendung derselben Kennung kann zur Erfassung von ausreichend ICID-Daten der Stufe L2 führen, so dass die Identität des Kunden offenbart wird.

Kategorisierung von Informationen	Bankgeheimnis			Eingeschränkt - Intern
Kategorie	**Direkte CID (DCID)**	**Indirekte CID (ICID)**		
		Indirekt (Stufe L1)	**Potenziell Indirekt (Stufe L2)**	**Unpersönliche Kennung (Stufe L3)**
Art der Information	Kundenname	Container-Nummer / Container-Kennung	Vorname	Kennung interne Verarbeitung
	Firmenname	Nummer des MACC (Geldkonto unter einer Avaloq-Container-Kennung)	Geburtstag	Eindeutige statische Kennung
	Kontoauszug	Adresse	Staatsangehörigkeit	Dynamische Kennung
	Unterschrift	IBAN	Titel	Externe Container-Kennung
	Kennung für soziales Netzwerk	Anmeldedaten E-Banking	Familienverhältnisse	
	Reisepass-Nummer	Nummer der Depotverwahrung	Postleitzahl	
	Telefonnummer	Kreditkartennummer	Vermögensverhältnisse	
	E-Mail-Adresse		Nachname	
	Tätigkeitsbezeichnung oder PEP-Titel		Letzter Kundenbesuch	
	Künstlername		Sprache	
	IP-Adresse		Geschlecht	

	Faxnummer		Ablaufdatum der Kreditkarte	
			Hauptansprechpartner	
			Geburtsort	
			Datum der Kontoeröffnung	
			Große Position/Transaktionswert	

Beispiel: Wenn Sie an externe Personen (einschließlich Dritte in der Schweiz / in Monaco) oder interne Kollegen in anderen verbundenen Unternehmen / Tochtergesellschaften, die in der Schweiz / in Monaco oder anderen Ländern (z. B. Vereinigtes Königreich) ansässig sind, eine E-Mail senden oder Dokumente an sie weitergeben.

1. Kundenname

   (DCID) = Verletzung des Bankgeheimnisses

2. Container-Kennung

   (ICID der Stufe L1) = Verletzung des Bankgeheimnisses

3. Vermögensverhältnisse + Staatsangehörigkeit

   (ICID der Stufe L2) + (ICID der Stufe L2) = Verletzung des Bankgeheimnisses

Anhang C: Barclays-Kennzeichnungsschema für Informationen

Tabelle C1: Barclays-Kennzeichnungsschema für Informationen

** Die Kennzeichnung „Bankgeheimnis“ ist spezifisch für Länder mit Bankgeheimnis.

Kennzeichnung	Definition	Beispiele
Bankgeheimnis	Informationen, die im Zusammenhang mit schweizerischen, Direkten oder Indirekten Daten, durch die Kunden identifiziert werden (CID), stehen. Die Kategorisierung „Bankgeheimnis“ gilt für Informationen, die im Zusammenhang mit Direkten oder Indirekten Daten, durch die Kunden identifiziert werden, stehen. Deshalb ist ein Zugriff durch sämtliche Mitarbeiter, auch wenn sie im Land der Verantwortlichkeit bzw. Verarbeitung der Informationen ansässig sind, nicht angemessen. Der Zugriff auf diese Informationen wird nur von denjenigen benötigt, die zur Erfüllung ihrer ordnungsgemäßen Aufgaben oder vertraglichen Pflichten diesbezüglich Wissensbedarf haben. Die unbefugte Offenlegung, der unbefugte Zugriff oder die unbefugte Weitergabe dieser Informationen, sowohl intern als auch außerhalb der Organisation, kann kritische Auswirkungen haben und zu strafrechtlichen Verfahren führen sowie zivilrechtliche und administrative Konsequenzen wie beispielsweise Geldbußen und den Verlust der Banklizenz nach sich ziehen, wenn die Informationen unbefugtem Personal gegenüber offengelegt werden, sowohl intern als auch extern.	• Kundenname • Adresse des Kunden • Unterschrift • IP-Adresse des Kunden (weitere Beispiele in Anhang B)

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 Framework (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 potenzielle 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 Jahresergebnisse (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). Diese Informationen sind nicht für die allgemeine Verbreitung bestimmt, die Empfänger können sie aber nach dem Grundsatz des Wissensbedarfs weiterleiten oder weitergeben.	• Strategien und Budgets. • Leistungsbeurteilungen. • Vergütung und personenbezogene Daten von Mitarbeitern. • Schwachstellenbewertungen. • Befunde und Berichte einer Betriebsprüfung.
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.
Uneingeschränkt	Informationen, die entweder für die allgemeine Verbreitung bestimmt sind oder die im Falle ihrer Verbreitung keine Auswirkungen auf die Organisation haben würden.	• Marketingmaterial. • Veröffentlichungen. • Öffentliche Bekanntgaben. • Stellenausschreibungen. • Informationen ohne Auswirkungen auf Barclays.

Tabelle C2: Kennzeichnungsschema für Informationen – Anforderungen an die Handhabung

** Spezifische Anforderungen an die Handhabung bei CID-Daten, um deren Vertraulichkeit gemäß den behördlichen Vorschriften sicherzustellen

Phase des Lebenszyklus	Anforderungen des Bankgeheimnisses
Erstellung und Kennzeichnung	Wie bei „Eingeschränkt – Extern“ sowie: • Ressourcen müssen einem Verantwortlichen für CID zugewiesen sein.
Speichern	Wie bei „Eingeschränkt – Extern“ sowie: • Ressourcen dürfen auf wechselbaren Medien nur so lange gespeichert werden, wie dies aufgrund eines spezifischen geschäftlichen Erfordernisses ausdrücklich notwendig ist oder von Aufsichtsbehörden oder externen Prüfern ausdrücklich verlangt wird. • Große Umfänge von Informationsressourcen, die dem Bankgeheimnis unterliegen, dürfen nicht auf tragbaren Geräten/Medien gespeichert werden. Weitere Informationen erteilt auf Anfrage das lokale Team für Cyber-Sicherheit und Informationssicherheit (nachstehend CIS genannt). • Gemäß dem Grundsatz des Wissensbedarfs bzw. dem Grundsatz der Erforderlichkeit des Besitzes dürfen Ressourcen (ob physisch oder elektronisch) nicht an Orten abgelegt werden, an denen unbefugte Personen in der Lage sein könnten, sie einzusehen oder auf sie zuzugreifen. • Sichere Praktiken am Arbeitsplatz, beispielsweise ein aufgeräumter Arbeitsplatz (Clear Desk) und eine Desktop-Sperre, müssen zur sicheren Aufbewahrung von Ressourcen (ob physisch oder elektronisch) eingehalten werden. • Informationsressourcen auf wechselbaren Medien dürfen für die Speicherung nur so lange verwendet werden, wie dies ausdrücklich erforderlich ist, und bei Nichtverwendung müssen sie weggeschlossen werden. • Für Ad-hoc-Datenübertragungen auf tragbare Geräte/Medien ist die Genehmigung des Verantwortlichen für die Daten, der Abteilung Compliance und der CIS erforderlich.
Zugriff und Verwendung	Wie bei „Eingeschränkt – Extern“ sowie: • Ohne die formelle Genehmigung vom Verantwortlichen für CID (oder dessen Stellvertreter) dürfen Ressourcen nicht an einen Ort außerhalb des Standorts (Räumlichkeiten von Barclays) verbracht bzw. dort eingesehen werden. • Ohne die formelle Genehmigung vom Verantwortlichen für CID (oder dessen Stellvertreter) und vom Kunden (Verzichtserklärung / beschränkte Vollmacht) dürfen Ressourcen nicht an einen Ort außerhalb des Buchungslandes des Kunden verbracht bzw. dort eingesehen werden. • Es müssen sichere Praktiken für die Telearbeit eingehalten werden, wobei sichergestellt wird, dass einem bei der Arbeit niemand über die Schulter sehen kann (kein Shoulder-Surfing), wenn physische Ressourcen an einen Ort außerhalb des Standorts verbracht werden.

	• Es muss sichergestellt werden, dass unbefugte Personen die elektronischen Ressourcen, auf denen sich CID befinden, über einen beschränkten Zugriff auf Geschäftsanwendungen weder beobachten noch darauf zugreifen können.
Weitergabe	Wie bei „Eingeschränkt – Extern“ sowie: • Ressourcen dürfen nur gemäß dem „Grundsatz des Wissensbedarfs“ UND innerhalb der Informationssysteme und unter den Mitarbeitern des Landes mit Bankgeheimnis, in dem sie entstanden sind, verteilt werden. • Für die Ad-hoc-Übertragung von Ressourcen mittels wechselbarer Medien ist die Genehmigung des Verantwortlichen für die Informationsressource und der CIS erforderlich. • Elektronische Mitteilungen müssen bei der Übertragung verschlüsselt sein. • Per Post (als Ausdruck) gesendete Ressourcen müssen mit einem Dienst zugestellt werden, bei dem eine Empfangsbestätigung verlangt wird. • Ressourcen dürfen nur nach dem „Grundsatz des Wissensbedarfs“ verteilt werden.
Archivieren und Entsorgen	Wie bei „Eingeschränkt – Extern“

*** 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	Eingeschränkt – Intern	Eingeschränkt – Extern	Geheim
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 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 geeignete Ausgleichskontrollen geschützt werden, wenn ein erhebliches Risiko des unbefugten Zugriffs besteht.	• 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 geeignete 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.
Zugriff und Verwendung	• 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 geeignete 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 geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Gedruckte Ressourcen müssen sofort aus dem Drucker entnommen werden. Ist dies nicht möglich, müssen sichere Druckprogramme verwendet werden. • Elektronische Ressourcen müssen durch geeignete 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 geeignete Kontrollmechanismen vorhanden sind (z. B. Sichtschutzelemente). • Für den Druck vorgesehene Ressourcen müssen mithilfe sicherer Druckprogramme gedruckt werden. • Elektronische Ressourcen müssen durch geeignete LAM-Kontrollmechanismen (logische Zugriffsverwaltung) geschützt werden.

Weitergabe	• 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, 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 Datenübertragung außerhalb des internen Netzwerks verläuft.	• 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. • Ressourcen dürfen nicht per Fax gesendet werden. • Elektronische Ressourcen müssen mithilfe eines zugelassenen kryptografischen Schutzmechanismus verschlüsselt werden, wenn die Datenübertragung außerhalb des internen Netzwerks verläuft.

			• Für elektronische Ressourcen muss eine Kontrollkette gepflegt werden.
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.	• 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. • Medien, auf denen als „Geheim” eingestufte elektronische Ressourcen gespeichert wurden, müssen vor oder

			während der Entsorgung entsprechend bereinigt werden.