Kontrollpflichten externer Lieferanten

Informations- und Cyber-Sicherheit

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

Version 9.0, April 2019

Kontrollbereich / 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-/Cyber-Sicherheitskontrollen sichergestellt wird, sowie ein Sicherheitsprogramm zum Schutz des Lieferanten vor Informations-/Cyber-Bedrohungen gemäß den bewährten Praktiken der Branche (unter anderem NIST, SANS, ISO27001) und den anwendbaren branchenspezifischen Anforderungen. Der Lieferant nimmt regelmäßig (mindestens alle 12 Monate) Risikobewertungen bezüglich der Informations-/Cyber-Sicherheit vor und implementiert entsprechende Kontrollen bzw. trifft alle erforderlichen Maßnahmen zur Minderung der erkannten Risiken. Wird ein wesentliches Risiko erkannt, das den Ruf oder den an Barclays bereitgestellten Dienst beeinträchtigen könnte, muss der Lieferant Barclays darüber in Kenntnis setzen. Der Lieferant muss vom Führungsstab genehmigte Richtlinien sowie Standards für das Management des Informations-/Cyber-Risikos des Lieferanten einhalten, und er muss sie mindestens einmal jährlich überprüfen.	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. Genehmigte Verwendung	Der Lieferant erstellt und veröffentlicht allgemeine Nutzungsbedingungen, die seine Mitarbeiter über ihre Verantwortlichkeiten in Kenntnis setzen. Folgende Themen sind zu berücksichtigen: (a) Nutzung des Internets; (b) Nutzung von Social Media; (c) Nutzung der Firmen-E-Mail; (d) Nutzung von Instant Messaging; (e) Nutzung von IT-Geräten, die vom Lieferanten bereitgestellt werden; (f) Nutzung von IT-Geräten, die nicht vom Lieferanten bereitgestellt werden (z. B. eigene Geräte der Mitarbeiter (Bring Your Own Device)); (g) Nutzung tragbarer/wechselbarer Speichergeräte; (h) Verantwortlichkeiten beim Umgang mit Informationsressourcen von Barclays; und (i) Output von Kanälen für Datenleckagen Der Lieferant unternimmt angemessene Schritte, um die Einhaltung der allgemeinen Nutzungsbedingungen sicherzustellen.	Allgemeine Nutzungsbedingungen helfen bei der Verstärkung der Kontrollumgebung zum Schutz von Informationsressourcen.
3. Funktionen und Verantwortlichkeiten	Der Lieferant muss Funktionen und Verantwortlichkeiten für die Informations-/Cyber-Sicherheit definieren und kommunizieren. Diese müssen regelmäßig (mindestens alle 12 Monate) und nach jeder wesentlichen Änderung am Betriebsmodell oder Geschäft des Lieferanten überprüft werden. Zu den Hauptfunktionen muss ein leitender Angestellter gehören, der für die Informations-/Cyber-Sicherheit zuständig ist.	Durch die klare Definition von Funktionen und Verantwortlichkeiten wird die Umsetzung des Vertragsanhangs „Kontrollpflichten externer Lieferanten“ unterstützt.

4. Einhaltung der rechtlichen und gesetzlichen Bestimmungen vor Ort	Der Lieferant muss sicherstellen, dass die geltenden auf Informationssicherheit bezogenen rechtlichen und gesetzlichen Bestimmungen der Rechtsordnung, in welcher der Lieferant arbeitet, eingehalten werden und dass die Einhaltung angemessen dokumentiert wird. Anm.: Für Lieferanten, die Barclays Switzerland und Barclays Monaco unterstützen, können die Teams vor Ort zusätzliche Anforderungen in Verbindung mit den Bankenrechtsvorschriften und der Bankenregulierung vor Ort vorgeben.	Die Nichteinhaltung der rechtlichen und gesetzlichen Bestimmungen vor Ort könnte sowohl für den Lieferanten als auch für Barclays ernsthafte Konsequenzen haben, unter anderem Geldbußen, und im Extremfall den Verlust der Banklizenz von Barclays.
5. Weiterbildung und Awareness	Der Lieferant muss allen relevanten Mitarbeitern Weiterbildung und Awareness-Angebote (Education & Awareness) zur Verfügung stellen. Die Education & Awareness sollte den Funktionen und Verantwortlichkeiten der Mitarbeiter entsprechend angemessen sein, und sie muss ausreichend sein, damit die Mitarbeiter in der Lage sind, wahrscheinliche Angriffe zu verstehen und zu identifizieren sowie Bedenken zu melden. In den Schulungen müssen zumindest die Aufrechterhaltung der Online-Sicherheit (bei der Arbeit, zu Hause und unterwegs), Risiken im Zusammenhang mit der Vorspiegelung falscher Tatsachen in sozialen Netzwerken u. Ä. (Social Engineering) und praktische Gegenmaßnahmen behandelt werden. Der Lieferant muss dafür sorgen, dass sämtliche Mitarbeiter (Neuzugänge / in eine neue Position gewechselte Mitarbeiter) die Schulungen innerhalb eines angemessenen Zeitraums absolvieren, um sicherzustellen, dass sie die nötigen Kenntnisse über ihre Funktionen und Verantwortlichkeiten in Bezug auf die Informationssicherheit haben. Systemadministratoren müssen mindestens einmal jährlich Schulungen zur Verbesserung der Awareness zur Informations-/Cyber-Sicherheit erhalten, in denen vermittelt wird, welche Szenarien/Bedrohungen für ihre Funktion spezifisch sind, wie Informations-/Cyber-Bedrohungen identifiziert werden, wie man sich vor Informations-/Cyber-Bedrohungen schützt und wie Bedenken gemeldet werden.	Durch Weiterbildung und Awareness werden alle anderen Kontrollen im Rahmen dieses Vertragsanhangs unterstützt. Wird diese Kontrolle nicht umgesetzt, sind relevante Mitarbeiter sich der Cyber-Risiken und Angriffsvektoren nicht bewusst und wären nicht in der Lage, Angriffe zu erkennen beziehungsweise zu verhindern.

6. 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. • Es muss ein Vorfallbehandlungsprozess für die zeitnahe Abwicklung und regelmäßige Meldung unbefugter Zugriffe auf Informationen von Barclays und/oder auf von Barclays genutzte Dienste eingerichtet sein. • Verstöße, bei denen nicht bekannt ist, dass sie Auswirkungen auf Systeme von Barclays gehabt haben, und die Abhilfemaßnahmen / Aktualisierungen bei diesen sollten Barclays dennoch zu Informationszwecken gemeldet werden. • Der Lieferant muss Sorge dafür tragen, dass Teams und Prozesse für die Vorfallbehandlung mindestens einmal jährlich getestet werden, um sicherzustellen, dass der Lieferant zur Behandlung von identifizierten Cyber-Sicherheitsvorfällen in der Lage ist. Bestandteil der Tests muss eine Validierung der Fähigkeit zur Benachrichtigung von Barclays sein; dies geschieht durch den Nachweis der Fähigkeit, die entsprechenden Personen zu kontaktieren. • Es muss ein Prozess festgelegt sein und betrieben werden, um nach einem Sicherheitsvorfall Schwachstellen zu identifizieren und deren Entschärfung zu managen, ohne dass Untersuchungen oder daraufhin unternommene Aktivitäten beeinträchtigt werden. • Beim Lieferanten muss es Prozesse und Verfahren für die Durchführung einer Analyse der Grundursachen geben, sowohl zu internen (beim Lieferanten) als auch externen Ereignissen. • Der Lieferant muss dafür sorgen, dass die festgelegten Abhilfemaßnahmen nach einem Vorfall gemäß einem Abhilfeplan (Aktion, Zuständigkeit, Frist) ausgeführt und mit Barclays abgesprochen und vereinbart werden.	Mit Hilfe eines Vorfallmanagement- und Vorfallbehandlungsprozesses wird sichergestellt, dass Vorfälle schnell eingedämmt werden und verhindert wird, dass sie sich ausweiten.

7. Kontinuierliche Verbesserung	Der Lieferant muss kontinuierlich aus Ereignissen lernen und die von ihm gezogenen Lehren anwenden, um die Abwehrmaßnahmen gegen Cyber-Risiken zu verbessern.	Wird diese Kontrolle nicht umgesetzt, sind Lieferanten nicht in der Lage, die Lehren aus früheren Ereignissen zu nutzen, um ihre Kontrollumgebung zu verbessern und zu verstärken.
8. Zuständigkeit für Informationsressourcen	Beim Lieferanten muss es eine benannte Kontaktperson geben, die Ansprechpartner für den Verantwortlichen für Informationsressourcen von Barclays ist.	Die Zuständigkeit für Informationsressourcen ist für den hinreichenden Schutz von Informationsressourcen von grundlegender Bedeutung.
9. 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 B2A2) 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.
10. Ressourcenmanagement	Der Lieferant muss eine genaue Bestandsliste aller betreffenden für das Erbringen von Diensten für Barclays verwendeten IT-Ressourcen führen und sie mindestens einmal jährlich überprüfen, um zu validieren, dass die Bestandsliste der IT-Ressourcen aktuell, vollständig und genau ist.	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 Rügen von Aufsichtsbehörden nach sich ziehen kann.

11. Sicherheit beim Transport	Informationsressourcen von Barclays (sofern sie nicht als „Uneingeschränkt“ oder einer gleichwertigen Kategorie zugehörig betrachtet werden) müssen beim Transport dem damit verbundenen Risiko entsprechend geschützt werden.	Durch Kontrollen zur Sicherheit beim Transport werden die Informationen von Barclays davor geschützt, abgefangen und offengelegt zu werden.
12. Vernichtung/Löschung/ Außerbetriebnahme von physischen und logischen Informationen	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.	Die sichere Vernichtung von Informationsressourcen hilft dabei, sicherzustellen, dass Informationsressourcen von Barclays nicht im Zusammenhang mit Datenschutzverletzungen, Datenverlust oder böswilligen Aktivitäten wiederherstellbar sind.

13. 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. Folgende Schutzmechanismen sollten vom Lieferanten in Betracht gezogen werden: • durch logische Trennung der Gerätemanagement-Ports/Schnittstellen vom Datenverkehr der Benutzer; • angemessene Authentifizierungskontrollen; und • das Ermöglichen sämtlicher verfügbaren Kontrollen zur Entschärfung von Exploits im Betriebssystem und in installierten Anwendungen und Agenten. Vom Lieferanten müssen Fähigkeiten festgelegt und betrieben werden, damit unzulässige Geräte, als bösartig identifizierte Software und unzulässige Hochrisikosoftware im Netzwerk des Lieferanten erkannt werden. Vom Lieferanten müssen Netzwerksensoren platziert werden, um Bedrohungen an sämtlichen Eintritts- und Austrittspunkten des Netzwerkperimeters zu erkennen. *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.*	Wird diese Kontrolle nicht umgesetzt, werden externe und interne Netzwerke möglicherweise durch Bedrohungsakteure beeinträchtigt.
14. Schutz des Perimeters	Der Lieferant muss eine Bestandsliste der externen Netzwerkverbindungen, über das Internet erreichbaren Hosts und Datenübertragungen führen, die zur Übermittlung von Barclays-Daten zurück an Barclays oder Dritte (darunter auch Subunternehmen des Lieferanten) verwendet werden. Im Perimeter muss ausgehend von der Risikoexposition und den geschäftlichen Erfordernissen ein in mehrere getrennte Bereiche unterteiltes Netzwerkdesign implementiert werden. Im Perimeter dürfen nur Geräte platziert werden, die den Zugang zu/von externen Netzwerken benötigen oder ermöglichen.	Ein angemessener Schutz für den Perimeter hilft dabei, sicherzustellen, dass das Netzwerk und die Informationsressourcen von Barclays angemessen geschützt sind.

15. Netzwerkzugriff und Fernzugriff	Der Lieferant muss durch angemessene Netzwerkzugriffskontrollen sicherstellen, dass der Zugriff auf das interne Netzwerk überwacht werden muss und nur Geräte mit entsprechender Berechtigung erlaubt sind. 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. Für die Verbindung vom Standort des Lieferanten / den Support außerhalb der Büro-/Geschäftszeiten ist der Fernzugriff auf Umgebungen von Barclays standardmäßig nicht vorgesehen. Jeder Fernzugriff muss durch die relevanten Teams von Barclays (einschließlich des Chief Security Office) genehmigt werden.	Netzwerkzugriffskontrollen helfen dabei, zu verhindern, dass unsichere Geräte mit dem Netzwerk des Lieferanten verbunden und auf diese Weise neue Schwachstellen eingebracht werden.
16. DoS-Erkennung	Der Lieferant muss Fähigkeiten zur Erkennung von DoS-Angriffen (Denial of Service) implementieren und aufrechterhalten. Der Lieferant muss dafür sorgen, dass mit dem Internet verbundene oder externe Kanäle zur Unterstützung der für Barclays erbrachten Dienste mit einem hinreichenden DoS-Schutz versehen sind, um die mit Barclays vereinbarten Verfügbarkeitskriterien sicherzustellen.	Wird diese Kontrolle nicht umgesetzt, sind Barclays und Lieferanten von Barclays möglicherweise nicht in der Lage, zu verhindern, dass ein DoS-Angriff sein Ziel erreicht.

17. Überwachung/Protokollierung	Der Lieferant muss sicherstellen, dass Fähigkeiten vorhanden sind, um die IT-Infrastruktur rund um die Uhr auf potenzielle Cybersicherheitsereignisse zu überwachen. Der Lieferant muss Ereignisdaten von den betreffenden Systemquellen und -sensoren erfassen und korrelieren, und er muss sie analysieren, um Angriffe/Vorfälle zu identifizieren und zu verstehen. Bei Identifizierung von wesentlichen Vorfällen und/oder Verletzungen von Sicherheitskontrollen muss der Lieferant sicherstellen, dass der entsprechende Vorfallmanagementprozess (siehe Abschnitt 6) eingeleitet wird. Alle wichtigen Systeme, auch wichtige Anwendungen, müssen vom Lieferanten so eingestellt werden, dass wichtige Ereignisse protokolliert werden, und die Systemzeit für alle Systeme muss vom Lieferanten mit NTP (Network Time Protocol) synchronisiert werden. Protokolle müssen zentralisiert, angemessen gesichert und vom Lieferanten mindestens 12 Monate lang aufbewahrt werden. Zu den wichtigen protokollierten Ereignissen müssen jene gehören, die potenziell die Vertraulichkeit, Integrität und Verfügbarkeit der für Barclays bereitgestellten Dienste beeinflussen könnten und die zur Identifizierung oder Untersuchung wesentlicher Vorfälle und/oder Zugriffsrechtsverletzungen bezüglich der Lieferantensysteme beitragen können.	Wird diese Kontrolle nicht umgesetzt, sind Lieferanten nicht in der Lage, Verletzungen der Cyber-Sicherheit zu erkennen und darauf zu reagieren oder sich von Cyber-Ereignissen, die in ihrem Netzwerk eingetreten sind, zu erholen und daraus zu lernen, indem sie die relevanten Protokolle analysieren.
18. Trennung von Informationsressourcen	Der Lieferant muss Informationsressourcen von Barclays in einem von anderen Clients (logisch und/oder physisch) getrennten Netzwerk speichern.	Ein getrenntes Netzwerk hilft dabei, für einen hinreichenden Schutz der Informationsressourcen von Barclays vor unbefugter Offenlegung zu sorgen.

19. Schutz vor Schadcode/Malware	Sofern dies auf Betriebssystem-Ebene unterstützt wird, muss bei IT-Systemen, IT-Diensten und IT-Geräten jederzeit eine Anti-Malware-Lösung vorhanden sein, damit Störungen des Dienstes bzw. Verletzungen der Sicherheit verhindert werden. Pflichten des Lieferanten: • Aktuellen Schutz vor Schadcode/Malware gemäß den bewährten Praktiken der Branche (z. B. NIST, ISO27001) einrichten und pflegen; und • Schutzmaßnahmen gegen die Übertragung von Schadcode an Systeme von Barclays, Kunden von Barclays und sonstige Dritte nach den branchenüblichen Verfahren (z. B. NIST, ISO27001) ergreifen.	Anti-Malware-Lösungen sind für den Schutz der Informationsressourcen von Barclays vor Schadcode von entscheidender Bedeutung.
20. Sichere Build-Standards und Abstimmung von Sicherheitsänderungen	Der Lieferant muss Build-Standards für sämtliche konfigurierbare Out-of-the-Box-Software, die massenweise eingesetzt wird (z. B. Betriebssysteme, Datenbanken), und Firmware von häufig gebrauchter Infrastruktur (z. B. SAN oder Netzwerkgeräte) definieren und implementieren. Bei Nichteinhaltung des Build-Standards müssen Abhilfemaßnahmen erfolgen. Bei Sicherheitsänderungen (z. B. Änderungen der Sicherheitskonfiguration, Änderung der Rechte für Konten) muss immer ein Protokoll generiert werden, das in einer manipulationssicheren Umgebung gespeichert wird. Es muss eine Abstimmung zwischen den übernommenen und den genehmigten Änderungen vorgenommen werden. 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.	Standardmäßige Build-Kontrollen helfen, Informationsressourcen vor unbefugtem Zugriff zu schützen. Die Einhaltung von Standard-Builds und Kontrollen, die sicherstellen, dass Änderungen genehmigt sind, hilft dabei, für den Schutz der Informationsressourcen von Barclays zu sorgen.
21. Technologien des Sicherheitsschutzes	Es müssen geeignete Technologien angewendet werden, um aktuellen und aufkommenden Cyber-Bedrohungen mit einer konsequenten Basis an Kontrollen zu begegnen, die aufrechterhalten werden, um die Zuführung, Ausführung und Ausnutzung von Angriffen sowie die Exfiltration zu verhindern.	Wird diese Kontrolle nicht umgesetzt, sind Informationsressourcen von Barclays möglicherweise nicht hinreichend vor Cyber-Angriffen geschützt.

22. 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.
23. Erkennung von unzulässigen Geräten und unzulässiger Software	Der Lieferant muss sicherstellen, dass er über die Fähigkeit und die Prozesse verfügt, um unzulässige Geräte, als bösartig identifizierte Software und unzulässige Hochrisikosoftware zu erkennen.	Wird diese Kontrolle nicht umgesetzt, sind Lieferanten möglicherweise nicht in der Lage, unzulässige bösartige Geräte oder Schadsoftware zu erkennen, zu entfernen oder zu deaktivieren, und sie setzen Ressourcen von Barclays dadurch Cyber-Angriffen aus.

24. 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); • Unzulässige Übertragung von Informationen auf tragbare Medien; • Unsicherer Austausch von Informationen mit Dritten (Subunternehmen); • Unangebrachtes Ausdrucken oder Kopieren von Informationen; • Fehler und Unterlassungen bei der Kategorisierung und Kennzeichnung von Ressourcen; und • Unzulässiges Durchsickern von Informationen über DNS (Domain Name System)	Angemessene Kontrollen zur Verhinderung von Datenleckagen sind ein wichtiges Element der Informationssicherheit, denn sie helfen dabei, sicherzustellen, dass Informationen von Barclays nicht verloren gehen.
25. Sichere Speicherung und Verarbeitung	Es müssen Kontrollen zum Schutz von Informationsressourcen (im Zusammenhang mit dem (den) vom Lieferanten für Barclays erbrachten Dienst(en)) vorhanden sein, unabhängig davon, wo sie gespeichert oder verarbeitet werden (dies gilt für Informationen, die im Rahmen von strukturierten und unstrukturierten Methoden gespeichert werden).	Informationsressourcen werden in der Regel zusammen gespeichert; sie stellen deshalb eine Risikokonzentration dar und müssen gesichert werden.
26. Backups und Wiederherstellung	Es müssen Vorkehrungen getroffen werden, um Sorge dafür zu tragen, dass Informationen unter Einhaltung der mit dem Verantwortlichen für die Informationsressource von Barclays vereinbarten Anforderungen angemessen durch Backups gesichert werden und wiederherstellbar sind und dass die Sicherheit der betreffenden Informationsressource während des Prozesses durchweg aufrechterhalten wird. Häufigkeit und Methode von Backups müssen mit dem Verantwortlichen für die Informationsressource vereinbart werden. Für Informationsressourcen, bei denen ein Backup durchgeführt wurde, muss es definierte Kontrollen geben, um sicherzustellen, dass der Zugriff nur gewährt wird, wenn er erforderlich ist.	Backups speichern Kopien von Informationsressourcen und müssen deshalb den gleichen Kontrollen unterliegen.

27. 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. 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:	Angemessene LAM-Kontrollen helfen dabei, sicherzustellen, dass Informationsressourcen vor unangemessener Verwendung geschützt werden.

	• Vorhandensein eines robusten Autorisierungsprozesses, bevor Konten erstellt/geändert/gelöscht werden; • regelmäßig durchgeführter Prozess zur Überprüfung des Zugriffs eines Benutzerkontos sowie mindestens einmal jährlich Validierung des Zugriffs des Benutzers • 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 innerhalb von 24 Stunden nach dem Zeitpunkt des Ausscheidens entfernt, alle anderen sekundären Zugriffsmöglichkeiten innerhalb von sieben Tagen entfernt; und • ruhende Konten, die 60 Tage in Folge oder länger nicht verwendet wurden, müssen gesperrt werden.	
28. Zugriffsmethoden	Die mit einem Konto durchgeführten Aktivitäten müssen eindeutig zu einer bestimmten Person zurückverfolgbar sein. Es müssen technische und den Prozess betreffende Maßnahmen angewendet werden, um den Zugriff auf die Informationsressource im entsprechenden Umfang durchzusetzen. Die Sicherheitskontrollen für Konten (z. B. starke Authentifizierung oder Break-Glass-Prozesse) müssen dem Risiko, dass Konten Schaden erleiden oder missbraucht werden, entsprechend angemessen sein. Die Zugriffsmethode muss gemäß den bewährten Praktiken der Branche definiert sein und mindestens Folgendes beinhalten: • 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. Der Fernzugriff für Dienste von Barclays muss über Mechanismen, denen die relevanten Barclays-Teams zugestimmt haben, erlaubt werden, und dabei muss eine Mehrfaktor-Authentifizierung erfolgen.	Zugriffsverwaltungskontrollen sorgen mit dafür, dass nur zugelassene Benutzerkonten auf die Informationsressourcen zugreifen können.

29. Schutz von Anwendungen	Anwendungen müssen mit sicheren Codierungsverfahren und in sicheren Umgebungen entwickelt werden. Wenn der Lieferant Anwendungen entwickelt, die der Nutzung durch Barclays dienen oder zur Unterstützung des für Barclays erbrachten Dienstes genutzt werden, müssen Prozesse und Kontrollen vorhanden sein, damit während des Entwicklungsprozesses Schwachstellen im Code identifiziert und behoben werden. Binärcodes von Anwendungen müssen vor unbefugten Änderungen geschützt werden, sowohl beim Einsatz als auch wenn sie sich in Source-Bibliotheken befinden. 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.	Kontrollen zum Schutz der Anwendungsentwicklung helfen, dafür zu sorgen, dass Anwendungen beim Einsatz geschützt sind.

30. Schwachstellenmanagement	Der Lieferant muss einen einheitlichen Mechanismus für die Erfassung, Einteilung und Behandlung identifizierter Schwachstellen zum Einsatz bringen. Der Lieferant muss Fähigkeiten aufbauen, um Sicherheits-Schwachstellen in IT-Systemen und Software ausgehend vom Risiko auf sämtlichen von der Organisation verwendeten Plattformen zu identifizieren und zu kategorisieren. Der Lieferant muss sicherstellen, dass das Schwachstellenmanagement Teil der normalen Betriebsabläufe ist, darunter Prozesse, um Schwachstellen zu erkennen und Risikobewertungen dazu vorzunehmen, um Schwachstellen in allen Systemen zu beseitigen oder zu beheben sowie um das Einbringen neuer Schwachstellen bei Änderungsprozessen und bei der Bereitstellung neuer Systeme zu verhindern. Alle Sicherheitsprobleme und Schwachstellen, die wesentliche Auswirkungen auf Systeme von Barclays oder auf die vom Lieferanten für Barclays erbrachten Dienste haben könnten, bei denen sich der Lieferant zur Inkaufnahme des Risikos entschieden hat, müssen Barclays sofort mitgeteilt und mit Barclays schriftlich abgestimmt werden. IT-Sicherheitspatches und Updates zum Schließen von Sicherheitslücken müssen vom Lieferanten über einen internen genehmigten Prozess (des Lieferanten) zeitnah installiert werden, um Verletzungen der Sicherheit zu verhindern. Lieferantensysteme, die aus irgendwelchen Gründen nicht aktualisiert werden können, müssen über Maßnahmen zum Schutz des ansonsten angreifbaren Systems verfügen.	Wird diese Kontrolle nicht umgesetzt, könnten Angreifer Schwachstellen innerhalb von Systemen ausnutzen, um Cyber-Angriffe auf Barclays und Lieferanten von Barclays durchzuführen.

31. Bedrohungssimulation / Penetrationstests / IT-Sicherheitsbewertung	Der Lieferant muss unter Einbeziehung eines unabhängigen qualifizierten Sicherheitsdienstleisters eine IT-Sicherheitsbewertung / Bedrohungssimulation durchführen, die sich auf die IT-Infrastruktur und Anwendungen im Zusammenhang mit dem (den) vom Lieferanten an Barclays erbrachten Dienst(en) bezieht. Dies muss mindestens einmal jährlich erfolgen, um Schwachstellen zu identifizieren, die ausgenutzt werden könnten, um die Vertraulichkeit der Daten von Barclays durch Cyberattacken zu verletzen. Alle Schwachstellen müssen vorrangig behandelt und bis zu ihrer Auflösung überwacht werden. Jedes Problem, bei dem das Risiko in Kauf genommen wird, muss mit Barclays abgesprochen und abgestimmt werden. Der Lieferant muss Barclays über den Umfang der Sicherheitsbewertung informieren und den Umfang mit Barclays abstimmen, insbesondere Datum/Uhrzeit für deren Start und Ende, damit Störungen bei wichtigen Aktivitäten von Barclays vermieden werden.	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 und Stärke ihrer Abwehrmaßnahmen einzuschätzen.

32. Änderungs- und Patchmanagement	Die Daten von Barclays und die zu ihrer Speicherung oder Verarbeitung verwendeten Systeme müssen vor unsachgemäßen Änderungen geschützt werden, welche die Verfügbarkeit oder Integrität beeinträchtigen könnten. Der Lieferant entwickelt und implementiert eine Patchmanagementstrategie, die von den Managementkontrollen sowie von den Patchmanagementverfahren und operativen Dokumenten unterstützt wird. IT-Sicherheitspatches und Updates zum Schließen von Sicherheitslücken müssen, sobald sie verfügbar sind, über einen genehmigten Prozess zeitnah installiert werden, um Verletzungen der Sicherheit zu verhindern. Bei Lieferantensystemen, die aus irgendwelchen Gründen nicht aktualisiert werden können, müssen Sicherheitsmechanismen zum Schutz des ansonsten angreifbaren Systems installiert sein. Alle Änderungen müssen in Übereinstimmung mit dem genehmigten Änderungsmanagementprozess des Lieferanten vorgenommen werden. Open-Source-Anwendungen werden auf mögliche Schwachstellen geprüft. Der Lieferant stellt sicher, dass verfügbare, genehmigte Notbehelfsmaßnahmen implementiert werden, sofern dadurch keine höheren geschäftlichen Risiken entstehen. Bei Lieferantensystemen, die aus irgendwelchen Gründen nicht aktualisiert werden können, müssen Sicherheitsmechanismen installiert sein, die einen umfassenden Schutz des ansonsten angreifbaren Systems bieten. Alle Änderungen müssen in Übereinstimmung mit dem Änderungsmanagementprozess des Lieferanten vorgenommen werden.	Wird diese Kontrolle nicht umgesetzt, sind Dienste möglicherweise anfällig für Sicherheitsprobleme, die zur Gefährdung von Verbraucherdaten oder zum Ausfall des Dienstes führen oder andere bösartige Aktivitäten ermöglichen könnten.
33. Kryptografie	Der Lieferant muss die von ihm angewendeten kryptografischen Technologien und Algorithmen überprüfen und bewerten, um sicherzustellen, dass sie noch für ihren Zweck geeignet sind. Die Stärke der eingesetzten Verschlüsselung muss im richtigen Verhältnis zur Risikoneigung stehen, da sie sich auf den Betrieb oder die Leistung auswirken kann. Kryptografische Implementierungen müssen den definierten Anforderungen und Algorithmen entsprechen.	Ein aktueller und angemessener Schutz durch Verschlüsselung sowie aktuelle und angemessene Verschlüsselungsalgorithmen stellen den kontinuierlichen Schutz der Informationsressourcen von Barclays sicher.

34. Cloud-Computing	Jede Nutzung von (öffentlichen / privaten / gemeinschaftlichen / hybriden) Cloud-Computing-Diensten wie beispielsweise SaaS / PaaS / IaaS, die im Rahmen der Erbringung vereinbarter Dienste für Barclays verwendet werden, muss durch die relevanten Teams von Barclays (einschließlich des Chief Security Office) überprüft und genehmigt werden; und 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.
35. 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.
36. Banktechnischer Raum	Für Dienste, die formell einen banktechnischen Raum (BDS, Bank Dedicated Space) benötigen, müssen bestimmte physische und technische Anforderungen erfüllt werden. (Wenn für den Dienst ein BDS vorgeschrieben ist, gelten die Kontrollbestimmungen in Anhang C.)	Wird diese Kontrolle nicht umgesetzt, sind angemessene physische und technische Kontrollen möglicherweise nicht vorhanden, was zu Verzögerungen oder Unterbrechungen des Dienstes oder zu Verletzungen der Cyber-Sicherheit führen kann.

Anhang A: Glossar

Definitionen	
Backup	Ein Backup oder Backup-Prozess ist die Erstellung von Datenkopien, damit diese zusätzlichen Kopien zur Wiederherstellung des Originals nach einem Datenverlust-Ereignis verwendet werden können.
Banktechnischer Raum	Banktechnischer Raum (Bank Dedicated Space, BDS) sind im Besitz oder unter der Kontrolle einer Konzerngesellschaft des Lieferanten oder von Subunternehmen befindliche Räumlichkeiten, die nur für Barclays zur Verfügung gestellt werden und von denen aus die Dienste erbracht oder bereitgestellt werden.
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. Oder Jegliche Einzelinformation oder Gruppe von Informationen, die einen Wert für die Organisation hat.
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.
Kryptografie	Die Anwendung mathematischer Grundlagen zur Entwicklung von Techniken und Algorithmen, die sich auf Daten anwenden lassen, damit Ziele wie Vertraulichkeit, Datenintegrität und/oder Authentifizierung erreicht werden.
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.
Verantwortlicher für Informationsressourcen	Die Einzelperson bei der Organisation, die für die Kategorisierung einer Ressource verantwortlich ist sowie dafür, dass der korrekte Umgang mit der Ressource sichergestellt wird.
Vernichtung/ Löschung	Das Überschreiben, Auslöschen oder physische Zerstören von Informationen auf eine solche Art und Weise, dass sie nicht wiederherstellbar sind.
Verschlüsselung	Die Umwandlung einer Nachricht (Daten-, Sprach- oder Videonachricht) in eine nichtssagende, für unbefugte Mitleser unverständliche Form. Diese Umwandlung erfolgt aus dem Klartextformat in Chiffretext.

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	• 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.

	ausdrückliche Genehmigung des Verantwortlichen für die Informationen können zur Zielgruppe auch externe Empfänger gehören.	• 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 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. • Ressourcen dürfen nur über die vom Unternehmen genehmigten Systeme, Methoden und Lieferanten verteilt werden.	• 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.	• 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 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 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.	• 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.

Anhang C: Banktechnischer Raum (BDS) – Kontrollbestimmungen [Anm.: Bei Bedarf bitte mit dem Sourcing-Mitarbeiter absprechen]

Kontrollbereich	Bezeichnung der Kontrolle	Beschreibung der Kontrolle
Banktechnischer Raum	Physische Trennung	Der physisch belegte Bereich muss Barclays zur Verfügung gestellt werden und darf nicht mit anderen Firmen bzw. Lieferanten geteilt werden.
Banktechnischer Raum	Physische Zugriffssteuerung	Für den Zugriff auf den BDS müssen u. A. die folgenden sicheren und automatischen Kontrollen eingesetzt werden: 1) Für autorisierte Mitarbeiter: i) Fotoausweis (jederzeit sichtbar zu tragen) ii) Berührungslose Kartenleser sind installiert iii) Aktiviertes Anti Passback (Verhinderung von zweimaligem Zutritt ohne vorhergehenden Austritt) 2) Besucher-/Lieferantenkontrollen i) Logbuch für jede Anmeldung ii) Eingeschränkter Ausweis (jederzeit sichtbar zu tragen)
Banktechnischer Raum	Physische Zugriffssteuerung	Warnsysteme müssen so konfiguriert sein, dass Warnmeldungen durch ein zentralisiertes Zugriffssystem mit nachprüfbarer Zugriffssteuerung ausgegeben werden.
Banktechnischer Raum	Physische Zugriffssteuerung und Hausdienste	Kontrollmechanismen sind zu überwachen, um dem BDS und sonstigen kritischen Bereichen den entsprechenden Zugriff zu gewähren. Der Zutritt zum BDS ist ausschließlich befugten Haustechnikern und unterstützendem Personal wie Elektrikern, HLK-Wartungstechnikern, Hausmeistern usw. erlaubt.

Banktechnischer Raum	Fernzugriff – ID&V	Alle Einzelbenutzer können sich vom BDS aus nur mit einem von Barclays gestellten Multifaktor-Authentifizierungstoken beim Barclays-Netzwerk anmelden.
Banktechnischer Raum	Fernzugriff – Software-Token	Jede Installation von RSA-Software und Soft-Token muss von autorisiertem Personal innerhalb des genehmigten BDS auf Desktop-Rechnern vorgenommen werden.
Banktechnischer Raum	Fernzugriff - Unterstützung außerhalb des Büros	Für den Support außerhalb der Büro-/Geschäftszeiten ist der Fernzugriff auf die BDS-Umgebung standardmäßig nicht vorgesehen. Jeder Fernzugriff muss durch die relevanten Teams von Barclays (einschließlich des Chief Security Office) genehmigt werden.
Banktechnischer Raum	E-Mail und Internet	Netzwerkverbindungen müssen sicher konfiguriert sein, damit E-Mail- und Internet-Aktivitäten im BDS-Netzwerk eingeschränkt sind.
Banktechnischer Raum	Softwareentwicklung, Tests und Entwicklungsumgebung	Der Lieferant muss sicherstellen, dass die Softwareentwicklung nur für die im Eigentum von Barclays befindlichen Programme innerhalb des banktechnischen Raums (BDS) stattfinden darf.
Banktechnischer Raum	Netzwerkkontrollen – Übertragung	Jede Übertragung von Informationen zwischen der BDS-Umgebung und Barclays muss auf sichere Weise geschehen, und für das Management der Netzwerkgeräte müssen sichere Protokolle verwendet werden.
Banktechnischer Raum	Netzwerkkontrollen – Routing	Routing-Konfigurationen müssen sicherstellen, dass Verbindungen nur zum Netzwerk von Barclays und nicht zu irgendwelchen anderen Netzwerken geleitet werden.
Banktechnischer Raum	Netzwerkkontrollen – Drahtlosnetzwerke	Drahtlosnetzwerke dürfen nicht im Barclays-Netzwerksegment verwendet werden, um Dienste bereitzustellen.

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 B2 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. Kennzeichnungs schema 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 D1 von Anhang D) anwenden, oder ein mit dem Land mit Bankgeheimnis vereinbartes alternatives Schema. Die Anforderungen an die Handhabung bei CID-Daten sind in Tabelle D2 von Anhang D 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 D: 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

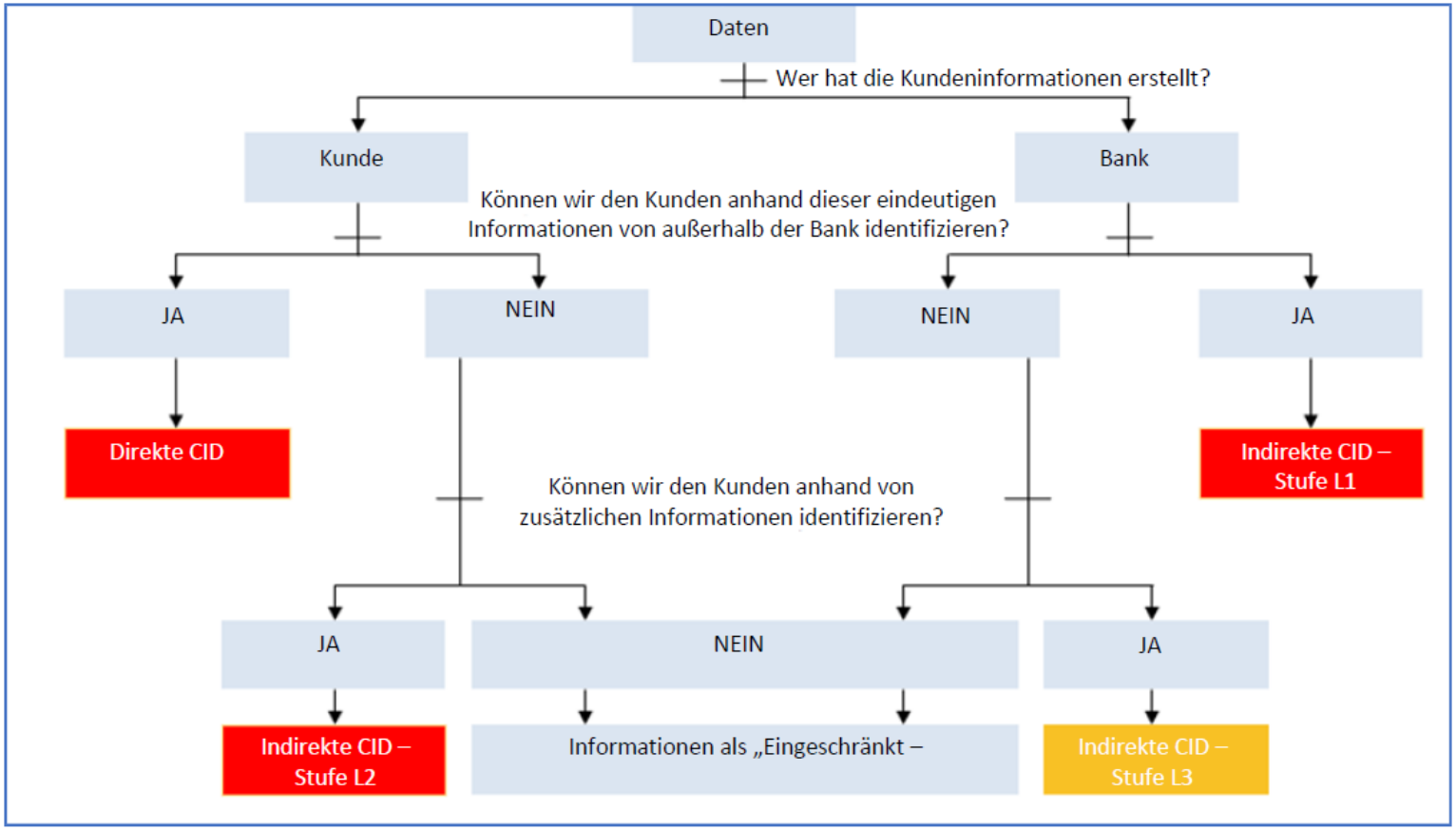
   (DCID) = Verletzung des Bankgeheimnisses

2. Container-Kennung

(ICID der Stufe L1) = Verletzung des Bankgeheimnisses

3. Vermögensverhältnisse + Staatsangehörigkeit

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


Daten
Wer hat die Kundeninformationen erstellt?
Kunde
Bank
Können wir den Kunden anhand dieser eindeutigen Informationen von außerhalb der Bank identifizieren?
JA
NEIN
NEIN
JA
Direkte CID
Indirekte CID – Stufe L1
Können wir den Kunden anhand von zusätzlichen Informationen identifizieren?
JA
NEIN
JA
Indirekte CID – Stufe L2
Informationen als „Eingeschränkt –
Indirekte CID – Stufe L3

Anhang E: Barclays-Kennzeichnungsschema für Informationen

Tabelle E1: 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 D)

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	• Neue Produktpläne. • Klientenverträge. • Rechtsgültige Verträge.

	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.	• 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 E2: 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.	• 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.	• 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.