

Capgemini – Binding Corporate Rules

Für Aktivitäten als Verantwortlicher

Öffentliche Übersetzungsversion des englischen Originals

BU Germany Data Protection
Juni 26



Capgemini 



Content

Dokumentenhistorie.....	4
Einführung.....	5
Definitionen	6
1. Anwendungsbereich der BCR-C	9
1.1 Sachlicher Anwendungsbereich.....	9
1.2 Geografischer Anwendungsbereich	9
2. Verbindlichkeit des BCR-C.....	10
2.1. Verbindlichkeit für Capgemini-Unternehmen	10
2.2. Verbindlichkeit für Capgemini-Mitarbeiter.....	10
3. Umsetzung der Datenschutzgrundsätze	10
3.1 Eindeutig festgelegter Zweck.....	11
3.2 Rechtsgrundlage	11
3.3 Datenminimierung	12
3.4 Datenqualität	12
3.5 Einschränkung der Datenspeicherung	12
3.6 Datensicherheit	12
3.7 Verarbeitung besonderer Kategorien personenbezogener Daten & Daten über strafrechtliche Verurteilungen und Straftaten	13
3.8 Entscheidungsfindung auf Grundlage automatisierter Verarbeitung	14
4. Transparenz	14
5. Rechte der betroffenen Personen.....	15
6. Durchsetzbare Rechte betroffener Personen	16
7. Verfahren zur Bearbeitung von Anträgen betroffener Personen	17
8. Datenschutzorganisation von Capgemini	17
9. Privacy by Design – Datenschutz durch Technikgestaltung.....	18
9.1 Aufzeichnung der Verarbeitungstätigkeiten.....	18
9.2 Datenschutzfolgeabschätzung	19
10. Ausbildung und Bewusstsein.....	20
10.1 Globale Pflichtschulung	20
10.2 Funktionsspezifische Schulungen und Leitlinien.....	20
11. Audits	20
12. Einsatz interner oder externer Auftragsverarbeiter	21
12.1. Vereinbarungen zur Datenverarbeitung oder Datenschutzklauseln	21
12.2 Zusätzliche Verpflichtungen bei Übermittlungen in Drittländer	22
13. Bewertung der Auswirkungen von Datenübermittlungen (Transfer Impact Assessment - TIA) ...	23



14. Umgang mit Auskunftersuchen von Behörden.....	25
15. Haftung von Capgemini im Falle eines Verstoßes gegen die BCR-C.....	26
16. Nichteinhaltung der BCR-C	27
17. Zusammenarbeit mit den Aufsichtsbehörden	27
18. Leichter Zugang zu den BCR	27
19. Aktualisierungen der BCR	28
20. Beendigung.....	28
Anhang 1 – Liste der an die BCR-C gebundenen Einheiten nach Ländern	29
Anhang 2 - Capgemini-Verarbeitungstätigkeiten und wichtigste Übermittlungen.....	38
Anhang 3 – Capgemini-Datenschutzorganisation.....	51
Anhang 4 - Wie können Sie Ihre Datenschutzrechte wahrnehmen?	52



Dokumentenhistorie

Versionsgeschichte		
Version	Datum	Kommentare
1.0	2016	Die ursprüngliche Fassung wurde der CNIL mitgeteilt und von dieser mit offiziellem Schreiben genehmigt
2.0	2018	Vollständige Neufassung der verbindlichen Unternehmensregeln
3.0	2023	Aktualisiert nach der Entscheidung Schrems II
4.0	2024-2025	Aktualisierung und Neugestaltung der verbindlichen Unternehmensregeln, getrennt nach für die Verarbeitung Verantwortlichen und Auftragsverarbeitern, um die Anforderungen des Europäischen Datenschutzausschusses (EDSA) zu erfüllen und eine bessere Lesbarkeit zu gewährleisten
Autoren und Mitwirkende		
Rolle	Tätigkeit	Kommentare
Nathalie Laneret	Group DPO	
Louise Achache	Senior Data Protection Legal Counsel	
Verteilung von Dokumenten		
Rolle	Standort	Aktion/Information
CNIL	Paris, Frankreich	Zur offiziellen Überprüfung und Genehmigung.
Gruppe und lokale Generalräte, Geschäftsführender Direktor der Gruppe	Paris, Frankreich	Zur offiziellen Information der Geschäftsführung und zur Bestätigung
Alle Mitarbeiter	Alle Capgemini-Standorte	Bei der Einstellung und während der gesamten Dauer des Arbeitsverhältnisses gemäß den gesetzlichen Bestimmungen informieren
Dokument geprüft und genehmigt von		
Rolle	Verantwortung	Kommentare
Group DPO, Emmanuelle Bartoli	Interner Genehmiger	
CNIL, Französische Datenschutzbehörde	Offizieller Prüfer & Genehmiger	Mit offiziellem Schreiben im Jahr 2016 genehmigt Überprüfte und bestätigte neuere Versionen gemäß dem offiziellen Behördenverfahren



Bei diesem Dokument handelt es sich um eine Übersetzung des englischen Originals. Es dient lediglich dem Verständnis der BCR im deutschsprachigen Raum. Im Fall von Abweichungen zwischen dieser deutschen Version und der englischen Originalversion, gilt ausschließlich die englische Originalversion.

Einführung

Als weltweit führender Anbieter von Beratung, Technologiedienstleistungen und digitaler Transformation steht Capgemini an der Spitze der Innovation und nutzt Cloud, Daten, KI-Konnektivität, Software, digitales Engineering und Plattformen, um die gesamte Bandbreite der Anforderungen unserer Kunden zu erfüllen. Wir helfen unseren Kunden, den richtigen Weg in eine bessere Zukunft zu finden - von der Verbesserung des digitalen Kundenerlebnisses bis hin zur Beschleunigung der intelligenten Industrie und der Transformation der Unternehmenseffizienz.

Capgemini verpflichtet sich, alle personenbezogenen Daten zu schützen, die ihr im Rahmen ihrer Tätigkeit anvertraut werden. Als internationaler Konzern mit Niederlassungen in mehr als 40 Ländern ist es für Capgemini unerlässlich, dass Informationen frei und sicher fließen. Die Gewährleistung eines hohen Schutzniveaus für personenbezogene Daten, die innerhalb der Gruppe übermittelt werden, ist einer der Gründe, warum Capgemini sich für die Umsetzung dieser verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules - BCR) entschieden hat. Diese wurden erstmals im März 2016 von der französischen Datenschutzbehörde CNIL genehmigt und wurden 2019 und 2023 weiter geändert, um der Allgemeinen Datenschutzverordnung (GDPR) und den aktualisierten Anforderungen des Europäischen Datenschutzausschusses nach der sogenannten Schrems-II-Entscheidung zu entsprechen.

Die BCR von Capgemini sind mehr als nur ein Mechanismus zur Datenübermittlung. Sie sind unsere globale Datenschutzpolitik, ein umfassender Rahmen, der unseren gesamten Verantwortungsansatz für die Verarbeitung personenbezogener Daten definiert. In den BCR von Capgemini sind nicht nur die Grundsätze festgelegt, die bei der Verarbeitung personenbezogener Daten einzuhalten sind, sondern auch die Verfahren, die Capgemini eingeführt hat, um die geltenden Datenschutzgesetze und insbesondere die Datenschutz-Grundverordnung 2016/679 (DSGVO) einzuhalten.



Definitionen

Für dieses Dokument gelten die folgenden begrifflichen Bestimmungen:

"Angemessenheitsbeschluss" bezeichnet eine Entscheidung der Europäischen Kommission, mit der festgestellt wird, dass ein Land ein angemessenes Datenschutzniveau bietet. Dadurch ist die Übermittlung personenbezogener Daten in dieses Land im Einklang mit der DSGVO ohne weitere Genehmigung zulässig.

"Anwendbares Datenschutzrecht" bedeutet alle anwendbaren Datenschutzvorschriften, insbesondere (1) die europäische Verordnung Nr. 2016/679 über die Verarbeitung personenbezogener Daten (GDPR) und (2) alle anwendbaren lokalen Gesetze und Vorschriften über die Verarbeitung personenbezogener Daten.

"Binding Corporate Rules" (BCR) („Verbindliche interne Datenschutzvorschriften“) sind Richtlinien zum Schutz personenbezogener Daten, die von einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter mit Sitz im Hoheitsgebiet eines Mitgliedstaats bei der Übermittlung oder einer Reihe von Übermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter in einem oder mehreren Drittländern innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, befolgt werden.

"Binding Corporate Rules for Controller Activities" oder „BCR-C" sind die BCR, die für die Aktivitäten von Capgemini als Datenverantwortlicher gelten, insbesondere für den Fall, dass Capgemini-Unternehmen, die als Datenverantwortliche handeln, personenbezogene Daten an ein anderes Capgemini-Unternehmen übermitteln, die als Datenverantwortlicher oder als Auftragsverarbeiter handelt.

"Binding Corporate Rules for Processor Activities" oder "BCR-P" sind die BCR, die für Capgeminis Tätigkeiten als Datenverarbeiter gelten.

"Blue Book (Blaues Buch)" bezeichnet Capgeminis Richtlinienammlung, in dem eine Reihe von gemeinsam angenommenen Grundsätzen, Werten, Richtlinien und Prozessen aufgeführt sind.

"Capgemini" oder "Gruppe" bezeichnet alle Unternehmen, die sich im Besitz und/oder unter der direkten oder indirekten Kontrolle der Capgemini SE befinden.

"Capgemini-Geschäftskontakt" bezeichnet einen Lieferanten, Unterauftragnehmer, Aktionär, Kunden oder Partner von Capgemini.

"Capgemini-Kunde" bezeichnet jede natürliche oder juristische Person, für die Capgemini Dienstleistungen im Rahmen eines Vertrags erbringt.

"Capgemini-Unternehmen(en)" bezeichnet jedes Unternehmen, das zur Gruppe gehört und an die Capgemini BCR gebunden ist.

"Capgemini-Mitarbeiter" bezeichnet alle derzeitigen, ehemaligen oder künftigen Beschäftigten von Capgemini, einschließlich Leiharbeitnehmern und Praktikanten.

"Zuständige Aufsichtsbehörde" ist entweder die Aufsichtsbehörde des Landes, in dem die betroffene Person ihren gewöhnlichen Aufenthalt, ihren Arbeitsplatz oder den Ort des mutmaßlichen Verstoßes hat, oder die Aufsichtsbehörde des Landes, in dem der für die Verarbeitung Verantwortliche seinen Sitz hat.

"Cybersecurity Organisation" bezeichnet die globale Funktion von Capgemini, die globale Sicherheitsrichtlinien erstellt und verwaltet und die Einhaltung der Richtlinien durch die Geschäftseinheiten (Business Units/ BU) und Global Business Lines (GBL) überwacht. Die Cybersecurity Organisation besteht aus einem Netzwerk von Cybersecurity Beauftragten, die für jede Geschäftseinheit (BU) ernannt werden.

Der **"Verantwortliche" oder "für die Verarbeitung Verantwortliche"** ist die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

"Datenexporteur" oder "Exporteur" bezeichnet die Stelle, die die personenbezogenen Daten übermittelt.

"Datenimporteur" oder "Importeur" bezeichnet den Empfänger einer Datenübermittlung.

"Datenverarbeiter" oder "Auftragsverarbeiter" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.



"Datenschutz-Folgenabschätzung" oder **"DPIA"** bezeichnet ein Verfahren, mit dem insbesondere Ursprung, Art, Besonderheit und Schwere eines mit der Verarbeitung personenbezogener Daten verbundenen Risikos bewertet werden. Der Zweck einer Datenschutz-Folgenabschätzung besteht darin, das mit einer Verarbeitung oder einer Reihe von Verarbeitungen personenbezogener Daten verbundene Risiko zu bewerten und zu mindern.

"Datenschutzbeauftragter" oder **"DPO"** bezeichnet die benannten Capgemini-Mitarbeiter, die bei der zuständigen Datenschutzbehörde ordnungsgemäß ernannt wurden, wo dies erforderlich ist, und die über Fachkenntnisse des Datenschutzrechts und der Datenschutzpraktiken verfügen, die Beratung, Information und Überwachung der Einhaltung der geltenden Datenschutzgesetze übernehmen. Sie sind Teil der in Abschnitt 8 dieses Dokuments beschriebenen Datenschutzorganisation.

"Betroffene (Person)" ist jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten verarbeitet werden.

"Europäischer Wirtschaftsraum" oder **"EWR"** bezeichnet die Mitgliedstaaten der Europäischen Union und drei Länder der Europäischen Freihandelsassoziation.

"EWR-Capgemini-Unternehmen" bezeichnet jedes Capgemini Unternehmen mit Sitz im Europäischen Wirtschaftsraum ("EWR").

"Personenbezogene Mitarbeiterdaten" sind personenbezogene Daten, die sich auf einen derzeitigen, ehemaligen oder zukünftigen Mitarbeiter von Capgemini beziehen.

"Datenschutz-Grundverordnung" oder **"GDPR"** bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

"Gruppeninterne Vereinbarung" ist die rechtsverbindliche Vereinbarung, die dazu dient, die Binding Corporate Rules (BCR) für alle Capgemini-Unternehmen verbindlich zu machen.

"Nicht-EWR-Capgemini-Unternehmen" bezeichnet jedes Capgemini-Unternehmen mit Sitz außerhalb des EWR.

"Personenbezogene Daten" sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer (ID), zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

"Verletzung des Schutzes personenbezogener Daten" oder **"Datenschutzverletzung"** bedeutet eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Weitergabe oder zum Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.

"Verarbeitung" ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder einer Reihe personenbezogener Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

"Dienstleistungsvertrag" ist eine schriftliche Vereinbarung zwischen einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter, wonach der Auftragsverarbeiter für den für die Verarbeitung Verantwortlichen Dienstleistungen erbringt, die die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter nach den Anweisungen des für die Verarbeitung Verantwortlichen beinhalten.

"Standardvertragsklauseln" sind die von der Europäischen Kommission herausgegebenen Vertragsklauseln, die Datenübermittlungen von für die Verarbeitung Verantwortlichen mit Sitz im EWR an für die Verarbeitung Verantwortliche mit Sitz außerhalb des EWR und von für die Verarbeitung Verantwortlichen mit Sitz im EWR an Auftragsverarbeiter mit Sitz außerhalb des EWR regeln.

"Aufsichtsbehörde(n)" oder **"Datenschutzbehörde(n)"** bezeichnet eine unabhängige öffentliche Behörde, die von einem Mitgliedstaat der Europäischen Union oder einem anderen Staat eingerichtet wurde.



"Drittland" bedeutet ein Land, das von der Europäischen Kommission nicht als Land anerkannt wurde, das über ein angemessenes Datenschutzniveau verfügt.

"Übermittlung" bedeutet die Offenlegung, Übermittlung oder Bereitstellung von personenbezogenen Daten an Dritte.



1. Anwendungsbereich der BCR-C

Die Capgemini BCR-C gelten für alle Verarbeitungen personenbezogener Daten, die von Capgemini als für die Verarbeitung Verantwortlichem durchgeführt werden. Die Capgemini BCR-C bilden den Rahmen für alle Übermittlungen personenbezogener Daten von einem Capgemini-Unternehmen, das als für die Verarbeitung Verantwortlicher handelt, an ein anderes Capgemini-Unternehmen, die entweder als für die Verarbeitung Verantwortlicher oder als Auftragsverarbeiter handelt. Die Capgemini-Unternehmen sind dafür verantwortlich und in der Lage nachzuweisen, dass sie die BCR-C einhalten.

Wenn das lokale Recht strenger ist und ein höheres Schutzniveau verlangt als die in den BCR-C von Capgemini definierten Verpflichtungen, haben diese Vorrang vor den BCR-C. Capgemini hält sich an das geltende lokale Datenschutzrecht.

1.1 Sachlicher Anwendungsbereich

Diese BCR-C gelten für alle personenbezogenen Daten, die innerhalb von Capgemini verarbeitet werden, wenn Capgemini als Verantwortlicher handelt. Insbesondere gelten diese BCR-C für die folgenden Übermittlungen personenbezogener Daten und bilden die Rahmenbedingungen für diese:

- Von einem Capgemini-Unternehmen, welches als Verantwortlicher fungiert, zu einem anderen Capgemini-Unternehmen, das als Verantwortlicher fungiert.
- Von einem Capgemini-Unternehmen, das als Verantwortlicher fungiert, zu einem Capgemini-Unternehmen, das als Verarbeiter fungiert.

In der Praxis verarbeitet Capgemini als Verantwortlicher hauptsächlich die personenbezogenen Daten seiner Mitarbeiter und Geschäftskontakte. Die Zwecke dieser Verarbeitung stehen hauptsächlich im Zusammenhang mit Personalwesen, Cybersicherheit, interner und externer Kommunikation, Marketing und Compliance.

Einen umfassenderen Überblick über die Verarbeitungstätigkeiten von Capgemini als Verantwortlicher, einschließlich der häufigsten von Capgemini durchgeführten Datenübermittlungen, sind in Anhang 1. zu finden.

1.2 Geografischer Anwendungsbereich

Diese BCR-C gelten für alle personenbezogenen Daten, die innerhalb der Gruppe übermittelt und weiterverarbeitet werden, unabhängig davon, woher die personenbezogenen Daten stammen. Die BCR-C gelten für alle Übermittlungen personenbezogener Daten innerhalb der Gruppe, einschließlich der Weiterübermittlung.

- von einem Capgemini-Unternehmen innerhalb des EWR an ein anderes Capgemini-Unternehmen innerhalb des EWR;
- von einem Capgemini-Unternehmen innerhalb des EWR an ein Capgemini-Unternehmen außerhalb des EWR;
- von einem Capgemini-Unternehmen außerhalb des EWR an ein Capgemini-Unternehmen innerhalb des EWR;
- von einem Capgemini-Unternehmen außerhalb des EWR an ein anderes Capgemini-Unternehmen außerhalb des EWR.

Die Capgemini-Unternehmen, die zur Einhaltung dieser BCR-C verpflichtet sind, sind in Anhang 1 aufgeführt.



2. Verbindlichkeit des BCR-C

Alle Capgemini-Unternehmen und ihre Mitarbeiter sind gesetzlich verpflichtet, diese BCR-C einzuhalten.

2.1. Verbindlichkeit für Capgemini-Unternehmen

In der Praxis erteilt jedes Capgemini-Unternehmen Capgemini International BV eine Vollmacht für die Unterzeichnung der gruppeninternen Vereinbarung in seinem Namen, sodass jedes Unternehmen von Capgemini dazu verpflichtet ist, die BCR im Umgang miteinander einzuhalten. Durch die Unterzeichnung der Vereinbarung verpflichtet sich das Capgemini-Unternehmen dazu, die Bestimmungen der BCR einzuhalten und in seiner eigenen Organisation umzusetzen.

Wenn Capgemini neue Unternehmen gründet oder erwirbt, insbesondere wenn diese außerhalb des EWR angesiedelt sind, werden keine personenbezogenen Daten an diese übertragen, bis sie in der Lage sind, die BCR-C in vollem Umfang einzuhalten und gemäß dem oben genannten Mechanismus tatsächlich an sie gebunden sind.

2.2. Verbindlichkeit für Capgemini-Mitarbeiter

Alle Mitarbeiter von Capgemini sind zur Einhaltung dieser BCR-C verpflichtet, indem sie in ihrem Arbeitsvertrag ausdrücklich darauf hingewiesen werden und/oder sich in allen Arbeitsverträgen verpflichten, die Richtlinien von Capgemini, zu denen die BCR ebenfalls gehören, einzuhalten.

In der Praxis wird vor Ort eine Bewertung durchgeführt, um festzustellen, wie die BCR (Binding Corporate Rules) gemäß den geltenden Gesetzen für die Mitarbeitenden rechtsverbindlich gemacht werden können. In den meisten Fällen besteht dies darin, eine Klausel in den Arbeitsvertrag und/oder in die Kollektivvereinbarung aufzunehmen. Gegebenenfalls wird auch sichergestellt, dass die zuständigen Betriebsräte rechtzeitig informiert und/oder konsultiert werden.

Wie in den Abschnitten 10 und 17 der BCR-C näher ausgeführt, werden die Mitarbeiter von Capgemini durch interne Kommunikation und Schulungen auf die BCR und damit verbundenen Verpflichtungen aufmerksam gemacht. Die Mitarbeiter von Capgemini werden auch darauf hingewiesen, dass die Nichteinhaltung der BCR nach geltendem Recht disziplinarisch geahndet wird.

3. Umsetzung der Datenschutzgrundsätze

Capgemini verpflichtet sich, die in diesen BCR-C dargelegten Datenschutzgrundsätze einzuhalten und umzusetzen, unabhängig von den geltenden lokalen Datenschutzgesetzen, es sei denn, diese Gesetze stellen strengere Anforderungen als die in diesen BCR-C vorgesehenen.

In der Praxis bedeutet dies, dass Capgemini mindestens die in den BCR festgelegten Grundsätze und Verpflichtungen einhalten muss. Soweit das anwendbare lokale Recht von Capgemini die Einhaltung zusätzlicher oder strengerer Grundsätze und/oder Verpflichtungen verlangt, wird Capgemini auch diese einhalten.

Alle in den BCR beschriebenen Grundsätze und Verpflichtungen werden bei Capgemini durch eine Reihe von Grundsätzen, Verfahren, Leitlinien und Schulungen gefördert und umgesetzt.



3.1 Eindeutig festgelegter Zweck

Wenn Capgemini als Verantwortlicher handelt, darf sie personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erheben und weiterverarbeiten und sie nicht in einer Weise weiterverarbeiten, die mit diesen Zwecken unvereinbar ist.

In der Praxis bedeutet dies, dass der Zweck bzw. die Zwecke, zu denen personenbezogene Daten erhoben und weiterverarbeitet werden, vor der Erhebung festgelegt sein müssen. Wenn Capgemini als Verantwortlicher handelt, kann das Unternehmen personenbezogene Daten aus verschiedenen Gründen erheben und verarbeiten, insbesondere für Zwecke im Zusammenhang mit dem Personalwesen (z.B. Rekrutierung, Personalverwaltung), der Cybersicherheit, der Vermarktung von Capgeminis Angeboten usw. Im Rahmen des Prüfungs- und Genehmigungsprozesses muss der fachlich verantwortliche Projektleiter/Business Owner für jedes Projekt, das die Verarbeitung personenbezogener Daten beinhaltet, die Gründe darlegen, warum diese Daten erhoben und weiterverarbeitet werden sollen.

3.2. Rechtsgrundlage

Wenn Capgemini als für die Verarbeitung Verantwortlicher auftritt, darf sie personenbezogene Daten nur verarbeiten, wenn eine der folgenden Bedingungen erfüllt ist:

1. Die Verarbeitung ist zur Wahrung eines **berechtigten Interesses erforderlich, das von Capgemini** oder von einem Dritten verfolgt wird.

So beruft sich Capgemini beispielsweise auf ein berechtigtes Interesse als Rechtsgrundlage, wenn es die personenbezogenen Daten seiner Mitarbeiter zu sicherheitsbezogenen Zwecken verarbeitet, um sein Netzwerk, seine Vermögenswerte und/oder seine Einrichtungen zu schützen.

Wenn Capgemini sich auf das berechtigte Interesse beruft, wird eine Abwägung vorgenommen, um festzustellen, ob die eigenen berechtigten Interessen durch die Interessen oder Grundrechte und -freiheiten der betroffenen Personen, deren personenbezogene Daten verarbeitet werden, überlagert werden – insbesondere in Fällen, in denen der Schutz dieser personenbezogenen Daten erforderlich ist.

2. **Die betroffenen Personen**, deren personenbezogene Daten verarbeitet werden, **haben in diese Verarbeitung eingewilligt**. Damit eine solche Einwilligung gültig ist, muss sie freiwillig, spezifisch, informiert und unmissverständlich erfolgen.

Capgemini stützt sich beispielsweise auf die Einwilligung der betroffenen Personen, wenn personenbezogene Daten direkt von diesen erhoben werden – etwa zur Anmeldung zu einer Veranstaltung, zum Abonnieren eines Newsletters oder zum Herunterladen eines Berichts über Kontaktformulare auf der Website.

3. Die Erhebung und Weiterverarbeitung personenbezogener Daten ist für die **Erfüllung eines Vertrages erforderlich**, dessen Vertragspartei die Person ist, deren personenbezogene Daten verarbeitet werden, oder um auf Antrag der Person Maßnahmen zu ergreifen, die dem Abschluss eines solchen Vertrages vorausgehen.

Die Verarbeitung von Gehaltsinformationen und Bankkontodaten ist beispielsweise für die Auszahlung von Gehältern erforderlich, die Teil der Ausführung eines Arbeitsvertrags ist.

4. Die Verarbeitung ist erforderlich, um einer **rechtlichen Verpflichtung nachzukommen**, der Capgemini unterliegt.

So kann beispielsweise die Übermittlung personenbezogener Daten an Steuerbehörden nach geltendem Recht erforderlich sein.

In der Praxis sind dies die vier Rechtsgrundlagen, auf die Capgemini bei der Verarbeitung personenbezogener Daten am wahrscheinlichsten zurückgreift.



3.3 Datenminimierung

Capgemini wird nur die personenbezogenen Daten erheben und weiterverarbeiten, die für den/die zuvor festgelegten Zweck(e) unbedingt erforderlich sind.

In der Praxis bedeutet dies, dass Capgemini vor Beginn der Verarbeitung festlegt, welche personenbezogenen Daten erforderlich sind, um die angestrebten Zwecke zu erreichen. Folglich wird Capgemini keine nicht erforderlichen personenbezogenen Daten erheben, speichern oder anderweitig verarbeiten, nur um sie möglicherweise zu einem später definierten hypothetischen Zweck zu verwenden.

3.4 Datenqualität

Capgemini stellt sicher, dass die personenbezogenen Daten während des gesamten Lebenszyklus der Verarbeitung korrekt sind und auf dem neuesten Stand gehalten werden.

In der Praxis bedeutet dies, dass es ein Verfahren gibt, mit dem bestimmt wird, welche Daten aktualisiert oder gelöscht werden müssen, um sicherzustellen, dass die Datenqualität in den Systemen auf dem richtigen Stand bleibt. Dies bedeutet auch, dass Capgemini betroffenen Personen die Möglichkeit gibt, die Berichtigung, Aktualisierung oder Löschung unrichtiger Daten zu verlangen. So können die Mitarbeiter von Capgemini beispielsweise über ein spezielles Dashboard Änderungen an ihrem Profil vornehmen.

3.5 Einschränkung der Datenspeicherung

Capgemini bewahrt personenbezogene Daten nur so lange auf, wie es für die Zwecke, für die die personenbezogenen Daten erhoben wurden, erforderlich ist.

Das bedeutet, dass Capgemini die Aufbewahrungsfrist für die Daten im Voraus und entsprechend den Zwecken der Verarbeitung festlegt, wobei Folgendes zu berücksichtigen und abzuwägen ist:

- geltende gesetzliche Bestimmungen
- Geschäftsanforderungen
- Interessen der betroffenen Personen, deren personenbezogene Daten verarbeitet werden

In der Praxis wird Capgemini für jedes Projekt, das die Verarbeitung personenbezogener Daten beinhaltet, feststellen, ob lokale Gesetze die Aufbewahrung von Daten vorschreiben, und das Gesamtziel des Projekts mit den Interessen der betroffenen Personen abwägen. Anhand dieser Bewertung kann Capgemini die Dauer der Datenaufbewahrung für die jeweilige Verarbeitungstätigkeit festlegen.

3.6 Datensicherheit

Capgemini ergreift geeignete technische und organisatorische Maßnahmen, um die Sicherheit der ihr anvertrauten personenbezogenen Daten zu gewährleisten und sie vor unrechtmäßigem Zugriff, Verlust, Zerstörung oder Veränderung zu schützen.

In der Praxis bedeutet dies, dass Capgemini mindestens die von seiner Cybersicherheit Organisation definierten Anforderungen und bewährten Verfahren umsetzt. Diese Sicherheitsmaßnahmen werden unter Berücksichtigung der Art der zu verarbeitenden personenbezogenen Daten und der mit einer solchen Verarbeitung verbundenen Risiken entwickelt.



Im Falle einer Datenschutzverletzung hält sich Capgemini an die unternehmensinterne Richtlinie zum Management von Cybersicherheitsvorfällen und zur Meldung von Datenschutzverletzungen. Diese Richtlinie beschreibt alle notwendigen Schritte, die Capgemini zur Erfüllung der Anforderungen an das Vorfalldmanagement unternehmen muss – von der Vorbereitungsphase bis zum Abschluss.

Insbesondere wird der Datenschutzbeauftragte (DPO) in alle Vorfälle einbezogen, die personenbezogene Daten betreffen könnten, und es werden Aufzeichnungen über sämtliche derartige Vorfälle gemäß den gesetzlichen Vorgaben geführt. In der Praxis umfassen diese Aufzeichnungen die Fakten zum Vorfall, seine Auswirkungen sowie die ergriffenen Abhilfemaßnahmen und werden der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt.

Der DPO bewertet anschließend die Schwere aller Vorfälle anhand von Kriterien, die auf den Empfehlungen der ENISA (Europäische Agentur für Cybersicherheit) basieren, und legt fest, welche Meldungen und Informationen Capgemini in Anbetracht der identifizierten Risiken vornehmen muss.

- Wenn die Datenschutzverletzung voraussichtlich ein Risiko für die Rechte und Freiheiten von Personen darstellt, informiert Capgemini die zuständige(n) Aufsichtsbehörde(n) gemäß den geltenden Datenschutzgesetzen unverzüglich und spätestens innerhalb von 72 Stunden, nachdem das Unternehmen von der Verletzung Kenntnis erlangt hat.
- Darüber hinaus informiert Capgemini die betroffenen Personen unverzüglich, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.

Schließlich – und im Besonderen – informiert das Capgemini-Unternehmen, das personenbezogene Daten importiert, im Falle einer Datenschutzverletzung unverzüglich das Capgemini-Unternehmen, das die personenbezogenen Daten exportiert hat

3.7 Verarbeitung besonderer Kategorien personenbezogener Daten & Daten über strafrechtliche Verurteilungen und Straftaten

Capgemini verarbeitet besondere Kategorien personenbezogener Daten – wie Angaben zur rassischen oder ethnischen Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, Gewerkschaftszugehörigkeit sowie genetische und/oder biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten oder Angaben zum Sexualleben oder zur sexuellen Orientierung – nur, wenn dies unbedingt erforderlich und/oder gesetzlich vorgeschrieben ist.

- Die Person hat ausdrücklich in die Verarbeitung dieser personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt.
- Die Verarbeitung dieser Daten ist für Capgemini oder die betroffene Person erforderlich, um einer Verpflichtung nachzukommen oder bestimmte Rechte aus dem Arbeits-, Sozialversicherungs- und Sozialschutzrecht auszuüben.
- Die Verarbeitung ist erforderlich, um die lebenswichtigen Interessen der Person, deren Daten verarbeitet werden, oder einer anderen Person zu schützen.
- Die Verarbeitung ist für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder in Fällen, in denen Gerichte in ihrer richterlichen Funktion handeln, erforderlich.
- Die Verarbeitung ist aus Gründen eines wichtigen öffentlichen Interesses erforderlich.
- Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich, beispielsweise zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsbedrohungen.

In der Praxis sieht Capgemini von der Verarbeitung besonderer Kategorien personenbezogener Daten und/oder personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten ab, sofern nicht eine der oben genannten Bedingungen erfüllt ist.



Besondere Kategorien personenbezogener Daten und/oder Daten über strafrechtliche Verurteilungen und Straftaten werden nur dann aus dem Europäischen Wirtschaftsraum (EWR) in andere Länder übermittelt, wenn dort ein gleichwertiges Schutzniveau wie nach den EWR-Vorschriften gewährleistet ist.

3.8 Entscheidungsfindung auf Grundlage automatisierter Verarbeitung

Betroffene Personen haben das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dieses Recht gilt jedoch nicht, wenn die Verarbeitung:

- erforderlich ist für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und Capgemini
- durch geltendes lokales Recht, dem Capgemini unterliegt, erlaubt ist und dieses Recht gleichzeitig geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorsieht
- auf der ausdrücklichen Einwilligung der betroffenen Person beruht.

Darüber hinaus ist Capgemini bestrebt, den betroffenen Personen die zugrunde liegende Logik jeder sie betreffenden automatisierten Verarbeitung zu erläutern.

In der Praxis informiert Capgemini die betroffenen Personen durch einen Datenschutzhinweis, in dem dargelegt wird, wie die betroffenen Personen sich an Capgemini wenden können, um das Recht auf ein menschliches Eingreifen zu erlangen und/oder die Entscheidung anzufechten.

4. Transparenz

Capgemini stellt den betroffenen Personen alle erforderlichen Informationen über die Verarbeitung ihrer personenbezogenen Daten zur Verfügung.

Werden personenbezogene Daten direkt von den Betroffenen erhoben, so teilt Capgemini mindestens die folgenden Informationen mit:

- Die Identität und die Kontaktdaten des Unternehmens Capgemini, das als Datenverantwortlicher fungiert
- Die Kontaktdaten des zuständigen DPO
- Der Zweck/die Zwecke, zu dem/denen die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage(n) für die Verarbeitung
- Beruht die Verarbeitung auf dem berechtigten Interesse von Capgemini, ist das verfolgte Interesse von Capgemini zu beschreiben
- Die Empfänger oder Kategorien von Empfängern, falls vorhanden - dies ist in Fällen relevant, in denen Capgemini die Daten weitergeben würde
- Ob Capgemini beabsichtigt, personenbezogene Daten in Länder außerhalb des EWR zu übermitteln, und ob ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt oder nicht, oder den Verweis auf die entsprechenden Garantien (wie BCR oder Standardvertragsklauseln) und wie man eine Kopie davon erhält
- Der Zeitraum, für den personenbezogene Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien, nach denen dieser Zeitraum bestimmt wird
- Das Recht der betroffenen Person, Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung oder die Einschränkung der Verarbeitung zu verlangen oder der Verarbeitung zu widersprechen, sowie das Recht auf Übertragbarkeit
- Beruht die Verarbeitung auf der Einwilligung der betroffenen Person, so hat diese das Recht, ihre Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der Verarbeitung berührt wird
- Das Recht, eine Beschwerde bei einer Datenschutz- und/oder Aufsichtsbehörde einzureichen



- Ob die Bereitstellung personenbezogener Daten gesetzlich oder vertraglich vorgeschrieben oder für den Abschluss eines Vertrags erforderlich ist, ob die Person zur Bereitstellung der personenbezogenen Daten verpflichtet ist und welche Folgen die Nichtbereitstellung dieser Daten haben kann
- Das Vorhandensein einer automatisierten Entscheidungsfindung, einschließlich Profiling, und Informationen über die zugrunde liegende Logik sowie die Bedeutung und die voraussichtlichen Folgen einer solchen Verarbeitung für die betroffene Person

Wurden die personenbezogenen Daten nicht direkt von der betroffenen Person erhoben, so stellt Capgemini ihr dennoch innerhalb einer angemessenen Frist nach Erhebung der personenbezogenen Daten die oben genannten Informationen sowie eine Beschreibung der Kategorien personenbezogener Daten und der Quelle(n) dieser personenbezogenen Daten zur Verfügung. Werden die Daten zur Kontaktaufnahme mit der betroffenen Person verwendet, stellt Capgemini ihr die Informationen zum Zeitpunkt der ersten Kontaktaufnahme zur Verfügung.

In der Praxis stellt Capgemini den Betroffenen "Datenschutz"- oder "Privacy"-Hinweise zur Verfügung, um sie mit den notwendigen Informationen zu versorgen.

Wenn personenbezogene Daten direkt von Betroffenen für bestimmte Zwecke erhoben werden, z. B. durch benutzerseitige Anwendungen oder Tools, erstellt Capgemini angepasste Hinweise und stellt diese zur Verfügung.

Capgemini hat auch allgemeinere Datenschutzhinweise verfasst und veröffentlicht, wie z. B. den auf seiner Website verfügbaren, der ein breiteres Spektrum an Verarbeitungstätigkeiten abdeckt, z. B. die Verarbeitung im Zusammenhang mit Marketing.

5. Rechte der betroffenen Personen

Personen, deren personenbezogene Daten von Capgemini erhoben, verwendet oder anderweitig verarbeitet werden, können Auskunft über ihre Daten sowie deren Berichtigung oder Löschung verlangen. Darüber hinaus können die betroffenen Personen der Verarbeitung ihrer Daten widersprechen und haben das Recht, nicht Gegenstand von Entscheidungen zu sein, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhen. Darüber können die betroffenen Personen die Übermittlung ihrer personenbezogenen Daten in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format verlangen.

In der Praxis werden Betroffene durch spezielle Mitteilungen über ihre Rechte informiert und können ihre Rechte wahrnehmen, indem sie sich gemäß dem in Anhang 4 beschriebenen Verfahren an Capgemini wenden.

Betroffene Personen können diese Rechte ausüben, indem sie sich an den DPO oder gegebenenfalls an eine andere Kontaktstelle wenden und dabei das interne Verfahren befolgen. Betroffene Personen können über dasselbe Verfahren auch eine Beschwerde über die Verarbeitung ihrer personenbezogenen Daten einreichen.

Darüber hinaus hat jede Person das Recht, bei der/den zuständigen Aufsichtsbehörde(n) und/oder vor dem zuständigen Gericht eine Beschwerde über die Verarbeitung ihrer personenbezogenen Daten einzureichen.

Im Falle eines Verstoßes gegen die in den BCR-C garantierten Rechte und/oder Pflichten fordert Capgemini die Betroffenen auf, eine Beschwerde über das in Anhang 4 beschriebene Verfahren einzureichen. Betroffene haben jedoch auch das Recht, eine Beschwerde bei der/den zuständigen Aufsichtsbehörde(n) einzureichen - dies kann entweder die Behörde des EU-Mitgliedstaats sein, in dem sie ihren gewöhnlichen Aufenthalt haben, in dem sie arbeiten oder in dem der mutmaßliche Verstoß stattfindet. Darüber hinaus können Betroffene eine Beschwerde bei dem Gericht des Mitgliedstaats einreichen, in dem sie ihren gewöhnlichen Aufenthalt, ihren Arbeitsplatz oder den Ort des mutmaßlichen Verstoßes haben. Erfolgt die Verarbeitung personenbezogener Daten durch eine nicht dem EWR angehörende Capgemini-Unternehmen, so können die betroffenen Personen eine Beschwerde bei dem nach dem anwendbaren lokalen Recht zuständigen Gericht einreichen, es sei denn, die verarbeitende und/oder nicht dem EWR angehörende Capgemini-Unternehmen unterliegt der DSGVO; in diesem Fall gelten die oben genannten Bestimmungen.



Die betroffenen Personen haben das Recht auf gerichtliche Rechtsbehelfe und das Recht auf Wiedergutmachung und gegebenenfalls auf Entschädigung im Falle eines Verstoßes gegen einen der in Abschnitt 6 aufgeführten durchsetzbaren Bestandteile der BCR-C

Betroffene Personen können sich zur Ausübung dieser Rechte von einer gemeinnützigen Organisation oder einem Verband vertreten lassen, sofern dies nach geltendem lokalen Recht zulässig ist.

In der Praxis können Betroffene im Falle eines Verstoßes gegen die BCR-C eine Beschwerde direkt bei Capgemini und/oder bei der zuständigen Datenschutzbehörde und/oder einem Gericht einreichen. Darüber hinaus können Betroffene im Falle eines Verstoßes gegen eines der in Abschnitt 6 aufgeführten Elemente Rechtsmittel, Rechtsbehelfe und Entschädigungen beantragen.

6. Durchsetzbare Rechte betroffener Personen

Betroffene Personen können die folgenden Elemente der BCR-C als Drittbegünstigte durchsetzen:

- Die Umsetzung der in den Abschnitten 3, 4 und 12 der BCR-C aufgeführten Datenschutzgrundsätze.
- Die Verpflichtung von Capgemini zur Weitergabe relevanter Informationen an Betroffene über die ihrer personenbezogenen Daten gemäß Abschnitt 4 sowie die Verpflichtung, einen einfachen Zugang zu BCR-C gemäß Abschnitt 17 zu ermöglichen.
- Rechte des Betroffenen in Bezug auf die Verarbeitung seiner personenbezogenen Daten, wie in Abschnitt 5 vorgesehen.
- Das Recht des Betroffenen, sich über das interne Beschwerdeverfahren von Capgemini zu beschweren, wie in Abschnitt 5 aufgeführt
- Das Recht des Betroffenen, bei der/den zuständigen Aufsichtsbehörde(n) und/oder den zuständigen Gerichten eine Beschwerde einzureichen, wie in Abschnitt 5 vorgesehen.
- Die Verpflichtung jedes Capgemini-Unternehmens außerhalb des EWR, die personenbezogene Daten importiert, das Capgemini-Unternehmen im EWR, welches diese personenbezogenen Daten exportiert, sowie die Capgemini-Zentrale zu benachrichtigen, falls ein Konflikt zwischen dem anwendbaren lokalen Recht und den BCR-C besteht, wie in Abschnitt 13 vorgesehen.
- Die Verpflichtung jedes Capgemini-Unternehmens, das personenbezogene Daten importiert, das exportierende Capgemini-Unternehmen sowie den Hauptsitz von Capgemini – und sofern gesetzlich zulässig auch die betroffene Person – über Anfragen von Behörden und/oder Strafverfolgungsbehörden zum Zugriff auf personenbezogene Daten zu informieren, wie in Abschnitt 14 vorgesehen und näher erläutert.
- Die Pflicht von Capgemini zur Zusammenarbeit mit den Aufsichtsbehörden, wie in Abschnitt 16 vorgesehen.
- Die Verpflichtung für jedes EWR-Capgemini-Unternehmen, das personenbezogene Daten an ein Nicht-EWR-Capgemini-Unternehmen übermittelt, die Haftung für etwaige Verstöße gegen die BCR-C durch das Nicht-EWR-Capgemini-Unternehmen, das die Daten erhält, zu übernehmen, wie in Abschnitt 15 vorgesehen.
- Die Tatsache, dass im Falle eines Verstoßes gegen die BCR-C durch ein Nicht-EWR-Unternehmen das EWR-Capgemini-Unternehmen, das die personenbezogenen Daten exportiert hat, nachweisen muss, dass der Empfänger (d. h. das Nicht-EWR-Capgemini-Unternehmen) nicht gegen die BCR-C verstoßen hat, wie in Abschnitt 15 vorgesehen.
- Die Verpflichtung von Capgemini, Betroffene über jede Aktualisierung der BCR-C - einschließlich der Liste der an die BCR-C gebundenen Capgemini-Unternehmen - gemäß Abschnitt 18 zu informieren.
- Die Verpflichtung von Capgemini, Betroffene zu ermöglichen, die in diesem Abschnitt aufgeführten Elemente der BCR-C als Drittbegünstigte durchzusetzen.
- Das Recht von Betroffenen, im Falle eines Verstoßes gegen die in diesem Abschnitt aufgeführten durchsetzbaren Elemente der BCR-C - wie in Abschnitt 5 vorgesehen - gerichtliche Rechtsbehelfe einzulegen, Abhilfe zu schaffen und gegebenenfalls Schadenersatz zu erhalten.



7. Verfahren zur Bearbeitung von Anträgen betroffener Personen

Capgemini hat ein spezielles internes Verfahren eingerichtet, das es Betroffenen ermöglicht, Anfragen und/oder Beschwerden über die Verarbeitung ihrer personenbezogenen Daten und/oder Verstöße gegen die BCR-C einzureichen. Wie in Anhang 4 näher erläutert, können sich Betroffene direkt an die Gruppe, den regionalen und/oder lokalen DPO und/oder andere Kontaktstellen wenden.

Das in Anhang 4 beschriebene Verfahren erläutert den betroffenen Personen, wo und wie sie einen Antrag und/oder eine Beschwerde einreichen können, die Fristen für die Beantwortung, die Folgen im Falle der Ablehnung des Antrags oder der Beschwerde, die Folgen, wenn der Antrag oder die Beschwerde als gerechtfertigt angesehen wird, und das Recht der betroffenen Person, bei der/den zuständigen Aufsichtsbehörde(n) oder dem/den Gericht(en) Klage einzureichen.

In der Praxis können Betroffenen jeden Antrag in Bezug auf die Verarbeitung ihrer personenbezogenen Daten stellen, indem sie sich an einen DPO oder eine andere Kontaktstelle wenden, wie in Anhang 4 beschrieben. Capgemini bestätigt zunächst den Eingang des Antrags und kann um weitere Informationen bitten, um die Bearbeitung des Antrags zu erleichtern. Nach Prüfung des Antrags und/oder der Beschwerde entscheidet der DPO und/oder eine andere für die Bearbeitung von Anträgen zuständige Stelle, ob und inwieweit dem Antrag entsprochen werden kann, und antwortet dann dem Antragsteller.

Capgemini wird dem Anfragenden unverzüglich und in jedem Fall spätestens innerhalb von 30 Tagen nach Eingang der Anfrage antworten. Sollte Capgemini nicht in der Lage sein, die Anfrage innerhalb dieser Frist ordnungsgemäß zu bearbeiten, wird der Anfragende darüber informiert. Diese Mitteilung erfolgt innerhalb der 30-Tage-Frist und enthält eine Erklärung, dass die Prüfungs- und Bearbeitungsfrist um weitere zwei Monate verlängert werden kann, sowie eine Begründung für die Verlängerung.

Capgemini bearbeitet solche Anfragen nach seinem internen Verfahren.

8. Datenschutzorganisation von Capgemini

Capgemini hat eine gruppenweite zentrale Datenschutzstelle unter der Leitung des Group DPO sowie regionale und lokale DPO, Datenschutz-Champions und spezielle Ansprechpartner (SPOCS) ernannt (siehe Anhang 3).

Wenn Sie sich an die Datenschutzstelle der Gruppe wenden möchten, wenden Sie sich bitte an uns:

- Senden Sie uns eine E-Mail an: dpocapgemini.global@capgemini.com
- Schreiben Sie uns an die folgende Adresse: 11 rue de Tilsitt, 75017 Paris, Frankreich.

Wenn Sie sich an einen unserer örtlichen DPO wenden möchten, füllen Sie bitte die entsprechenden Kontaktformulare auf unserer [Website](#) aus.

Die DPO überwachen und gewährleisten die Einhaltung der geltenden lokalen Datenschutzgesetze und der BCR durch die Capgemini-Unternehmen in ihrem Zuständigkeitsbereich. Die DPO bieten Unterstützung in allen datenschutzrelevanten Angelegenheiten, setzen das globale Datenschutzprogramm um, bearbeiten und/oder beraten bei Datenschutzverletzungen und pflegen eine aktive Beziehung zur lokalen Aufsichtsbehörde.

Als Teil der Rechtsabteilung werden die DPO bei ihrer Aufgabe von ihren lokalen Legal-Teams unterstützt. Die DPO erstatten dem Vorstand des jeweiligen Landes oder dem Aufsichtsrat jährlich Bericht über datenschutzrelevante Angelegenheiten wie Umsetzung des globalen Datenschutzprogramms, Datenschutzprobleme, die bei großen Deals aufgetreten sind, kritische Datenschutzverletzungen und/oder gegebenenfalls Anträge von Betroffenen usw.

Die DPO fungieren als Geschäftspartner und unterstützen die verschiedenen Funktionen und Abläufe, um sicherzustellen, dass sie die Datenschutzgrundsätze und -verpflichtungen in ihrem Tagesgeschäft verstehen und umsetzen.



In der Praxis bedeutet dies, dass die behördlichen DPO eine Datenschutzstrategie und ein Datenschutzprogramm umsetzen müssen, um die Einhaltung des geltenden lokalen Rechts sowie der Gruppen-Richtlinien und -verfahren zu gewährleisten.

- Die DPO beraten die Unternehmen, wenn ein Projekt die Erhebung und Weiterverwendung personenbezogener Daten beinhaltet, um sicherzustellen, dass der Datenschutz von Anfang an einbezogen wird. Die DPO prüfen und genehmigen Projekte, die die Verarbeitung personenbezogener Daten betreffen. Darüber hinaus stellen die DPO Vorlagen, Verfahren und Leitlinien zur Verfügung, um sicherzustellen, dass die Datenschutzauflagen des Unternehmens standardmäßig berücksichtigt werden.
- Die DPO unterstützen Unternehmensjuristen bei der Prüfung und Aushandlung von Datenverarbeitungsverträgen mit Kunden, Anbietern und/oder Partnern.
- Die DPO prüfen und bewerten Datenschutzrisiken im Zusammenhang mit Geschäftsmöglichkeiten und empfehlen Maßnahmen zur Risikominderung, um diese Risiken zu beseitigen oder zu minimieren.
- Die DPO entwickeln und halten funktionspezifische Schulungen zum Datenschutz ab.
- Die DPO bearbeiten Datenschutzverletzungen in Zusammenarbeit mit der Cybersicherheit und anderen relevanten Stakeholdern, bewerten die Schwere der Verletzung, nehmen erforderliche Meldungen vor und unterstützen die Umsetzung von Abhilfemaßnahmen.
- Die DPO prüfen und bearbeiten Anfragen betroffener Personen – in Zusammenarbeit mit Group IT, HR und/oder anderen relevanten Stakeholdern.

Das DPO-Netzwerk wird von Datenschutz-Champions (DPC) unterstützt, die die einzelnen Gruppenfunktionen und gegebenenfalls die einzelnen globalen Geschäftsbereiche (GBL) vertreten. Datenschutz-Champions werden als Vertreter ihrer Funktion oder GBL ernannt, um sicherzustellen, dass die Datenschutzrichtlinien, -prozesse und -verfahren in der gesamten Gruppe ordnungsgemäß umgesetzt werden. Datenschutz-Champions spielen eine Schlüsselrolle in der Datenschutzorganisation, da sie es den DPO ermöglichen, einen besseren Einblick in die Abläufe zu erhalten, um das Unternehmen mit maßgeschneiderten Inhalten besser unterstützen zu können.

9. Privacy by Design – Datenschutz durch Technikgestaltung

9.1 Aufzeichnung der Verarbeitungstätigkeiten

Handelt Capgemini als für die Verarbeitung Verantwortlicher, so muss sie ein schriftliches Verzeichnis der Verarbeitungstätigkeiten führen und aufbewahren, welches die folgenden Informationen enthält:

- Name und Kontaktdaten des Capgemini-Unternehmens, welches als für die Verarbeitung Verantwortlicher fungiert, des zuständigen DPO und gegebenenfalls des/der gemeinsam für die Verarbeitung Verantwortlichen
- Zwecke der Verarbeitungstätigkeiten
- Eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien von verarbeiteten personenbezogenen Daten
- Die Kategorien von Empfängern, an die personenbezogene Daten weitergegeben wurden oder werden, einschließlich Empfängern außerhalb des EWR
- Gegebenenfalls sind grenzüberschreitende Übermittlungen personenbezogener Daten anzugeben, einschließlich der Empfängerländer sowie der verwendeten Übermittlungsmechanismen, mit denen diese Übermittlungen geregelt werden
- Die Dauer der Datenspeicherung



- Eine allgemeine Beschreibung der Sicherheitsmaßnahmen

In der Praxis muss der Business Owner eines Tools, einer Anwendung oder eines anderen Projekts, das die Verarbeitung personenbezogener Daten beinhaltet, einen Eintrag in das Register vornehmen, der alle oben genannten Angaben enthält. Der zuständige DPO prüft dann den Eintrag, um sicherzustellen, dass er alle erforderlichen Informationen enthält, damit er die Übereinstimmung des betreffenden Projekts mit den geltenden Datenschutzgesetzen beurteilen kann. Auf der Grundlage ihrer Bewertung gibt der DPO Empfehlungen ab, um sicherzustellen, dass der Business Owner die Verarbeitungstätigkeiten in Übereinstimmung mit dem BCR-C und den geltenden Datenschutzgesetzen durchführt.

Wenn Capgemini als Datenverarbeiter tätig ist, führt Capgemini auch Aufzeichnungen über die im Auftrag des für die Verarbeitung Verantwortlichen durchgeführten Verarbeitungstätigkeiten und behält diese bei:

- Name(n) und Kontaktdaten der Capgemini-Gesellschaft(en), die als Auftragsverarbeiter tätig ist/sind, sowie Name(n) und Kontaktdaten jedes für die Verarbeitung Verantwortlichen, in deren Auftrag die Daten verarbeitet werden
- Die Kategorien der Verarbeitungstätigkeiten, die im Auftrag jedes Verantwortlichen durchgeführt werden
- Gegebenenfalls grenzüberschreitende Übermittlungen personenbezogener Daten, einschließlich der Empfängerländer sowie der verwendeten Übermittlungsmechanismen, mit denen diese Übermittlungen geregelt werden
- Eine allgemeine Beschreibung der Sicherheitsmaßnahmen

Capgemini stellt den zuständigen Aufsichtsbehörden auf Anfrage die Aufzeichnungen über die Verarbeitung zur Verfügung.

9.2 Datenschutzfolgeabschätzung

Capgemini führt eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) durch, wenn eine Verarbeitungstätigkeit wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt.

Der Group DPO und/oder der lokale DPO bewerten die Verarbeitungstätigkeiten, um festzustellen, ob sie als "risikoreich" einzustufen sind, indem sie eine Methodik anwenden, die mit den Empfehlungen des Europäischen Datenschutzausschusses und mit anderen lokalen Praktiken und/oder Leitlinien der Datenschutzbehörde übereinstimmt.

Der Group DPO und/oder der lokale DPO stellen fest, ob für eine risikoreiche Verarbeitung eine Datenschutzfolgeabschätzung erforderlich ist, wobei sie Folgendes berücksichtigen:

1. Die Möglichkeit eines unerwünschten Ereignisses - z. B. unrechtmäßiger oder unbefugter Zugriff auf die Daten, Änderung oder Löschung der Daten usw.
2. Die Wahrscheinlichkeit, dass ein solches unerwünschtes Ereignis eintritt
3. Die Schwere der Folgen für die Rechte und Freiheiten der betroffenen Personen

In der Praxis bestimmen der Group DPO und/oder der lokale DPO bei der Überprüfung von Datenverarbeitungstätigkeiten, wie in Unterabschnitt 9.1. näher beschrieben, ob der Eigentümer eine Datenschutzfolgeabschätzung einleiten muss, indem er einen Fragebogen zur Bewertung der Risiken beantwortet. Der Group DPO und/oder der lokale DPO prüft dann die Bewertung und gibt Empfehlungen zur Minderung der Risiken ab.

Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitungstätigkeit ein hohes Risiko mit sich bringen würde, und stellt der Group DPO und/oder der lokale DPO fest, dass keine Maßnahme zur Minderung dieses Risikos ergriffen werden kann, konsultiert sie die zuständige Aufsichtsbehörde. Die Aufsichtsbehörde prüft



und bewertet die Verarbeitungstätigkeit und stellt fest, ob Capgemini die Risiken im Rahmen der Datenschutz-Folgenabschätzung ordnungsgemäß bewertet hat und ob die Schutzmaßnahmen, die Capgemini zur Behebung der Risiken zu ergreifen beabsichtigt, angemessen sind.

10. Ausbildung und Bewusstsein

10.1 Globale Pflichtschulung

Capgemini hat eine obligatorische Datenschutzschulung für alle Mitarbeiter entwickelt und durchgeführt. Das Ziel dieser Pflichtschulung ist es, sicherzustellen, dass alle Capgemini-Mitarbeiter die wichtigsten Grundsätze und Anforderungen des Datenschutzes kennen und verstehen. Dieses obligatorische E-Learning behandelt die folgenden Themen:

- Verständnis der wichtigsten Grundsätze und Anforderungen des Datenschutzes
- Datenübermittlung und Einsatz von Dienstleistern
- Umgang mit Datenschutzverletzungen
- Anfragen zur Offenlegung personenbezogener Daten durch Strafverfolgungsbehörden und/oder öffentliche Stellen (sowie andere Dritte)

Am Ende des Trainings müssen die Mitarbeiter einen Test absolvieren. Erzielen sie dabei nicht mindestens 80 %, müssen sie das gesamte Training erneut durchlaufen. Nach erfolgreichem Bestehen des Tests werden die Mitarbeiter aufgefordert, die BCR (Binding Corporate Rules) herunterzuladen, damit ihre Teilnahme am Training als ‚absolviert‘ registriert wird – insbesondere im Hinblick auf das Verfahren, das im Falle einer Anfrage zur Offenlegung personenbezogener Daten durch Dritte, Behörden oder Strafverfolgungsstellen zu befolgen ist

Capgemini-Mitarbeiter sind verpflichtet, das Datenschutztraining beim Eintritt in das Unternehmen zu absolvieren. Jährlich müssen sie zudem Datenschutz-bezogene Fragen beantworten, um ihr Wissen zu überprüfen. Können die Fragen nicht korrekt beantwortet werden, ist das vollständige Training erneut zu absolvieren. Unabhängig vom Ergebnis des Fragebogens ist das vollständige Training in jedem Fall alle drei Jahre zu wiederholen

10.2 Funktionsspezifische Schulungen und Leitlinien

Zusätzlich zum globalen obligatorischen eLearning erstellt die Datenschutzorganisation funktionsspezifische Richtlinien und Schulungen. Ziel ist es, die Funktionen mit maßgeschneiderten Inhalten besser zu unterstützen: Es geht um Anwendungsfälle, die für einige Funktionen spezifisch sind.

In der Praxis müssen alle Capgemini-Mitarbeiter unabhängig von ihrer Tätigkeitsbeschreibung das weltweit obligatorische E-Learning zum Datenschutz absolvieren, um sicherzustellen, dass sie die Grundsätze und Verpflichtungen der BCR kennen und verstehen. Darüber hinaus halten die, DPO und DPC länder- und/oder funktionsspezifische Schulungen ab.

11. Audits

Capgemini führt regelmäßig Datenschutz-Audits durch, die alle Aspekte der BCR abdecken. Die Prüfungen und Kontrollen sollen insbesondere sicherstellen, dass die BCR sowie alle damit zusammenhängenden Richtlinien, Verfahren oder Leitlinie innerhalb von Capgemini (das sogenannte "Datenschutzprogramm") sowie die geltenden Datenschutzgesetze umgesetzt, dokumentiert und bewertet werden.

Die Audits werden entweder von internen oder externen qualifizierten und unabhängigen Prüfern durchgeführt.



Capgemini führt Audits zu Datenschutzpflichten durch, die sich auf Governance- und Richtlinienaspekte beziehen („Entity Audits“), sowie zu Datenschutzpflichten, die die Umsetzung dieser Richtlinien in den tatsächlichen Verarbeitungstätigkeiten betreffen („Activity Audits“). Die Kombination all dieser Audits bildet das BCR-Auditprogramm.

In der Praxis führt Capgemini 3 Arten von Datenschutz-Audits durch:

- **Level 1 - Lokale Auditoren sind für die Prüfung ihrer lokalen Aktivitäten verantwortlich.**
 - Der lokale DPO muss jährlich eine Selbsteinschätzung seines Datenschutzprogramms durchführen.
 - Der lokale DPO ist auch für die Prüfung der lokalen Stakeholder (Zentrale Funktionen und/oder GBL) verantwortlich. Die Audits können entweder vom DPO selbst oder von einem von ihm beauftragten Dritten durchgeführt werden, um die Einhaltung der BCR und des Datenschutzprogramms von Capgemini zu überprüfen.
 - Schließlich prüft der lokale DPO die lokalen Aktivitäten (Engagement, Aktivitäten von Dienstleistern und/oder der für die Verarbeitung Verantwortlichen), um die Umsetzung des Datenschutzprogramms zu überprüfen.
- **Level 2 - Der Group DPO ist für die Prüfung lokalen Aktivitäten zuständig.**
 - Der Group DPO prüft das Datenschutzprogramm des lokalen DPO, um die Einhaltung der von der Gruppe vorgegebenen BCR zu gewährleisten.
 - Der Group DPO prüft lokale und/oder globale Aktivitäten, die sich auf die Einhaltung lokaler Vorschriften auswirken können (Aufträge, Dienstleister, Tätigkeiten von Verantwortlichen).
 - Die Level 2 - Audits können von externen qualifizierten und unabhängigen Prüfern durchgeführt werden.
- **Stufe 3 - Das interne Audit durch die Capgemini Gruppe** ist für die Prüfung sowohl der lokalen als auch der globalen DPOs, der GBL's und/oder der Zentralen Funktionen zuständig – und zwar im Hinblick auf das „Blue Book“ sowie die BCR.

Im Rahmen unserer Verpflichtung zur Umsetzung strenger Kontrollmechanismen und unter Berücksichtigung der unterschiedlichen Standorte und Strukturen unseres Unternehmens ist unser BCR-Auditprogramm so konzipiert, dass es Jahr für Jahr innerhalb eines Zeitraums von maximal fünf Jahren alle Bereiche umfasst. Auf diese Weise wird sichergestellt, dass jeder Aspekt unserer Geschäftstätigkeit innerhalb dieses Zeitrahmens dargestellt und geprüft wird.

Die Auditberichte, einschließlich der vorgeschlagenen Abhilfemaßnahmen zur Behebung und Minderung der Risiken, werden der Datenschutzorganisation - und insbesondere dem zuständigen lokalen DPO - sowie der obersten Leitung übermittelt und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt.

12. Einsatz interner oder externer Auftragsverarbeiter

12.1. Vereinbarungen zur Datenverarbeitung oder Datenschutzklauseln

Capgemini greift nur dann auf Auftragsverarbeiter innerhalb oder außerhalb der Unternehmensgruppe zurück, wenn diese ausreichende Garantien bieten, um technische und organisatorische Maßnahmen umzusetzen, die sicherstellen, dass die Verarbeitung im Einklang mit dem geltenden lokalen Datenschutzrecht erfolgt.

Wenn Capgemini eine andere Capgemini-Gesellschaft (interner Auftragsverarbeiter) oder einen Drittanbieter (externer Auftragsverarbeiter) mit der Verarbeitung personenbezogener Daten beauftragt, wird eine Vereinbarung zur Datenverarbeitung (Data Processing Agreement, DPA) oder eine Datenschutzklausel abgeschlossen, die die



Bedingungen regelt, unter denen der Auftragsverarbeiter die personenbezogenen Daten verarbeitet. Mindestens muss die DPA oder Datenschutzklausel Folgendes vorsehen:

- Die personenbezogenen Daten dürfen nur auf dokumentierte Anweisung von Capgemini verarbeitet werden – einschließlich im Hinblick auf Datenübermittlungen in Länder außerhalb des EWR
- Personen, die zur Verarbeitung personenbezogener Daten befugt sind, müssen sich zur Vertraulichkeit verpflichtet haben
- Es müssen technische und organisatorische Maßnahmen umgesetzt werden, um ein angemessenes Schutzniveau für die personenbezogenen Daten sicherzustellen
- Ein Subunternehmer darf nur mit vorheriger spezifischer oder allgemeiner Genehmigung von Capgemini eingesetzt werden, und es muss eine Vereinbarung mit diesem Subunternehmer abgeschlossen werden, die dieselben Verpflichtungen enthält wie hier beschrieben
- Capgemini muss bei der Erfüllung seiner Verpflichtung zur Beantwortung von Anfragen betroffener Personen unterstützt werden
- Capgemini muss bei der Einhaltung seiner Verpflichtungen hinsichtlich der Sicherheit der Verarbeitung, der Durchführung von Datenschutz-Folgenabschätzungen (DPIAs) und der Meldung von Datenschutzverletzungen unterstützt werden
- Nach Wahl von Capgemini und wie in der DPA oder Datenschutzklausel vereinbart, müssen die personenbezogenen Daten nach Beendigung der Dienstleistung entweder gelöscht oder zurückgegeben werden
- Capgemini müssen alle Informationen zur Verfügung gestellt werden, die erforderlich sind, um die Einhaltung der Verpflichtungen gemäß dem geltenden Datenschutzrecht, insbesondere der DSGVO, nachzuweisen, einschließlich der Ermöglichung von Datenschutz-Audits
- Jede Datenschutzverletzung muss unverzüglich gemeldet werden

In der Praxis muss Capgemini vor der Beauftragung eines externen Auftragsverarbeiters:

1. Eine Datenschutz- und Cybersicherheitsprüfung-(Due-Diligence) durchführen, um die Reife des Anbieters zu bewerten und sicherzustellen, dass personenbezogene Daten auf sichere Weise verarbeitet werden. Capgemini hat spezielle Fragebögen entwickelt, die diese Bewertung ermöglichen. Anbieter sind verpflichtet, diesen Fragebogen auszufüllen, sodass Capgemini den Reifegrad ihres Datenschutzes sowie der von ihnen zu erbringenden Dienstleistungen beurteilen kann.
2. Eine Vereinbarung abschließen, die eine DPA oder Datenschutzklausel enthält und die Bedingungen festlegt, unter denen der Anbieter personenbezogene Daten im Auftrag von Capgemini verarbeitet. Capgemini hat DPA-Vorlagen für verschiedene Szenarien erstellt – je nach Qualifikation der Parteien (Verantwortlicher/Verantwortlicher, Verantwortlicher/Auftragsverarbeiter usw.). Unabhängig davon, ob Capgemini auf eine solche Vorlage zurückgreift, wird Capgemini alle DPAs prüfen und verhandeln, um sicherzustellen, dass Anbieter personenbezogene Daten nur im Einklang mit dem geltenden Datenschutzrecht abrufen, erheben oder anderweitig verarbeiten.

12.2 Zusätzliche Verpflichtungen bei Übermittlungen in Drittländer

Zusätzlich zur Umsetzung der oben genannten DPA oder Datenschutzklausel muss Capgemini, wenn der Einsatz eines Auftragsverarbeiters mit grenzüberschreitenden Übermittlungen personenbezogener Daten verbunden ist,



sicherstellen, dass ein angemessenes Schutzniveau gewährleistet ist – gemäß den nachstehend beschriebenen Anforderungen.

In der Praxis bedeutet dies, dass:

- Wenn ein Capgemini-Unternehmen im EWR als Verantwortlicher personenbezogene Daten an ein Capgemini-Unternehmen außerhalb des EWR übermittelt, das entweder als Verantwortlicher oder als Auftragsverarbeiter handelt, gelten diese BCR-C (Binding Corporate Rules – Controller)
- Wenn ein Capgemini-Unternehmen im EWR als Verantwortlicher personenbezogene Daten an eine Drittpartei außerhalb des EWR übermittelt, die als Verantwortlicher oder Auftragsverarbeiter handelt, schließt Capgemini die entsprechenden Module der von der Europäischen Kommission genehmigten Standardvertragsklauseln ab
- Wenn ein Capgemini-Unternehmen außerhalb des EWR als Verantwortlicher personenbezogene Daten an ein Capgemini-Unternehmen oder an eine Drittpartei in einem Land übermittelt, das nach geltendem Datenschutzrecht kein angemessenes Schutzniveau bietet, implementiert Capgemini zusätzlich zu diesen BCR-C alle erforderlichen Schutzmaßnahmen, die nach dem jeweiligen Datenschutzrecht vorgeschrieben sind

Darüber hinaus muss Capgemini bei der Übermittlung personenbezogener Daten aus dem EWR in ein Land, das nicht über einen Angemessenheitsbeschluss der Europäischen Kommission verfügt, zusätzlich die Bestimmungen von Abschnitt 13 dieser BCR-C einhalten.

13. Bewertung der Auswirkungen von Datenübermittlungen (Transfer Impact Assessment - TIA)

Capgemini-Unternehmen im EWR dürfen personenbezogene Daten nur dann an Capgemini-Unternehmen außerhalb des EWR oder an Dritte – also Datenempfänger – in einem Land übermitteln, das nicht über einen Angemessenheitsbeschluss der Europäischen Kommission verfügt, wenn sie zuvor bewertet haben, dass die Gesetze und Praktiken dieses Landes den Datenempfänger nicht daran hindern, seinen Verpflichtungen gemäß den BCR nachzukommen.

Diese Bewertung muss unter der Annahme erfolgen, dass die Gesetze und Praktiken des Landes, in das die personenbezogenen Daten übermittelt werden, das Wesen der Grundrechte und -freiheiten der betroffenen Personen achten und nicht über das hinausgehen, was in einer demokratischen Gesellschaft zur Wahrung von Zielen von öffentlichem Interesse notwendig und verhältnismäßig ist.

In der Praxis muss Capgemini bei der Durchführung einer Transfer Impact Assessment (TIA) Folgendes berücksichtigen:

1. Die spezifischen Umstände der Übermittlung oder der Übermittlungen sowie etwaiger geplanter Weiterübermittlungen innerhalb desselben Landes oder in ein anderes Land, einschließlich:
 - Der Zweck(e) der Übermittlung und der weiteren Verarbeitung der Daten (z. B. Personalwesen, IT-Support usw.)
 - Die Art der an der Übermittlung beteiligten Stellen
 - Der Wirtschaftssektor des Datenimporteurs und des Datenexporteurs, in dem die Übermittlung erfolgt
 - Die Kategorie(n) und das Format der übermittelten personenbezogenen Daten
 - Der Ort der Verarbeitung, einschließlich der Speicherung
 - Die verwendeten Übertragungskanäle
2. Die Gesetze und Praktiken des Bestimmungslandes, die im Hinblick auf die Umstände der Übermittlung relevant sind – einschließlich solcher, die die Offenlegung personenbezogener Daten gegenüber Behörden verlangen oder den Zugriff durch solche Behörden erlauben, sowie solcher, die während der Übermittlung



Zugriff auf diese personenbezogenen Daten gewähren – sowie die geltenden Beschränkungen und Schutzmaßnahmen

3. Alle relevanten vertraglichen, technischen oder organisatorischen Schutzmaßnahmen, die zusätzlich zu den Schutzmaßnahmen gemäß den BCR-C umgesetzt wurden – einschließlich Maßnahmen, die während der Übermittlung und Verarbeitung personenbezogener Daten im Bestimmungsland angewendet werden.

Wenn das Transfer Impact Assessment (TIA) ergibt, dass zusätzliche Schutzmaßnahmen, über die in den BCR-C vorgesehenen hinaus erforderlich sind, müssen die übertragenden Capgemini-Unternehmen im EWR sowie deren Datenschutzbeauftragte (DPOs) benachrichtigt und in die Umsetzung dieser Schutzmaßnahmen einbezogen werden.

Capgemini überwacht fortlaufend die Gesetzgebung und Praxis in Drittländern, in denen Capgemini-Unternehmen ansässig sind und in die personenbezogene Daten gemäß den BCR-C übermittelt werden, um Änderungen zu erkennen, die eine Aktualisierung der TIA(s) und die Umsetzung zusätzlicher Schutzmaßnahmen erforderlich machen könnten.

Wenn ein Capgemini-Unternehmen außerhalb des EWR, das personenbezogene Daten importiert, Grund zur Annahme hat, dass es Gesetzen und Praktiken unterliegt, die es daran hindern, seinen Verpflichtungen gemäß den BCR-C nachzukommen, muss es das Group Data Protection Office benachrichtigen, damit geeignete zusätzliche Schutzmaßnahmen zur Sicherung der Übermittlung(en) umgesetzt werden können.

Ebenso muss ein Capgemini-Unternehmen, das personenbezogene Daten exportiert, das Group Data Protection Office benachrichtigen, wenn es Grund zur Annahme hat, dass ein Capgemini-Unternehmen als Datenimporteur seinen Verpflichtungen gemäß den BCR-C nicht mehr nachkommen kann, um sicherzustellen, dass geeignete zusätzliche Schutzmaßnahmen umgesetzt werden.

Die zuständigen lokalen Datenschutzbeauftragten (DPOs) unterstützen Capgemini-Unternehmen, die als Datenexporteur oder -importeur agieren, bei der Identifizierung und Umsetzung geeigneter zusätzlicher Maßnahmen, um sicherzustellen, dass Datenübermittlungen mit den geltenden lokalen Gesetzen und den BCR-C im Einklang stehen.

Wenn ein Capgemini-Unternehmen feststellt, dass die BCR-C – selbst nach Umsetzung zusätzlicher Maßnahmen – für eine bestimmte Übermittlung oder eine Gruppe von Übermittlungen nicht mehr eingehalten werden können, oder wenn eine zuständige Aufsichtsbehörde dies anordnet, muss die betreffende Übermittlung bzw. Gruppe von Übermittlungen sowie alle Übermittlungen, für die dieselbe Bewertung und Begründung zu einem ähnlichen Ergebnis führen würden, ausgesetzt werden, bis die Einhaltung wiederhergestellt ist oder die Übermittlung beendet wird. Wird die Einhaltung der BCR-C nicht innerhalb eines Monats nach der Aussetzung wiederhergestellt, ist die betreffende Übermittlung bzw. Gruppe von Übermittlungen zu beenden. Personenbezogene Daten, die vor der Aussetzung übermittelt wurden, sowie alle Kopien davon, sind nach Wahl des Capgemini-Unternehmens, das als Datenexporteur handelt, vollständig zurückzugeben oder zu vernichten.

Capgemini dokumentiert und archiviert alle TIAs, einschließlich der Art der umgesetzten zusätzlichen Schutzmaßnahmen zur Sicherung der Übermittlung. Diese Dokumentation ist den zuständigen Aufsichtsbehörden auf Anfrage zur Verfügung zu stellen.

In der Praxis werden die Bewertungen der Gesetze und Praktiken von Drittländern sowie die spezifisch durchgeführten Transfer Impact Assessments (TIAs) für eine Übermittlung oder eine Gruppe von Übermittlungen, die identifizierten und umgesetzten zusätzlichen Schutzmaßnahmen sowie alle relevanten Dokumentationen – einschließlich der Fälle, in denen keine zusätzlichen Maßnahmen umgesetzt werden konnten – allen Datenschutzbeauftragten (DPOs) von Capgemini zur Verfügung gestellt.

Dies ermöglicht es Capgemini, die Einhaltung der BCR-C sicherzustellen und eine einheitliche Umsetzung innerhalb der gesamten Unternehmensgruppe zu gewährleisten.



14. Umgang mit Auskunftersuchen von Behörden

Capgemini überprüft systematisch die Rechtmäßigkeit eines behördlichen Auskunfts- oder Offenlegungersuchens in Bezug auf personenbezogene Daten. Capgemini wird ein solches Ersuchen anfechten, wenn nach sorgfältiger Prüfung begründete Zweifel an der Rechtmäßigkeit des Ersuchens bestehen – insbesondere im Hinblick auf das geltende Recht, internationale Verpflichtungen sowie die Grundsätze der internationalen Höflichkeit (international comity). Unter denselben Voraussetzungen wird Capgemini auch Rechtsmittel gegen das Ersuchen einlegen, sofern dies möglich ist.

In der Praxis sind Capgemini-Mitarbeitende dazu angehalten, jedes Auskunftersuchen bezüglich personenbezogener Daten, das sie erhalten, an ihre lokale Rechtsabteilung zur Prüfung weiterzuleiten.

Wenn Capgemini ein behördliches Auskunftersuchen anfecht, wird das Unternehmen einstweilige Maßnahmen beantragen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde eine Entscheidung in der Sache getroffen hat.

Capgemini wird die angeforderten personenbezogenen Daten nicht offenlegen, solange dies nicht ausdrücklich gemäß den geltenden Verfahrensvorschriften vorgeschrieben ist.

Wenn Capgemini verpflichtet ist, auf das Ersuchen zu reagieren, wird es nur das unbedingt erforderliche Mindestmaß an Informationen bereitstellen. Darüber hinaus dürfen Übermittlungen oder Gruppen von Übermittlungen, die Capgemini zur Erfüllung eines Ersuchens einer Behörde oder Strafverfolgungsbehörde durchführt, nicht massenhaft, unverhältnismäßig oder wahllos erfolgen – also nicht über das hinausgehen, was in einer demokratischen Gesellschaft notwendig ist.

Sofern gesetzlich zulässig, wird das Capgemini-Unternehmen, das als Datenimporteur handelt, unverzüglich das Capgemini-Unternehmen, das als Datenexporteur handelt, sowie – soweit möglich – die betroffenen Personen benachrichtigen, wenn es:

1. Ein rechtlich bindendes Auskunftersuchen einer Behörde über die Offenlegung personenbezogener Daten erhält, die im Rahmen der BCR-C übermittelt wurden
2. Kenntnis von einem direkten Zugriff einer Behörde auf personenbezogene Daten erlangt, die im Rahmen der BCR-C übermittelt wurden

Diese Benachrichtigung muss alle dem als Datenimporteur handelnden Capgemini-Unternehmen zur Verfügung stehenden Informationen enthalten, insbesondere:

- die angeforderten personenbezogenen Daten
- die ersuchende Behörde
- die rechtliche Grundlage des Ersuchens sowie
- die erteilte Antwort

Wenn es dem Datenimporteur verboten ist, den Datenexporteur und/oder die betroffenen Personen zu benachrichtigen, muss er alle zumutbaren Anstrengungen unternehmen, um eine Aufhebung dieses Verbots zu erwirken, damit er so viele Informationen wie möglich und so schnell wie möglich weitergeben kann.

Diese Bemühungen sind zu dokumentieren, um sie dem Datenexporteur auf Anfrage nachweisen zu können.



In der Praxis sind alle Capgemini-Gesellschaften verpflichtet, monatlich Informationen über Anfragen von Behörden und/oder Strafverfolgungsbehörden zum Zugriff auf personenbezogene Daten, die sie erhalten haben, zu überwachen und aufzuzeichnen. Diese Berichterstattung umfasst insbesondere:

- Die Anzahl der Anfragen
- Die Art(en) der angeforderten Daten
- Die Behörde(n), die das Ersuchen gestellt hat (haben)
- Ob die Anträge angefochten wurden
- Das Ergebnis

Die lokalen und regionalen behördlichen Datenschutzbeauftragten zeichnen diese Informationen auf und teilen sie mit dem Group Data Protection Office. Die Informationen müssen für alle regionalen und lokalen Datenschutzbeauftragten zugänglich sein, so lange wie nötig aufbewahrt werden und den Aufsichtsbehörden auf Anfrage zur Verfügung gestellt werden.

Wenn es einem Capgemini-Unternehmen untersagt ist oder wird, über die oben genannten Informationen Bericht zu erstatten, muss es das Group Data Protection Office unverzüglich benachrichtigen.

15. Haftung von Capgemini im Falle eines Verstoßes gegen die BCR-C

Jedes Capgemini-Unternehmen im EWR, das personenbezogene Daten an ein Capgemini-Unternehmen außerhalb des EWR übermittelt, haftet gegenüber den betroffenen Personen für Verstöße gegen die BCR-C, die durch das Capgemini-Unternehmen außerhalb des EWR verursacht wurden.

In allen anderen Fällen – (1) Übermittlungen von einem Capgemini-Unternehmen im EWR an ein anderes Capgemini-Unternehmen im EWR, (2) Übermittlungen zwischen zwei Capgemini-Unternehmen außerhalb des EWR oder (3) Übermittlungen von einem Capgemini-Unternehmen außerhalb des EWR an ein Capgemini-Unternehmen im EWR – haftet jedes Capgemini-Unternehmen für einen Verstoß gegen die BCR-C, den es selbst verursacht hat.

Wenn eine Übermittlung zwischen zwei Capgemini-Unternehmen außerhalb des EWR eine Weiterübermittlung darstellt, haftet das Capgemini-Unternehmen im EWR, das die Übermittlung ursprünglich initiiert hat, gegenüber den betroffenen Personen für Verstöße gegen die BCR-C, die von einem der beiden Capgemini-Unternehmen außerhalb des EWR verursacht wurden.

Die Liste der Capgemini-Unternehmen ist in Anhang 1 aufgeführt. Betroffene Personen können ihre Datenschutzrechte ausüben und/oder eine Beschwerde über das in Abschnitt 7 und Anhang 4 beschriebene spezielle Verfahren von Capgemini einreichen.

In der Praxis bedeutet dies, dass das Capgemini-Unternehmen, das gemäß dem oben beschriebenen Schema als verantwortlich identifiziert wurde, die Verantwortung dafür übernehmen muss, Schadensersatz zu leisten und den Verstoß zu beheben, wenn dadurch ein Schaden für eine betroffene Person entstanden ist. Betroffene Personen können Anfragen oder Beschwerden über das dafür vorgesehene Verfahren an die zuständigen Datenschutzbeauftragten (DPOs) richten.

Wenn ein Capgemini-Unternehmen außerhalb des EWR gegen die BCR-C verstößt, sind Gerichte oder andere Justizbehörden im EWR zuständig, und betroffene Personen haben gegenüber dem haftenden Capgemini-Unternehmen im EWR (d. h. dem Capgemini-Unternehmen im EWR, das die personenbezogenen Daten an das Unternehmen außerhalb des EWR übermittelt hat) dieselben Rechte und Rechtsmittel, als ob der Verstoß im Mitgliedstaat des EWR-Unternehmens selbst erfolgt wäre.

Darüber hinaus liegt es in der Verantwortung von Capgemini nachzuweisen, dass kein Verstoß gegen die BCR-C vorliegt. Im Falle einer Übermittlung zwischen einem Capgemini-Unternehmen im EWR und einem Capgemini-Unternehmen außerhalb des EWR muss, wenn der behauptete Verstoß dem Unternehmen außerhalb des EWR



angelastet wird, das EWR-Unternehmen nachweisen, dass das Unternehmen außerhalb des EWR die BCR-C tatsächlich nicht verletzt hat.

16. Nichteinhaltung der BCR-C

Sollte ein Capgemini-Unternehmen, das als Datenimporteur auftritt, aus irgendeinem Grund nicht mehr in der Lage sein, die BCR-C einzuhalten, muss es das/die Capgemini-Unternehmen, das/die als Datenexporteur(e) fungieren, darüber informieren. Wird ein Capgemini-Unternehmen, das als Datenexporteur auftritt, auf einen Verstoß und/oder die Unfähigkeit des Datenimporteurs zur Einhaltung der BCR-C aufmerksam, muss es die Datenübermittlung aussetzen.

Das Capgemini-Unternehmen, das als Datenimporteur auftritt, muss – nach Wahl des Datenexporteurs – die im Rahmen der BCR-C übermittelten personenbezogenen Daten einschließlich aller Kopien entweder unverzüglich zurückgeben oder vollständig löschen, wenn:

- der Datenexporteur die Übermittlung ausgesetzt hat und die Einhaltung der BCR-C nicht innerhalb eines angemessenen Zeitraums, spätestens jedoch innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde oder
- der Datenimporteur in erheblichem oder wiederholtem Maße gegen die BCR-C verstößt oder
- der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde in Bezug auf seine Verpflichtungen aus den BCR-C nicht nachkommt.

Verlangt der Datenexporteur vom Datenimporteur die Löschung der Daten, so muss der Datenimporteur dem Datenexporteur zusätzlich die Löschung der Daten bestätigen. Bis zur Rückgabe oder Löschung der Daten muss der Datenimporteur weiterhin die Einhaltung der BCR-C sicherstellen.

Wenn lokale Gesetze, die für den Datenimporteur gelten, die Rückgabe oder Löschung der übermittelten personenbezogenen Daten verbieten, verpflichtet sich der Datenimporteur, weiterhin die Einhaltung der BCR-C sicherzustellen und die Daten nur in dem Umfang und für die Dauer zu verarbeiten, wie es das lokale Recht vorschreibt.

17. Zusammenarbeit mit den Aufsichtsbehörden

Capgemini arbeitet mit den Aufsichtsbehörden zusammen.

In der Praxis bedeutet dies, dass Capgemini den Empfehlungen und/oder Entscheidungen der zuständigen Aufsichtsbehörden Folge leisten und sich von diesen prüfen und/oder inspizieren lassen wird (gegebenenfalls auch vor Ort) und/oder auf Anfrage Unterlagen mit ihnen teilen wird.

Jede Streitigkeit im Zusammenhang mit der Ausübung der Aufsicht durch die zuständige Aufsichtsbehörde hinsichtlich der Einhaltung der BCR-C wird von den Gerichten des Mitgliedstaats dieser Aufsichtsbehörde gemäß dem Verfahrensrecht dieses Mitgliedstaats entschieden, und die Capgemini-Unternehmen erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

18. Leichter Zugang zu den BCR

Die öffentliche Version der BCR-C ist sowohl auf der Website von Capgemini als auch im Intranet von Capgemini verfügbar.

Die öffentliche Version der BCR-C enthält alle Elemente der internen Version, mit Ausnahme der folgenden Anhänge, bei denen es sich um vertrauliche Dokumente handelt, die nicht außerhalb der Organisation weitergegeben werden dürfen:

- Die BCR-Vereinbarung zur konzerninternen Datenübermittlung
- Capgeminis Richtlinie zur Bearbeitung von Anfragen betroffener Personen
- Stellenbeschreibungen der konzernweiten, regionalen und lokalen Datenschutzbeauftragten (DPOs)



- Capgemini verpflichtendes E-Learning zum Datenschutz
- Capgemini Datenschutz-Auditrichtlinie
- Richtlinie zum Umgang mit Anfragen zur Offenlegung personenbezogener Daten

Die jeweils aktuelle Version der BCR-C wird allen Capgemini-Mitarbeitenden zur Verfügung gestellt.

Bei einer wesentlichen Aktualisierung der BCR-C informiert Capgemini seine Mitarbeitenden durch eine gezielte Kommunikationskampagne, um sicherzustellen, dass sie ihre Pflichten und Rechte im Rahmen der BCR-C kennen und verstehen.

Darüber hinaus enthält das verpflichtende Datenschutz-E-Learning von Capgemini Verweise auf die BCR-C, und die Mitarbeitenden sind verpflichtet, die BCR-C nach Abschluss der Schulung herunterzuladen und zu lesen.

19. Aktualisierungen der BCR

Capgemini hält die BCR-C stets auf dem aktuellen Stand, insbesondere um regulatorische Änderungen – einschließlich Empfehlungen des Europäischen Datenschutzausschusses – zu berücksichtigen.

Das Group Data Protection Office ist für die Aktualisierung der BCR-C verantwortlich, einschließlich der Pflege der Liste der Capgemini-Unternehmen. Es informiert die Capgemini-Unternehmen und deren jeweilige Datenschutzbeauftragte (DPOs) unverzüglich über jede Änderung der BCR-C. In diesem Zusammenhang stellt das Group Data Protection Office auch sicher, dass betroffene Personen und/oder Aufsichtsbehörden entsprechend informiert werden.

Sollte Capgemini wesentliche Änderungen an der BCR-C vornehmen, wird zunächst die federführende Aufsichtsbehörde – die CNIL – kontaktiert und über die Änderungen informiert.

Einmal jährlich übermittelt Capgemini der CNIL alle vorgenommenen Änderungen an der BCR-C, einschließlich einer aktualisierten Liste der Capgemini-Unternehmen. Diese Mitteilung enthält auch eine Bestätigung in Bezug auf die Vermögenswerte der Gruppe.

20. Beendigung

Sollte ein Capgemini-Unternehmen, das als Datenimporteur fungiert, nicht mehr an die BCR-C gebunden sein, so muss es die im Rahmen der BCR-C übermittelten personenbezogenen Daten entweder behalten, zurückgeben oder löschen.

Die Entscheidung, ob das ehemalige Capgemini-Unternehmen die personenbezogenen Daten behalten darf, trifft das Group Data Protection Office. Wird dem ehemaligen Capgemini-Unternehmen gestattet, die personenbezogenen Daten zu behalten, verpflichtet es sich, diese Daten in Übereinstimmung mit allen geltenden Datenschutzvorschriften, einschließlich der DSGVO, zu verarbeiten.



Anhang 1 – Liste der an die BCR-C gebundenen Einheiten nach Ländern

Land	Name/ Rechtsform	Registrierungsnummer	Registrierte Adresse
Argentina	Capgemini Argentina SA	1.613.291 Inspeccion General de Justicia	Avenida Presidente Roque Sáenz Peña 615, Piso 2º, Edificio Bencich C1035AAB Buenos Aires Argentina
Australia	The WorksSydney Pty Ltd	ACN 102 213 794	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Australia	Purpose Asia Pacific Pty Ltd	ACN 625 798 807	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Australia	Capgemini Australia Pty Ltd	ACN 092 284 314	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Austria	Capgemini Consulting Österreich AG	FN 194903y Handelsgericht Wien	Millenium Tower Handelskai 94-96, 22. Stock 1200 Wien Austria
Belgium	Capgemini Belgium NV/SA	0407.184.521 Brussels	Hermeslaan 9, 1831 Machelen Belgium
Brazil	RADI Software Do Brasil Ltda	11.855.485/0001-11	Rua Alexandre Dumas, No. 1711, 1st floor, unit 101, Chácara Santo Antônio, Zip Code 04717-004, City of São Paulo, State of São Paulo Brazil
Brazil	Purpose Campaigns Do Brasil Ltda	35231013042	RUA CUBATAO 472 SAO PAULO CITY- SP Brazil
Brazil	Capgemini Brasil Ltda	65.599.953\0001-63	ALAMEDA GRAJAÚ, 60, 14º ANDAR Alphaville, Cidade de Barueri 06454-050 BARUERI, ALPHAVILLE São Paulo Brazil
Canada	Microsys Technologies Inc	001909086	3710 Nashua Drive, Suite 1 L4V 1M5 Mississauga Canada
Canada	Capgemini Solutions Canada Inc.	860883149NP002	44 Chipman Hill, 10th Floor, P.O. Box 7289 Station "A", E2L 4S6 Saint John New Brunswick Canada
Canada	Société en Commandite Capgemini Québec - Capgemini Québec LP	NEZ 3367034736	1100 boul. René-Lévesque Ouest, Suite 1110 H3B 4N4 Montréal Québec Canada
Canada	Capgemini Canada Inc	610099	44 Chipman Hill, 10th Floor, P.O. Box 7289 Station "A", E2L 4S6 Saint John New Brunswick Canada
China	Altran (Beijing) Technologies Company Limited	91110108078535347A	Room 132008, 17th FL, Building C, Tower 1 of Wangjing SOHO, No. 1 Futong East Road, Chaoyang District 100020 Beijing, China
China	Altran (Shanghai) Information & Technologies Company Limited	913101153125083000	The 3rd floor, Building 1, No. 400 Fangchun Road, Pilot Free Trade Zone 201203 Shanghai China
China	Altran (Xi'an) Technologies Company Limited	91610131MA6UQKMU7U	5th FL, A11 Building, No.156 Tian Gu 8 Road, Software New Town of Hi-tech Development Zone. Xi'an China



China	Sicon Design Technologies (Shanghai) Company Limited	9131011509422053X2	700 Shangfeng Road, Unit 8, Room 301A, Pudong 200120 Shanghai China
China	Capgemini (Hangzhou) Co Ltd	330100400004425	15F, Building E, Tiantang Software Park, 3 XiDouMen Road 310012 Hangzhou Zhe Jiang Province China
China	Capgemini Business Services (China) Limited	440101400083545	6/F Podium, Glory IFC No. 25 Ronghe Road 528200 Nanhai District, Foshan City China
China	Capgemini (China) Co Ltd	310115400049352	Room A256, Floor 2, Building 3, 2250 South Pudong Road, China (Shanghai) Pilot Free Trade Zone China
China	Capgemini (KunShan) Co Ltd	320583400050999	NO.1 Jinjie Road, service outsourcing area Huaqiao, Kunshan Jiangsu Province China
China_HK	Altran China Limited	876293	Suites 1202-04, Tower 2, The Gateway, 25 Canton Road, TST, Kowloon Hong Kong China
China_HK	Capgemini Hong Kong Ltd	536651	Suites 4101-02, 41/F., One Island East, Taikoo Place, 18 Westlands Road, Quarry Bay, Hong Kong, China
Colombia	Capgemini Colombia SAS	2197990	Cra 7 No.71 - 72 Torre B Piso 9 Bogota DC Colombia
Costa_Rica	Capgemini Costa Rica SRL (formerly Rivet Logic Costa SRL)	NUMERO DE CERTIFICACION: RNPDIGITAL-1423520-2022	San José, Escazú, Guachipelín, 400 meters north of Construplaza, Edificio Latitud Norte, 3rd floor, Quatro Legal Office
Czech_Republic	Capgemini Czech Republic SRO	260 33 062	5. května 1746/22 CZ-140 00 Praha 4 Czech Republic
Denmark	Capgemini Danmark AS	25606965	Delta Park 40 2665 Vallensbaeck Strand Denmark
Denmark	Capgemini Services Danmark ApS	43792067	Delta Park 40 2665 Vallensbaeck Strand Denmark
Egypt	Capgemini Egypt LLC	183227	Plot 202 - Sector 2, Fifth Settlement, New Cairo, Cairo 12477, Egypt
Finland	Capgemini Finland Oy	1628142-5	Keilaranta 10 E 02150 Espoo Finland
France	Knowledge Expert SAS	841 323 736 RCS THONON LES BAINS	77 T Impasse du Clou 74500 Evian les Bains France
France	Open Cascade SAS	RCS: 420 919 805 RCS NANTERRE SIRET: 420 919 805 00093	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	Capgemini Engineering Allemagne SAS [France] (formerly Altran Allemagne)	519 093 041 RCS PARIS SIRET: 519 093 041 00043	76 avenue Kléber 75016 Paris France
France	Logiqua SAS	487 550 683 RCS TOULOUSE SIRET: 487 550 683 00030	4 avenue Didier Daurat 31700 Blagnac France
France	Capgemini France SAS	328 781 786 RCS NANTERRE SIRET: 328 781 786 01143	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France



France	Sogeti SAS	434 325 973 RCS PARIS SIRET: 434 325 973 00031	11, rue de Tilsitt 75017 PARIS France
France	Altran Lab SAS	449 397 561 RCS NANTERRE SIRET: 449 397 561 00043	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
France	Altran Technology & Engineering Center SAS	817 459 357 RCS TOULOUSE SIRET: 817 459 357 00023	4 avenue Didier Daurat 31700 Blagnac France
France	Altran Prototypes Automobiles SAS	487 549 693 RCS NANTERRE SIRET: 487 549 693 00025	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
France	Altran Technologies SAS	702 012 956 RCS PARIS SIRET Paris: 702 012 956 00935 SIRET Issy: 702 012 956 00943	76 avenue Kléber 75016 Paris France
France	Capgemini Engineering ACT SAS (formerly Altran ACT)	817 459 209 RCS NANTERRE SIRET: 817 549 203 00026	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
France	Global Management Treasury Services SNC	448 370 080 RCS PARIS SIRET: 448 370 080 00054	11 rue de Tilsitt 75017 Paris France
France	Capgemini SE	330 703 844 RCS PARIS SIRET : 330 703 844 00036	11, rue de Tilsitt 75017 PARIS France
France	Capgemini Service SAS	652 025 792 RCS PARIS SIRET: 652 025 792 00084	11, rue de Tilsitt 75017 PARIS France
France	Capgemini Gouvieux SAS	428571186 RCS PARIS SIRET: 428571186 00017	11, rue de Tilsitt 75017 PARIS France
France	Immobilière Les Fontaines SARL	421 776 311 RCS PARIS SIRET: 421 776 311 00019	11, rue de Tilsitt 75017 PARIS France
France	SCI Paris Etoile	331 338 558 R.C.S PARIS SIRET: 331 338 558 00033	11, rue de Tilsitt 75017 PARIS France
France	Capgemini Latin America SAS	487 606 782 RCS PARIS SIRET: 487 606 782 00018	11, rue de Tilsitt 75017 PARIS France
France	Capgemini Ventures SAS	440 330 090 RCS PARIS SIRET: 440 330 090 00018	11, rue de Tilsitt 75017 PARIS France
France	Capgemini Technology Services SAS	479 766 842 RCS NANTERRE SIRET: 479 766 842 00724	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	Capgemini Consulting SAS	479766800 RCS NANTERRE SIRET: 479 766 800 00060	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	Capgemini Engineering Research and Development SAS	444495774 RCS NANTERRE SIRET: 444 495 774 00531	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
Germany	Capgemini Engineering Deutschland SAS & Co KG (formerly Altran Deutschland SAS & Co KG)	HRA 100894	81 Frankfurter Ring 80807 München Germany



Germany	Capgemini Deutschland Holding Gmbh	HRB 102576 Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany
Germany	Capgemini Deutschland Services Gmbh	HRB 215542 B Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany
Germany	Capgemini Engineering Service GmbH (formerly Altran Service GmbH)	HRA 89337	81 Frankfurter Ring 80807 München Germany
Germany	XL2 Gmbh	HRB 773865 Amtsgericht Stuttgart	Potsdamer Platz 5 10785 Berlin Germany
Germany	Capgemini Deutschland Gmbh	HRB 98814 Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany
Germany	Capgemini Outsourcing Services Gmbh	HRB 58881 Amtsgericht Düsseldorf	Balcke-Dürr-Allee 7 40882 Ratingen Germany
Greece	HDL Design House Greece Private Company	N° 134685604000	1, Plateia Dimokratias, Thessaloniki, 54629 (floor 6, office no. 610) Greece
Guatemala	Capgemini Business Services Guatemala SA	Company Patent - No.77886 Folio 548 Book 171 of Companies	15, avenida 5-00 Zona 13 Edificio World Technology Center Torre Sur Nivel 11 Ciudad de Guatemala Guatemala
Hungary	Restaurant Application Development International Hungary	Tax number: 23528480-2-09 EU tax number: HU23528480 Company registration number: 09-09-035337	028 Debrecen, Tüzér utca 4. A. ép. 2. em., Magyarország / H-4028 Debrecen, Tüzér Street 4. A building 2nd floor, Hungary
Hungary	Capgemini Magyarország Kft	13-09-087168 Pest County Registry Court	Rétköz utca 5 HU-1118 Budapest Hungary
India	Capgemini IT Solutions India Pte Ltd	CIN No. U74995MH2018FTC330429	5th Floor Part A, Block IV, Plot IT-3 IT-4, Airoli Knowledge Park, TTC Industrial Area, MIDC, Airoli, 400708 Navi Mumbai, Maharashtra, India
India	Leading Purpose Campaigns (India) Pte Ltd	U74999DL2018FTC329926	FIRST FLOOR D-3 SOAMI NAGAR 110017 DELHI NEW DELHI India
India	Capgemini Technology Services India Limited	U85110PN1993PLC145950	No. 14, Rajiv Gandhi Infotech Park Hinjewadi Phase-III, MIDC-SEZ, Village Man, Taluka Mulshi, 411057 PUNE, Maharashtra India
Ireland	Capgemini Ireland Ltd	67792	Ground Floor, Metropolitan Building, James Joyce Street, Dublin 1 Ireland
Israel	Altran Israel Limited	514792282	7 Rival Street 6777840 Tel-Aviv-Yafo Israel
Italy	Knowledge Expert SRL	6988270820	Via Mariano Stabile 160 90139 Palermo Italy
Italy	Capgemini Italia SPA	4877961005	Via di Torre Spaccata, 140 00173 Roma Italy
Italy	Capgemini Finance Tech SRL	16239151000	Via di Torre Spaccata, 140 00173 Roma Italy



Japan	Cambridge Consultants Japan Incorporated	9-0104-01-126095	6F Spline Aoyama Tokyu Building, 3-1-3 Minamiaoyama, Minato-ku, 107-0062 Tokyo Japan
Japan	Capgemini Japan KK	0104-02-035069	Toranomon Hills Mori Tower, 1-23-1 Toranomon, Minato-ku, Tokyo
Japan	BTC Corporation [Japan]	0100—01—193831	Mita 43MT Bld, 3-13-16 Mita, Minato-ku, Tokyo
Luxembourg	Capgemini Reinsurance International SA	163.854 RCS Luxemburg	534 rue de Neudorf 2220 Luxembourg Grand-Duché de Luxembourg
Luxembourg	Sogeti Luxembourg SA	B42610	36 Route de Longwy 8080 Bertrange Grand-Duché de Luxembourg
Malaysia	Capgemini Services Malaysia Sdn Bhd	201101031070 (959205-M)	Suite 15-01,G Tower, 199 Jalan Tun Razak 50400 Kuala Lumpur Malaysia
Mexico	Capgemini Mexico S De RL De CV	219759	Av. Santa Fe No. 428, Torre 3, Piso 15, Colonia Santa Fe Cuajimalpa, Alcaldía Cuajimalpa, Ciudad de México, 05348 Mexico
Morocco	Altran Maroc SARLU	IF N°14457667 RC N°289225	1100 boulevard Al Qods, Casanearshore, Shore 17, Quartier Sidi Maarouf 20270 Casablanca Morocco
Morocco	MG2 Engineering SA	IF N° 26143419 RC N°412549	1100 boulevard Al Qods, Casanearshore, Shore 12, Quartier Sidi Maarouf 20270 Casablanca Morocco
Morocco	Capgemini Technology Services Maroc SA	164141	Shore 8 - A - Casanearshore 1100, Boulevard Al Qods - Sidi Maarouf Casablanca Morocco
New_Zealand	Capgemini New Zealand Ltd	1128855	Level 4, 80 Willis Street Wellington, 6011 New Zealand
Norway	Capgemini Norge AS	943 574 537	Karenslyst Allé 20 0278 Oslo Norway
Norway	Matiq AS	985 149 437	Abels gate 7 7030 TRONDHEIM Norway
Philippines	Whitesky Labs (Philippines) Inc	CS201410583 Metro Manila, Philippines	3304 ROBINSONS EQUITABLE BUILDING 4 ADB AVENUE ORTIGAS MANILA Philippines
Philippines	Capgemini Digital Services Philippines Corp	CS201405679	7th Floor, Tower 2 Insular Life Corporate Centre, Insular Life Drive, Filinvest Corporate City, Alabang, 1781 Muntinlupa City, Philippines
Philippines	Capgemini Philippines Corp	CS200714668	12 Floor, 10 West Campus, McKinley West, Fort Bonifacio, Taguig City, Philippines
Poland	Capgemini Polska SP Zoo	KRS 0000040605 District Court for Warsaw, XIIth Commercial Division of the National Court Register	Ul. Żwirki i Wigury 16a 02-092 Warsaw Poland



Portugal	Capgemini Portugal SA	504272179	Av. Colégio Militar, Torre Colombo, Piso 10 Lisboa Portugal
Romania	Capgemini Services Romania SRL	J40/22612/2007 Bucharest Trade Registry	Gara Herastrau Street, no. 4D Green Court building, 4th floor Bucharest, Sector 2 Romania
Saudi_Arabia	Capgemini Saudi Ltd	1024341133776	Centria Mall Office Tower, Suite 506, 5th floor, Prince Muhammad ibn Abdulaziz Road / Olaya Street, Al Olaya District, 12241-6055 Riyadh Kingdom of Saudi Arabia
Serbia	PRIVREDNO DRUŠTVO HDL DESIGN HOUSE ZA INŽENJERING I KONSALTING EXPORT-IMPORT DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VRAČAR) [Serbia]	17376667	Golsvortijeva 35, Beograd, Serbia
Singapore	Altran (Singapore) Pte Ltd	200106758M	4 Battery Road, #25-01 Bank of China Building 049908 Singapore Singapore
Singapore	Liquidhub Pte Ltd	Registration Number : 201703318C	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Singapore	Cambridge Consultants (Singapore), Private Limited	201230536C	4 Battery Road, #25-01 Bank of China Building 049908 Singapore Singapore
Singapore	Capgemini Asia Pacific Pte Ltd	199602754G	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Singapore	Capgemini Singapore Pte Ltd	199106419N	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Slovakia	Altran Slovakia SRO	46655956	Piešťanská 3 917 01 Trnava Slovakia
Spain	Ecosat Airships SL	B-47794425	Calle Nicostrato Vela, 20 24009 León Spain
Spain	ACIE Agencia de Certification Espanola SLU	B-82271313	En calle Campezo 1, edificio 4, planta 0 28022 Madrid Spain
Spain	Capgemini Espana SL	Tomo 27.544; Folio 54; Hoja M-287781 Registro Mercantil de Madrid	Calle Puerto de Somport, Edificio Oxseo, CP 28050 Madrid Spain
Sweden	Capgemini Engineering Sverige AB (formerly Altran Sverige)	556542-2531	37 Södra Hamngatan SE 411 06 Göteborg Sweden
Sweden	Sogeti Sverige AB	556631-4687 Stockholm	Svetsarvägen 4 171 41 Solna Sweden
Sweden	Capgemini AB	556447-9763 Stockholm	Flemingatan 18, 112 26 Stockholm Sweden
Sweden	Capgemini Sverige AB	556092-3053 Stockholm	Flemingatan 18, 112 26 Stockholm Sweden
Switzerland	Knowledge Expert SA	CHE-114.807.854	9 rue de la Gabelle 1227 Carouges (GE) Switzerland



Switzerland	Capgemini Suisse SA	CHE-106.108.52 Handelsregister des Kantons Zürich	World Trade Center Leutschenbachstrasse 95 8050 Zurich Switzerland
The_Netherlands	Capgemini Semiconnext Platform BV	865742030	"Reykjavikplein 1 3543 KA Utrecht The Netherlands "
The_Netherlands	Altran Netherlands BV	34106539	1Reykjavikplein 3543KA Utrecht The Netherlands
The_Netherlands	Altran International BV	33294562	1 Reykjavikplein 3543KA Utrecht The Netherlands
The_Netherlands	Sogeti Nederland BV	30200252 Kamer van Koophandel Midden- Nederland (Utrecht)	Lange Dreef 17 4131 NJ Vianen The Netherlands
The_Netherlands	Capgemini NV	30067608 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	Capgemini Business Services BV	33030578 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	Knowledge Expert BV	85051232	Lange Viestraat 2B 3511 BK Utrecht The Netherlands
The_Netherlands	Capgemini International BV	33268283 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	Capgemini Nederland BV	30053172 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	Capgemini Sourcing BV	30135992 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	Capgemini Educational Services BV	30197497 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
Tunisia	Altran Telnet Corporation SA	Identifiant unique 1062046P Ancien numéro d'enregistrement B2455592008 (à noter : Selon la nouvelle loi relative au registre national des entreprises, le matricule fiscal sera l'identifiant unique annulant et remplaçant ainsi le numéro d'immatriculation au registre de commerce.)	Centre urbain Nord, Immeuble Ennour 1082 Tunis El Mahrajène Tunisia
Tunisia	KE Tunisie SARL	Identifiant unique 1760466T Ancien numéro d'enregistrement C0182112022 (à noter : Selon la nouvelle loi relative au registre national des entreprises, le matricule fiscal sera l'identifiant unique annulant et remplaçant ainsi	Rue du Lac Lochness, Immeuble Fajr, RDC, 1053 Les Berges du Lac, Tunis Tunisia



		le numéro d'immatriculation au registre de commerce.)	
UAE	Altran Middle East FZ-LLC	17595	1803-1804 Al Thuraya Tower 1, PO Box 502709 Dubai Media City United Arab Emirates
UK	Quorsus Limited	11521293	1 Forge End GU21 6DB Woking United Kingdom
UK	Altran UK Holding Ltd	03066512	1 Forge End GU21 6DB Woking United Kingdom
UK	Information Risk Management Ltd	03612719	1 Forge End GU21 6DB Woking United Kingdom
UK	23RED Ltd	3974936	1 Forge End GU21 6DB Woking United Kingdom
UK	Cambridge Consultants Ltd	01036298	Milton Road, Science Park - Unit 29 CB4 0DW Cambridge United Kingdom
UK	Purpose Europe Ltd	8340026	Raleigh House 14C Compass Point Business PK Stocks Bridge Way PE27 5JL ST Ives, Cambridgeshire, United Kingdom
UK	CGS Holdings Ltd	02798276 England & Wales	No. 1 Forge End, Woking GU21 6DB, Surrey United Kingdom
UK	Capgemini UK PLC	943935 England & Wales	No. 1 Forge End, Woking GU21 6DB, Surrey United Kingdom
Ukraine	Lohika LTD, LLC	37413934	50 Prakhovkyh Simi Str. 01033 Kyiv Ukraine
USA	Annik Inc	Registration Number in Florida : P07000081250	Corporation Service Company 1201 Hays Street 32301 Tallahassee, County of Leon, Florida United States of America
USA	VariQ Corporation	Employer identification number (EIN) / Tax Identification Number : 13- 4269151 (Nevada)	Corporation service company 112 North Curry street Carson city, NV 89703 United States of America
USA	Altran Engineering Solutions Inc	800653319	40600 Ann Arbor Road E, Suite 201 MI 48170- 4675 Plymouth USA
USA	Cambridge Consultants Inc	000867390	745 Atlantic Ave. 6th floor MA 02111 Boston USA Email Eve 28.09.22 : 2 Drydock Avenue Suite 1210 Boston, MA 02210
USA	Capgemini VariQ JV LLC	11267185	Corporation Service Company 100 Shockoe Slip, 2nd Floor Richmond, VA 23219 United States of America
USA	Purpose Global PBC	5045539	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America



USA	Purpose Campaigns LLC	3971119	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	Capgemini North America Inc	Registration number in Delaware: 3509818	c/o Corporation Service Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	Capgemini America Inc	Registration Number in New Jersey: 0100245598	c/o Corporation Service Company Princeton South Corporate Ctr., Ste. 160, 100 Charles Ewing Blvd., 08628 Ewing, New Jersey United States of America
USA	Capgemini Government Solutions LLC	Registration Number in Delaware: 3584244	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	Capgemini Technologies LLC	Registration number in Delaware- 3529062	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	Capgemini Business Services USA LLC	Registration Number in Delaware: 5010627	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
VietNam	Capgemini Services Vietnam Limited Liability Company (formerly Aodigy Vietnam Limited Liability Company)	401966898	150-156 Nguyen Van Linh, Vinh Trung Ward, Thanh Khe District, Da Nang City, Vietnam
VietNam	Capgemini Vietnam Co Ltd	411043001695	Centre Point Building, 106 Nguyen Van Troi, Ward 8, Phu Nhuan District, Ho Chi Minh City Vietnam
VietNam	Công Ty THNN Bigtree Technology & Consulting Vietnam	107650321	Floor 7, No. 444 Hoang Hoa Tham, Thuy Khue Ward, Tay Ho District, Hanoi, Vietnam
Thailand	Capgemini Services (Thailand) Co Ltd	N° 105557076173	8 Wework, T-One Building, 20th Floor, Soi Sukhumvit 40, Sukhumvit Road, Khlong Toei District, Phra Khanong Sub-District, Bangkok THAILAND



Anhang 2 - Capgemini-Verarbeitungstätigkeiten und wichtigste Übermittlungen

Die nachstehende Tabelle beschreibt die wichtigsten von Capgemini durchgeführten und von den BCR erfassten Datenverarbeitungsaktivitäten, bei denen Capgemini als für die Datenverarbeitung Verantwortlicher fungiert.

Die nachstehende Liste soll so vollständig wie möglich sein, erhebt jedoch keinen Anspruch auf Vollständigkeit und wird bei aktualisiert.

Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Rekrutierung, einschließlich Hintergrundüberprüfungen nach geltendem Recht	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder ▪ Finanzielle Informationen in Bezug auf Vergütung, Sozialleistungen und Pensionsregelungen, z B. Einzelheiten zu Gehalt, Bankkonto, Steuernummern, Reisekosten, Aktienoptionen, Aktienkaufplan; ▪ Informationen zur Einstellung, wie z. B. Lebenslauf, Bewerbungsformular, Gesprächsnotizen, Referenzen (falls vorhanden), Qualifikationen, Testergebnisse (falls vorhanden); ▪ Informationen zur Berufserfahrung, z.B. Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise; ▪ Fotos	Kandidaten	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Leistungsbewertung und Schulung	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Informationen zur Ausbildung; ▪ Leistungsbewertung einschließlich Jahresendbewertung	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist
Lohn- und Gehaltsabrechnung und Verwaltung anderer beschäftigungsbezogener Leistungen (einschließlich Aktienoptionen, Aktienkaufplan oder anderer Unternehmenspläne oder -leistungen)	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Finanzielle Informationen in Bezug auf Vergütung, Sozialleistungen und Pensionsregelungen, z B. Einzelheiten zu Gehalt, Bankkonto, Steuernummern, Reisekosten, Aktienoptionen, Aktienkaufplan; ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Führerscheindetails und zugehörige Dokumente, Qualifikationsaufzeichnungen, staatlich ausgestellte Identifikationsnummern	Mitarbeiter Berater von Dritten	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Alltägliche Managementtätigkeiten wie Einsatz des Personals bei Projekten, Beförderungen, Disziplinarmaßnahmen, Bearbeitung von Beschwerden	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Führerscheindetails und zugehörige Dokumente, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z.B. Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise; ▪ Angaben zu den Aufenthaltsorten der Mitarbeiter am Capgemini-Standort, soweit sie von den elektronischen Kartenzugangssystemen von Capgemini erfasst werden; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Jedes Land, in dem Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Vermarktung der professionellen Dienstleistungen von Beratern an potenzielle Capgemini-Kunden (z. B. durch Angabe von Einzelheiten über die Erfahrungen mit früheren Projekten)	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Informationen zur Einstellung, wie z. B. Lebenslauf, Bewerbungsformular, Gesprächsnotizen, Referenzen (falls vorhanden), Qualifikationen, Testergebnisse (falls vorhanden); ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z.B. Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise; ▪ Fotos.	Mitarbeiter Berater	In allen Ländern, in denen Capgemini vertreten ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Verwaltung der laufenden Leistungen, einschließlich der persönlichen Rentenversicherung von Capgemini, der Lebensversicherung und der privaten Krankenversicherung	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Finanzielle Informationen in Bezug auf Vergütung, Sozialleistungen und Pensionsregelungen, z B. Einzelheiten zu Gehalt, Bankkonto, Steuernummern, Reisekosten, Aktienoptionen, Aktienkaufplan; ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Führerscheindetails und zugehörige Dokumente, Qualifikationsaufzeichnungen, staatlich ausgestellte Identifikationsnummern	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Beschäftigungsanalyse, z. B. Vergleich des Erfolgs verschiedener Anwerbungs- und/oder Mitarbeiterbindungsprogramme	▪ Informationen zur Einstellung, wie z. B. Lebenslauf, Bewerbungsformular, Gesprächsnotizen, Referenzen (falls vorhanden), Qualifikationen, Testergebnisse (falls vorhanden); ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z.B. beruflicher Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise	Mitarbeiter Kandidaten	Indien



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Einhaltung der Gesundheits- und Sicherheitsvorschriften und anderer gesetzlicher Verpflichtungen, die Capgemini als Arbeitgeber auferlegt werden	▪ Kontakt Daten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z.B. Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Wenn notwendig, die Verarbeitung, die Capgemini in die Lage versetzen soll, ihre gesetzlichen Rechte auszuüben und/oder ihre gesetzlichen Pflichten als Arbeitgeber zu erfüllen, soweit dies nach geltendem Recht des Landes, in dem das für die personenbezogenen Daten verantwortliche Capgemini-Unternehmen niedergelassen ist, erforderlich ist	▪ Kontakt Daten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Finanzielle Informationen in Bezug auf Vergütung, Sozialleistungen und Pensionsregelungen, z B. Einzelheiten zu Gehalt, Bankkonto, Steuernummern, Reisekosten, Aktienoptionen, Aktienkaufplan; ▪ Informationen zur Einstellung, wie z. B. Lebenslauf, Bewerbungsformular, Gesprächsnotizen, Referenzen (falls vorhanden), Qualifikationen, Testergebnisse (falls vorhanden); ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Führerscheindaten und zugehörige Dokumente, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z.B. Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise; ▪ Angaben zu den Aufenthaltsorten der Mitarbeiter am Capgemini-Standort, soweit sie von den elektronischen Kartenzugangssystemen von Capgemini erfasst werden;	Mitarbeiter Berater	Länder, in denen Capgemini niedergelassen ist



	▪ Angaben zur IT und Verbindungsdaten zu den IT-Systemen von Capgemini.		
Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Human Resource Management, Laufbahnmanagement und Mobilität	▪ Kontaktdaten, wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail, Anschrift, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu unterhaltsberechtigten Personen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Finanzielle Informationen in Bezug auf Vergütung, Sozialleistungen und Pensionsregelungen, z B. Einzelheiten zu Gehalt, Bankkonto, Steuernummern, Reisekosten, Aktienoptionen, Aktienkaufplan; ▪ Informationen zur Einstellung, wie z. B. Lebenslauf, Bewerbungsformular, Gesprächsnotizen, Referenzen (falls vorhanden), Qualifikationen, Testergebnisse (falls vorhanden); ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z.B. beruflicher Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise	Mitarbeiter Kandidaten	Länder, in denen Capgemini niedergelassen ist
Interne und externe Kommunikation	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Fotos	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Katastrophenplan und Krisenmanagement	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, Kontaktdaten für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Angaben zu den Aufenthaltsorten der Mitarbeiter am Capgemini-Standort, soweit sie von den elektronischen Kartenzugangssystemen von Capgemini erfasst werden; ▪ Angaben zur IT und Verbindungsdaten zu den IT-Systemen von Capgemini; ▪ Fotos	Mitarbeiter Angehörige von Arbeitnehmern	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Audit und Statistik	▪ Kontaktdaten wie Name, Geburtsdatum, Geschlecht, Alter, Adresse, Telefonnummern, E-Mail-Adresse, Anzahl der Kinder, Staatsangehörigkeit, Ausweisdaten, Visadaten, Angaben zur Arbeitserlaubnis, für Notfälle, Angaben zu Familienangehörigen, Familienstand, Begünstigte einer Lebensversicherung, Fotos oder Bilder; ▪ Finanzielle Informationen in Bezug auf Vergütung, Sozialleistungen und Pensionsregelungen, z B. Einzelheiten zu Gehalt, Bankkonto, Steuernummern, Reisekosten, Aktienoptionen, Aktienkaufplan; ▪ Informationen zur Einstellung, wie z. B. Lebenslauf, Bewerbungsformular, Gesprächsnotizen, Referenzen (falls vorhanden), Qualifikationen, Testergebnisse (falls vorhanden); ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Informationen zur Berufserfahrung, z. B. Lebenslauf, Qualifikationen, Einzelheiten zu Projekten, an denen die Mitarbeiter gearbeitet haben, Schulungsunterlagen, Mobilitätsnachweise; ▪ Angaben zu den Aufenthaltsorten der Mitarbeiter am Capgemini-Standort, soweit sie von den elektronischen Kartenzugangssystemen von Capgemini erfasst werden; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter Kandidaten Kontaktdaten der Kunden Kontaktdaten der Lieferanten	Indien



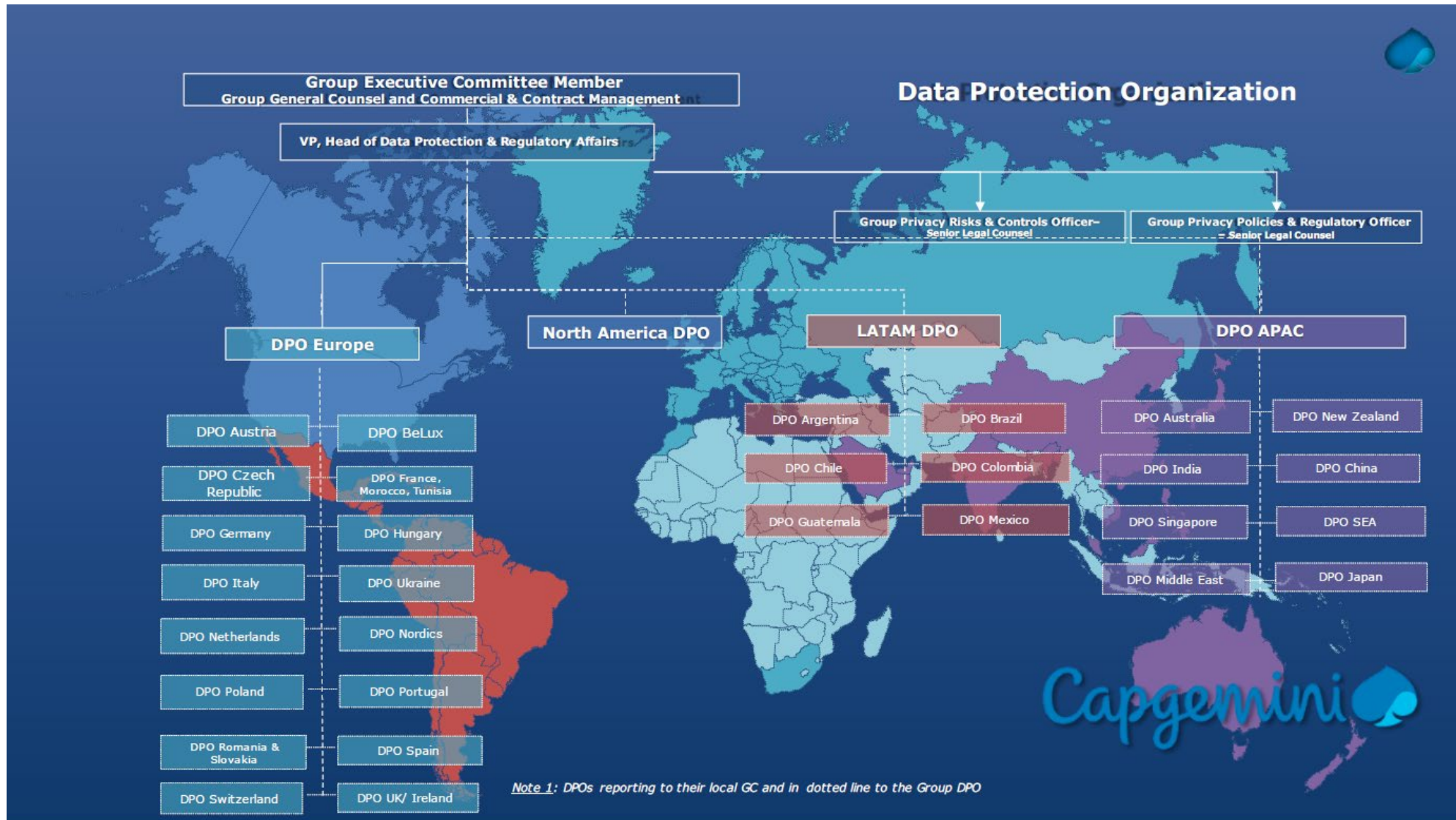
Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Verwaltung von Drittanbietern	▪ Kontaktdaten, wie Name, Adresse, Telefonnummern, E-Mail-Adresse	Daten der Betroffenen Mitarbeiter Mitarbeiter von Dritten	Länder, in denen Capgemini niedergelassen ist
Schutz vor Datenlecks	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter Mitarbeiter von Dritten	Länder, in denen Capgemini niedergelassen ist
Überwachung des Netzwerkverkehrs auf schädliche Aktivitäten	▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist
Schutz von Systemen, Netzwerken, Infrastruktur und Computern	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist
Identitäts- und Zugriffsmanagement	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist
BYOD-Programm-Management	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Informationen aus der Arbeitsverwaltung, wie z. B. Beschäftigungs- und Karriereverlauf, Besoldungsgruppen, Vorgesetzte, Einzelheiten zum Arbeitsvertrag, Abwesenheitsaufzeichnungen, Sicherheitsaufzeichnungen, Gesundheits- und Krankheitsaufzeichnungen, Unfallberichte, Übersichten über die persönliche Entwicklung, Angaben zum Führerschein und zugehörigen Dokumenten, Qualifikationsaufzeichnungen, von der Regierung ausgestellte Identifikationsnummern; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist



Zweck	Kategorien von Daten	Daten der Betroffenen	Länder, in die Daten übermittelt werden
Management von Vorfällen und Ereignissen ((Protokollierung, Behebung, Berichtigung usw.)	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist
Forensische Ermittlungen	▪ Kontaktdaten wie Name, Adresse, Telefonnummern, E-Mail-Adresse; ▪ Angaben zu IT- und Verbindungsdaten zu den IT-Systemen von Capgemini	Mitarbeiter	Länder, in denen Capgemini niedergelassen ist



Anhang 3 – Capgemini-Datenschutzorganisation





Anhang 4 - Wie können Sie Ihre Datenschutzrechte wahrnehmen?

Schlüsselbegriffe des Datenschutzes

Persönliche Daten	Alle Informationen, die zur direkten oder indirekten Identifizierung einer Person verwendet werden können, wenn sie in Kombination mit anderen verwendet werden.
Verarbeitung	Jeder Vorgang, der mit personenbezogenen Daten durchgeführt wird, wie das Sammeln, Erfassen, Organisieren, Strukturieren, Speichern, Anpassen oder Ändern, Umstrukturieren, Speichern, Anpassen oder Ändern, Abrufen, Abfragen, Verwenden, Weitergeben, Kombinieren, Einschränken, Löschen oder Vernichten
Controller	Die natürliche oder juristische Person, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.
Prozessor	Die natürliche oder juristische Person, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.
Zweck	Der Grund/die Gründe, warum der für die Verarbeitung Verantwortliche die personenbezogenen Daten erheben und weiterverarbeiten muss.



Capgemini Service SAS und/oder verbundene Unternehmen von Capgemini SE (zusammen als "**Capgemini**" bezeichnet) erhebt (erheben) und verarbeitet (verarbeiten) Ihre personenbezogenen Daten als für die Verarbeitung Verantwortlicher oder als Auftragsverarbeiter im Auftrag für die Verarbeitung Verantwortlichen. In jedem Fall können Sie sich an Capgemini wenden, um Ihre Datenschutzrechte geltend zu machen, und zwar gemäß dem nachstehend beschriebenen Verfahren.



Bitte beachten Sie, dass Sie auch eine Beschwerde bei einer Aufsichtsbehörde einreichen und/oder einen Rechtsbehelf bei Gericht einlegen können



Welche Rechte haben Sie?

Sie können beantragen, die folgenden Rechte in Bezug auf die Sie betreffenden personenbezogenen Daten, die Capgemini erhebt und weiterverarbeitet, auszuüben:

Auskunft	Sie können Capgemini fragen, ob Sie betreffende personenbezogene Daten verarbeitet werden, und wenn dies der Fall ist, können Sie Auskunft zu diesen personenbezogenen Daten verlangen.
Löschung	In einigen Fällen können Sie verlangen, dass Capgemini Ihre personenbezogenen Daten löscht.
Berichtigung	Sie können Capgemini auffordern, Ihre personenbezogenen Daten zu berichtigen, zu aktualisieren oder zu ergänzen.
Widerspruch	In einigen Fällen können Sie Capgemini auffordern, Ihre personenbezogenen Daten nicht zu verarbeiten.
Einschränkung	In einigen Fällen können Sie Capgemini auffordern, die Verarbeitung Ihrer personenbezogenen Daten auf bestimmte Zwecke und unter bestimmten Bedingungen zu beschränken.
Einwilligung zurückziehen	Sie können Ihre Zustimmung zur Verarbeitung Ihrer personenbezogenen Daten auch dann zurückziehen, wenn Sie Capgemini ursprünglich eine solche Zustimmung zur Verarbeitung der personenbezogenen Daten erteilt hatten.
Datenübertragbarkeit	In einigen Fällen können Sie Capgemini auffordern, Ihnen Ihre personenbezogenen Daten in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format zur Verfügung zu stellen und/oder diese Daten an einen anderen für die Verarbeitung Verantwortlichen zu übermitteln.
Beschwerde	Sie können sich auch beschweren, wenn Sie der Meinung sind, dass Capgemini gegen die geltende(n) Datenschutzverordnung(en) oder die BCR verstößt.

Bitte beachten Sie, dass **diese Rechte in einigen Situationen nach geltendem Recht eingeschränkt sein können**.

Dies ist beispielsweise der Fall, wenn die Gewährung der Auskunft zu Ihren personenbezogenen Daten dazu führen würde, dass personenbezogene Daten einer anderen Person offengelegt werden, oder wenn Sie Capgemini auffordern, Ihre personenbezogenen Daten zu löschen, obwohl das Unternehmen gesetzlich verpflichtet ist, sie aufzubewahren.





Kontaktieren Sie uns

Wenn Sie Ihre Rechte ausüben möchten oder Fragen oder Bedenken im Zusammenhang mit unserer Datenschutzpolitik haben, wenden Sie sich bitte an uns:



Verwenden Sie unser spezielles [Kontaktformular](#)



Per [E-Mail](#)



Per [Post](#)

(Eine vollständige Liste der Capgemini-Niederlassungen finden Sie auf unserer Website)



Per [Telefon](#)

(Eine vollständige Liste der Capgemini-Niederlassungen finden Sie auf unserer Website)

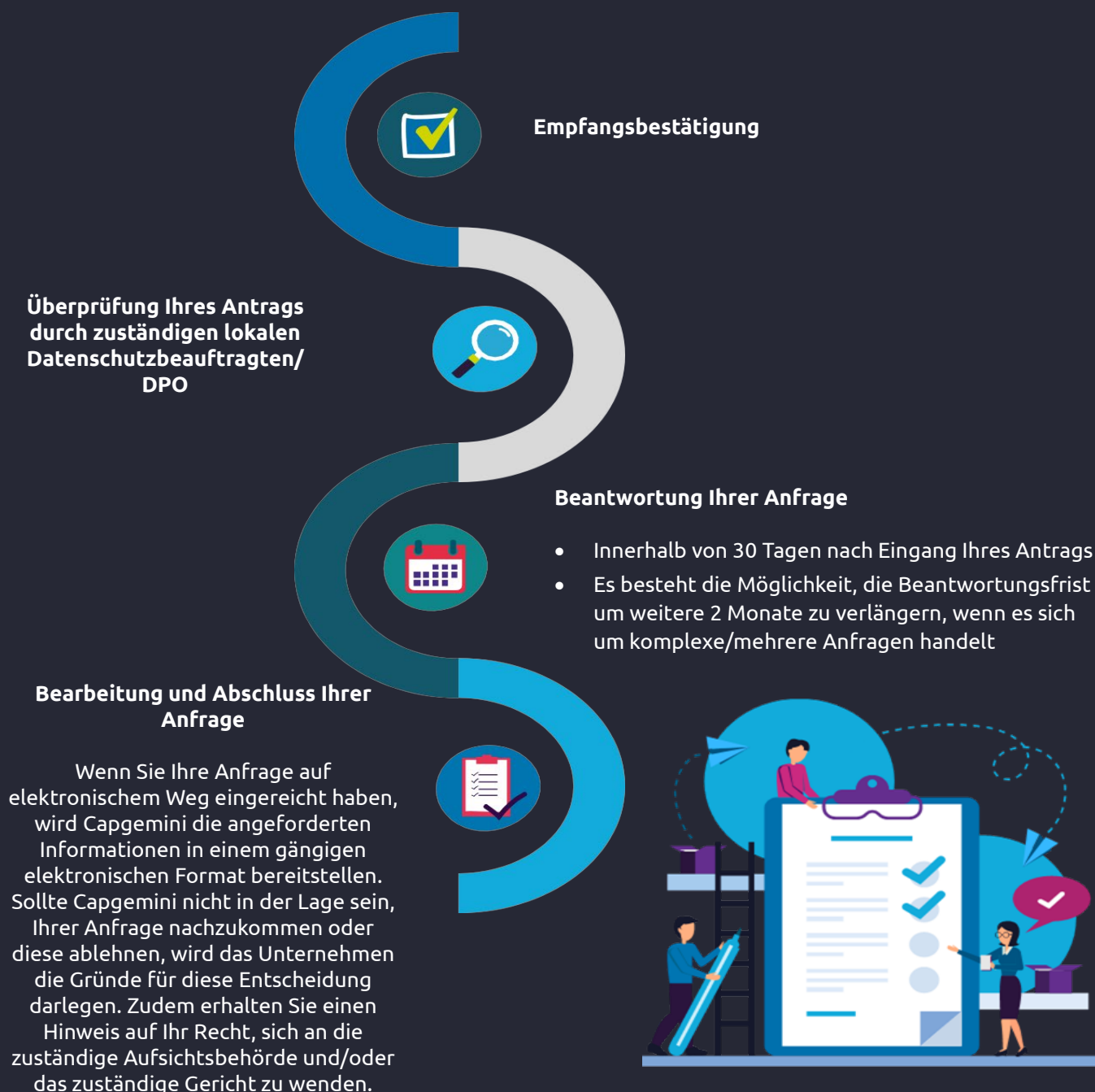
Damit wir Ihre Anfrage ordnungsgemäß bearbeiten können, teilen Sie uns bitte die folgenden Informationen mit:

- **Ihren vollständigen Namen***
- Ihren Status (Mitarbeiter, Bewerber, etc.)
- **Ihre E-Mail-Adresse oder andere bevorzugte Kommunikationsmittel***
- Identitätsüberprüfung: Sie können aufgefordert werden, geeignete Ausweispapiere vorzulegen
- Land/ Region
- **Die Art Ihrer Anfrage***

**ohne diese Angaben ist Capgemini nicht in der Lage Ihr Ersuchen zu bearbeiten*

Wie wird Capgemini Ihre Anfrage bearbeiten?

Capgemini prüft und bewertet Ihre Anfrage oder Beschwerde und geht unverzüglich darauf ein.





About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real. | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.