HERMES-GRUPPE

Verbindliche interne Vorschriften (Binding Corporate Rules, BCRs) für gruppeninterne Übertragungen personenbezogener Daten in Länder außerhalb des EWR

April 2020

1. ZWECK DER BCRs

Die HERMES-GRUPPE ist verpflichtet, die bestmögliche Kundenbetreuung zu gewährleisten und sicherzustellen, dass die Kunden uns vertrauen. In diesem Zusammenhang ist die Privatsphäre der Kunden für die HERMES-GRUPPE einer der wichtigsten Faktoren.

Gemäß den Bestimmungen der „Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (Datenschutz-Grundverordnung oder „DSGVO“) wird die Übertragung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums (EWR) durch besondere Schutzmaßnahmen geregelt, um die Nutzung personenbezogener Daten mit den europäischen Datenschutzgrundsätzen (definiert in Abschnitt 2) in Einklang zu bringen. Die Annahme und Umsetzung verbindlicher interner Vorschriften (BCRs) innerhalb der HERMES-GRUPPE zielt daher darauf ab, die gruppeninterne Datenübertragung im Zusammenhang mit personenbezogenen Daten, die von der HERMES-GRUPPE außerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet werden, gemäß den Bestimmungen der DSGVO und der EU-Richtlinie 2002/58 sowie aller anderen in Europa geltenden Gesetze und Vorschriften zu regeln.

Die HERMES-GRUPPE nimmt diese BCRs als ein wichtiges Werkzeug wahr, um unsere Kultur des Datenschutzes innerhalb der HERMES-GRUPPE effektiv zu fördern. Diese BCRs fördern auch die Datenschutz-Compliance und erleichtern die Verwaltung personenbezogener Daten innerhalb der gesamten Gruppe.

Darüber hinaus sind die HERMES-GRUPPE und ihre Mitarbeiter für den Schutz und die Einhaltung der Rechte in Bezug auf personenbezogene Daten verantwortlich, auf die sie Zugriff haben. Daher sind wir der Ansicht, dass unsere BCRs ein unentbehrliches Werkzeug sind, um diese wichtige Verantwortung effektiv zu verwalten und unsere Kultur in Bezug auf Datenschutz innerhalb der Gruppe weiterzugeben.

Im Hinblick auf den Anwendungsbereich unserer BCRs müssen Unternehmen der HERMES-GRUPPE, die den BCRs unterliegen, und Mitarbeiter der HERMES-GRUPPE die folgenden Bestimmungen sowie das maßgebliche Datenschutzrecht einhalten. Die HERMES-GRUPPE hat eine effektive Governance-Struktur eingerichtet, um diese Datenschutzverpflichtungen zu verwalten.

Auf lokaler Ebene und gemäß den Bedingungen unserer BCRs muss jeder lokale Datenverantwortliche eine BCR-Vereinbarung unterzeichnen und auf täglicher Basis jeden notwendigen Schritt ergreifen, um die Einhaltung der Bestimmungen der BCRs sicherzustellen. Die Einhaltung dieser Bestimmungen und Verfahren hängt besonders von Schulungsprogrammen und Prüfungsaktivitäten ab.

Aufgrund ihres weiten Umfangs im Hinblick auf die Datenschutz-Compliance wird die Verwendung von BCRs auf lokaler Ebene zweifellos das Management der Datenschutz-Compliance auf lokaler Ebene erleichtern und dabei helfen, sicherzustellen, dass örtliche Vertreter die Verantwortung für den Datenschutz übernehmen.

Sollte ein Verstoß gegen die BCRs festgestellt werden, können (rechtliche, technische oder organisatorische) Maßnahmen sowie angemessene Sanktionen (gegen den lokalen Datenverantwortlichen oder gemäß dem örtlichen Arbeitsgesetz gegen einen lokalen Mitarbeiter) auf Initiative des Hauptverantwortlichen, des globalen CRM-Managers, des globalen Datenschutzbüros, des lokalen Datenverantwortlichen oder des lokalen CRM-Managers ergriffen werden.

2. DEFINITIONEN UND DATENSCHUTZGRUNDSÄTZE

2.1. BEGRIFFSBESTIMMUNGEN

Die in den BCRs verwendeten Begriffe und Ausdrücke sind in Anhang 1 definiert, vorausgesetzt, diese Begriffe und Ausdrücke werden immer gemäß der DSGVO und der Richtlinie 2002/58 ausgelegt.

2.2. DATENSCHUTZGRUNDSÄTZE

Im Rahmen der BCRs (siehe Absatz 3) muss jede Übermittlung personenbezogener Daten in Übereinstimmung mit den Bestimmungen der DSGVO und Richtlinie 2002/58 an ein Drittland, das kein angemessenes Schutzniveau gewährleistet, immer den folgenden Datenschutzgrundsätzen entsprechen, die in bestimmten Absätzen der BCRs oder in Anhang 2 definiert sind.

- **Fairness und Transparenz der Verarbeitung**: Die Fairness erfordert, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Alle Informationen in Bezug auf die Verarbeitung der personenbezogenen Daten der betroffenen Personen werden in einem präzisen, transparenten, verständlichen und leicht zugänglichen Format zur Verfügung gestellt, wobei klare und verständliche Formulierungen verwendet werden (siehe Anhang 2).

- **Rechtmäßigkeit**: Damit die Verarbeitung rechtmäßig ist, wird die Verarbeitung personenbezogener Daten auf Basis der Einwilligung der betroffenen Person oder anderer legitimer Basis verarbeitet, einschließlich der Notwendigkeit der Einhaltung der gesetzlichen Verpflichtungen, denen der Verantwortliche unterliegt, usw. (siehe Anhang 2).
- **Zweckbegrenzung**: Personenbezogene Daten werden für festgelegte, explizite und legitime Zwecke erhoben und nicht auf Arten weiterverarbeitet, die mit diesen Zwecken nicht kompatibel sind (siehe Anhang 2).
- **Datenminimierung**: Personenbezogene Daten sind angemessen, relevant und auf das, was im Zusammenhang mit den Zwecken erforderlich ist, für die sie erhoben und/oder verarbeitet werden, beschränkt (siehe Anhang 2).
- **Datenqualität**: Personenbezogene Daten müssen korrekt sein und gegebenenfalls auf dem neuesten Stand gehalten werden (Richtigkeit) (siehe Anhang 2)
- **Begrenzte Speicherfristen:** Personenbezogene Daten werden in einer Form aufbewahrt, die es ermöglicht, betroffene Personen nicht länger zu identifizieren, als dies für die Zwecke erforderlich ist, für die die Daten erhoben oder für die sie weiterverarbeitet werden (siehe Anhang 2).
- **Datenschutz durch Technikgestaltung/Datenschutz durch datenschutzfreundliche Voreinstellungen**: Es ist notwendig, angemessene technische und organisatorische Maßnahmen umzusetzen, die entwickelt wurden, um diese Datenschutzgrundsätze effektiv umzusetzen und die notwendigen Sicherheitsmaßnahmen in die Verarbeitung zu integrieren. Diese Maßnahmen müssen sicherstellen, dass grundsätzlich nur personenbezogene Daten, die für den jeweiligen spezifischen Zweck der Verarbeitung erforderlich sind, verarbeitet werden (siehe Anhang 2).
- **Sicherheit und Vertraulichkeit**: Angemessene technische und organisatorische Maßnahmen müssen umgesetzt werden, um personenbezogene Daten vor versehentlichem/r oder unrechtmäßigem/r Vernichtung, Verlust, Veränderung, unbefugtem/r Offenlegung oder Zugriff sowie gegen alle anderen unrechtmäßigen Formen der Verarbeitung zu schützen (siehe Absatz 5.4).
- **Weiterleitung an Organisationen, die nicht an BCRs gebunden sind:** Die HERMES-GRUPPE setzt angemessene Sicherheitsmaßnahmen um, wenn personenbezogene Daten an ein Unternehmen übertragen werden sollen, das nicht Teil der HERMES-GRUPPE ist (siehe Absatz 5.6 und Anhang 2).
- **Verantwortlichkeit**: Der lokale Datenverantwortliche ist für die Einhaltung der oben genannten Datenschutzgrundsätze verantwortlich und muss die Einhaltung dieser nachweisen können.

3. ANWENDUNGSBEREICH DER BCRs

3.1. GEOGRAFISCHER ANWENDUNGSBEREICH

Die BCRs gelten für Übertragungen von personenbezogenen Daten zwischen Unternehmen der HERMES-GRUPPE, die überall auf der Welt ansässig sind, und die die BCRs oder eine gruppeninterne BCR-Vereinbarung unterzeichnet haben.

Anhang 3 enthält eine Liste aller Unternehmen der HERMES-GRUPPE, die an die BCRs gebunden sind.

3.2. SACHLICHER ANWENDUNGSBEREICH

Die Art und der Zweck der personenbezogenen Daten, die im Rahmen der BCRs übertragen werden, sind in Anhang 4 aufgeführt.

3.3. ABGEDECKTE UNTERNEHMEN

Der Zweck dieser BCRs besteht darin, einen Rahmen für gruppeninterne Übertragungen personenbezogener Daten zwischen den in Anhang 3 aufgeführten Unternehmen der HERMES-GRUPPE festzulegen, die entweder als lokale Datenexporteure oder als lokale Datenimporteure handeln.

Alle Unternehmen der HERMES-GRUPPE verpflichten sich, diese BCRs nach Unterzeichnung der gruppeninternen BCR-Vereinbarung (Anhang 5) zu befolgen.

4. EFFEKTIVITÄT DER BCRs

4.1. TRANSPARENZ UND RECHT AUF INFORMATIONEN

Um die Datenverarbeitung fair zu gestalten, müssen personenbezogene Daten immer auf transparente Weise erhoben und verarbeitet werden. Daher gilt:

1. Die BCRs müssen jeder betroffenen Person jederzeit zur Verfügung stehen und daher auf den Internet- und Intranetseiten der HERMES-GRUPPE hochgeladen werden. Eine betroffene Person muss stets in der Lage sein, auf Anfrage eine Kopie der BCRs vom lokalen CRM-Manager, dem lokalen Datenverantwortlichen, dem globalen CRM-Manager oder dem globalen Datenschutzbüro einzuholen. Die HERMES-GRUPPE stellt betroffenen Personen zudem die folgenden Informationen zur Verfügung:

a. Informationen über ihre Drittbegünstigtenrechte hinsichtlich der Verarbeitung ihrer personenbezogenen Daten und die Mittel, um diese Rechte auszuüben (siehe Absatz 5.3 unten);
b. Informationen über die Klausel bezüglich der Haftung (siehe Absatz 5.4 unten);
c. Informationen zu den Datenschutzgrundsätzen (siehe Anhang 2);
d. auf Anfrage Informationen zur Art der Vereinbarung zwischen gemeinsam Verantwortlichen (falls vorhanden) (siehe auch Absatz 5.6 unten).

2. Darüber hinaus werden spezifische FAQs für Kunden auf Internetwebsites der HERMES-GRUPPE zur Verfügung gestellt, um Fragen zu klären, die betroffene Personen möglicherweise zu den BCRs oder verwandten Themen haben, z. B. Bedenken oder Anträge im Zusammenhang mit der Übermittlung eines Zugriffsantrags auf ihre personenbezogenen Daten (siehe Absatz 5.2) oder Einreichung eines Anspruchs (siehe Absatz 5.3).

3. Die betroffenen Personen sind berechtigt, über die Verarbeitung ihrer personenbezogenen Daten informiert zu werden. Lokale CRM-Manager können in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro Mitteilungsvorlagen an jeden lokalen Datenverantwortlichen innerhalb der Gruppe zu jedem Zweck übermitteln, der die Bereitstellung von Informationen an die betroffenen Personen betrifft.

4. Wenn in Bezug auf eine bestehende Verarbeitung ein neuer Zweck oder eine neue Empfängerkategorie entsteht, muss die entsprechende Informationsmitteilung angepasst und müssen die entsprechenden betroffenen Personen über diese Änderung informiert werden.

5. Die HERMES-GRUPPE stellt einer betroffenen Person mindestens die folgenden Informationen zur Verfügung, außer sie verfügt bereits über diese Informationen:
    a. die Identität und Kontaktdaten des lokalen Datenverantwortlichen und ggf. seines Vertreters;
    b. ggf. die Kontaktdaten des zuständigen Datenschutzbeauftragten;
    c. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
    d. die berechtigten Interessen, die vom lokalen Datenverantwortlichen oder von einer Drittpartei (wenn die Verarbeitung auf dieser Grundlage erfolgt) verfolgt werden;
    e. die Empfänger oder Kategorien von Empfängern der Daten;
    f. soweit zutreffend, die Tatsache, dass der lokale Datenverantwortliche beabsichtigt, personenbezogene Daten in ein Drittland zu übertragen, sowie die Einzelheiten der relevanten Sicherheitsmaßnahmen, einschließlich der Existenz oder Nichtexistenz einer Angemessenheitsentscheidung durch die Europäische Kommission, und die Arten, auf die eine Kopie dieser erhalten werden kann oder diese eingesehen werden können;
    g. die Dauer, für die die personenbezogenen Daten gespeichert werden (oder die Kriterien für die Festlegung dieser Dauer);
    h. das Bestehen eines Rechts auf Auskunft seitens des lokalen Datenverantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie ggf. des Rechts auf Datenübertragbarkeit;
    i. wenn die Verarbeitung auf der Einwilligung der betroffenen Person als rechtmäßige Grundlage für die Verarbeitung oder für die Verarbeitung besonderer Kategorien personenbezogener Daten beruht, das Recht, die Einwilligung jederzeit zu widerrufen, ohne die Rechtmäßigkeit der Verarbeitung auf Basis der Einwilligung vor dem Widerruf zu beeinträchtigen;
    j. das Bestehen eines Rechts auf Beschwerde bei einer Aufsichtsbehörde;
    k. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist, sowie ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte;
    l. das Bestehen automatisierter Entscheidungen im Einzelfall einschließlich Profiling, einschließlich aussagekräftiger Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person;
    m. die Absicht, die personenbezogenen Daten zu einem anderen Zweck als dem zu verarbeiten, für den sie erhoben wurden;
    n. aus welcher Quelle die personenbezogenen Daten stammen und ob sie gegebenenfalls aus einer öffentlich zugänglichen Quelle stammen (wenn personenbezogene Daten nicht direkt von der betroffenen Person eingeholt wurden).

Verarbeitung

Wenn die Daten nicht direkt von den betroffenen Personen bezogen wurden, stellt die HERMES-GRUPPE den relevanten betroffenen Personen innerhalb einer angemessenen Frist, jedoch spätestens innerhalb eines Monats, nach Erhalt die oben genannten Informationen unter Berücksichtigung der spezifischen Umstände, unter denen die personenbezogenen Daten verarbeitet werden, zur Verfügung. Wenn die personenbezogenen Daten für die Kommunikation mit der betroffenen Person verwendet werden sollen, werden solche Informationen spätestens zum Zeitpunkt der ersten Mitteilung an diese betroffene Person bereitgestellt, oder wenn eine Offenlegung an einen anderen Empfänger vorgesehen ist, spätestens wenn die personenbezogenen Daten zum ersten Mal offengelegt werden.

Gemäß Artikel 14 Absatz 5 der DSGVO, der gilt, wenn die personenbezogenen Daten nicht direkt von den betroffenen Personen bezogen wurden, erfolgt diese Weitergabe von Informationen an die betroffene Person ungeachtet einer in den nationalen Rechtsvorschriften festgelegten spezifischen Bestimmung ausnahmsweise nicht, (i) wenn die betroffene Person bereits über die Informationen verfügt; (ii) wenn sich die Bereitstellung dieser Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand bedeuten würde; oder (iii) wenn das Einholen oder Offenlegen ausdrücklich per Gesetz festgelegt ist, dem der Datenverantwortliche unterliegt, und das angemessene Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht; oder (iv) wenn die personenbezogenen Daten vertraulich bleiben müssen, vorbehaltlich einer gesetzlich geregelten Verpflichtung zum Berufsgeheimnis (einschließlich einer gesetzlichen Geheimhaltungspflicht).

4.2. RECHT AUF ZUGRIFF, BERICHTIGUNG, LÖSCHUNG, EINSCHRÄNKUNG DER VERARBEITUNG, WIDERSPRUCH GEGEN DIE VERARBEITUNG UND DATENÜBERTRAGBARKEIT

Betroffene Personen sind berechtigt, darüber in Kenntnis gesetzt zu werden, welche Informationen die HERMES-GRUPPE über sie besitzt und diese Informationen unter Kontrolle zu halten. Daher gilt:

1. Jede betroffene Person hat (nachdem sie ihre Identität nachgewiesen und einen konkreten Antrag an die HERMES-GRUPPE gestellt hat) das Recht:

a. **von der HERMES-GRUPPE ohne Einschränkung in angemessenen Abständen und ohne übermäßige Verzögerung oder Kosten** das Folgende zu erhalten:
   - Aufklärung darüber, ob personenbezogene Daten im Zusammenhang mit der betroffenen Person verarbeitet werden;
   - wenn dies der Fall ist, Informationen zu den Elementen g), i), k), l), n), p) und r) gemäß Absatz 4.1.5 oben;
   - wenn personenbezogene Daten in ein Drittland übertragen werden, Informationen über die entsprechenden Sicherheitsmaßnahmen, die für die Datenübertragung verwendet werden;
   - eine Information in einer verständlichen Form über die Daten, die verarbeitet werden und ggf. die verfügbaren Informationen über ihre Quelle.
   -

b. **von der HERMES-GRUPPE unverzüglich die Berichtigung falscher personenbezogener Daten über sie zu verlangen.** Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen;

c. **von der HERMES-GRUPPE unverzüglich die Löschung personenbezogener Daten zu verlangen, wenn einer der folgenden Umstände vorliegt**: i) wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder anderweitig verarbeitet werden, nicht mehr erforderlich sind; ii) wenn die betroffene Person die der Verarbeitung zugrunde liegende Einwilligung widerruft und es keinen anderen Rechtsgrund und keine übergeordneten triftigen Gründe für die Verarbeitung gibt; iii) wenn die betroffene Person der Verarbeitung gemäß Punkt g. unten widerspricht, wenn keine übergeordneten triftigen Gründe für die Verarbeitung vorliegen oder die betroffene Person der Verarbeitung zum Zwecke des Direktmarketings gemäß Punkt h. unten widerspricht; iv) wenn die personenbezogenen Daten rechtswidrig verarbeitet wurden; v) wenn die personenbezogenen Daten gelöscht werden müssen, um einer gesetzlichen Verpflichtung nachzukommen, der die HERMES-GRUPPE unterliegt; vi) wenn die personenbezogenen Daten im Zusammenhang mit Diensten der Informationsgesellschaft erhoben wurden, wobei hiervon alle Dienste abgedeckt sind, die normalerweise gegen Honorar aus der Ferne mit elektronischen Geräten zur Verarbeitung und Speicherung von Daten erbracht werden;

   Macht die HERMES-GRUPPE die personenbezogenen Daten öffentlich und wird dann zu deren Löschung verpflichtet, so trifft die HERMES-GRUPPE angemessene Maßnahmen, auch technischer Art, um Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten bzw. zu Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat (dies unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten) und verlangt, dass der Verantwortliche diesem Antrag nachkommt;

   Ausnahmen von diesem Recht auf Löschung gelten jedoch, i) wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit erforderlich ist; ii) wenn dies zur Einhaltung einer gesetzlichen Verpflichtung oder zur Erfüllung einer Aufgabe, die im öffentlichen Interesse oder in Ausübung der dem Datenverantwortlichen übertragenen behördlichen Befugnis ausgeführt wird, notwendig ist; iii) wenn dies aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken, zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen notwendig ist;

d. **von der HERMES-GRUPPE die Einschränkung der Verarbeitung zu verlangen,** wenn einer der folgenden Gründe zutrifft: i) wenn die Richtigkeit der personenbezogenen Daten angefochten wird (dies betrifft den Zeitraum, der zur Überprüfung der Richtigkeit der Daten erforderlich ist); ii) wenn die Verarbeitung rechtswidrig ist und die betroffene Person die Einschränkung ihrer Nutzung beantragt; iii) wenn die HERMES-GRUPPE die Verarbeitung personenbezogener Daten nicht mehr benötigt, diese jedoch von der betroffenen Person für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden; und iv) wenn die betroffene Person einer Verarbeitung widersprochen hat, die die HERMES-GRUPPE auf der Grundlage des berechtigten Interesses der HERMES-GRUPPE vorgenommen hat (dies betrifft den Zeitraum, der erforderlich ist, um zu überprüfen, ob die triftigen Gründe der HERMES-GRUPPE vor denen der betroffenen Personen ggf. Vorrang haben);

e. **von der HERMES-GRUPPE zu verlangen, Dritte, an die die personenbezogenen Daten offengelegt wurden, über jegliche Berichtigung, Löschung oder Einschränkung, die in Übereinstimmung mit (b), (c), (d) ausgeführt wurde, zu informieren** es sei denn, dies ist unmöglich oder umfasst eine unverhältnismäßige Anstrengung. Der lokale Datenverantwortliche unterrichtet die betroffene Person über diese Dritten, wenn die betroffene Person dies verlangt;

f. **ihr Recht auf Datenübertragbarkeit auszuüben** und von der HERMES-GRUPPE das Recht zu erhalten, ihre personenbezogenen Daten, die sie der HERMES-GRUPPE zur Verfügung gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten ohne Hinderung durch die HERMES-GRUPPE an einen anderen Verantwortlichen zu übertragen, wenn die Verarbeitung auf Einwilligung oder auf einem Vertrag beruht und die Verarbeitung automatisiert erfolgt;

g. **der Verarbeitung** der personenbezogenen Daten der betroffenen Person (basierend auf dem berechtigten Interesse der HERMES-GRUPPE) jederzeit **aufgrund von überzeugenden triftigen Gründen in Bezug auf die besondere Situation der betroffenen Person zu widersprechen**.

Gemäß der DSGVO kann die Ausübung dieser Rechte bestimmten Beschränkungen unterliegen; lokale Datenverantwortliche können insbesondere Anträge ablehnen, die offensichtlich übermäßig umfassend sind, insbesondere, wenn sie sehr oft, wiederholt oder systematisch immer wieder gestellt werden;

h. **der Verarbeitung personenbezogener Daten jederzeit, kostenlos und ohne Angabe von triftigen Gründen zu widersprechen,** wenn diese zu Zwecken des Direktmarketings, einschließlich Profiling, erfolgt bzw. informiert zu werden, bevor personenbezogene Daten zum ersten Mal an Dritte offengelegt werden oder in deren Auftrag zu Zwecken des Direktmarketings verwendet werden, sowie über das Recht, einer solchen Offenlegung oder Nutzung kostenlos zu widersprechen, ausdrücklich informiert zu werden.

2. Konkrete Richtlinien und Verfahren müssen innerhalb der Gruppe auf lokaler Ebene vorhanden sein, um die Ausübung der oben genannten Rechte sicherzustellen. Insbesondere die Mitarbeiter der HERMES-GRUPPE, die personenbezogene Daten erheben, verarbeiten oder Zugriff auf personenbezogene Daten haben, müssen geschult werden, um Anträge einer betroffenen Person in Bezug auf Zugriff, Berichtigung, Löschung, Einschränkung, Widerspruch oder Übertragbarkeit zu erkennen. Jeder Antrag muss gemäß dem lokalen Verfahren bestätigt und gehandhabt werden.

3. Eine konkrete Antwort erhält die betroffene Person systematisch innerhalb einer angemessenen Frist (d. h. spätestens innerhalb eines Monats nach Erhalt des Antrags). Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die HERMES-GRUPPE unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine solche Fristverlängerung, zusammen mit den Gründen für die Verzögerung.

4. Wenn der Antrag legitim ist, muss die HERMES-GRUPPE alle notwendigen Schritte ergreifen, um die Angelegenheit in angemessener Zeit zu handhaben. Wenn der Antrag abgelehnt wird, wird der betroffenen Person der Grund für die Ablehnung schriftlich (oder per E-Mail) mitgeteilt. In diesem Fall kann die betroffene Person den in Absatz 4 festgelegten internen Beschwerdeprozess befolgen.

5. Lokale CRM-Manager müssen in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro sowohl den lokalen Datenverantwortlichen als auch den betroffenen Personen immer zur Verfügung stehen, um sie bei Bedarf im Zusammenhang mit den Anträgen betroffener Personen zu unterstützen.

4.3. AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL EINSCHLIEßLICH PROFILING

1. Gemäß maßgeblichem Datenschutzrecht hat jede betroffene Person das Recht, sich zu weigern, Entscheidungen unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhen, die ihr gegenüber rechtliche Wirkung entfalten oder sie erheblich beeinträchtigen.

2. Das oben Genannte gilt nicht, wenn die Entscheidung:
   - für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und der HERMES-GRUPPE erforderlich ist;
   - aufgrund von maßgeblichem Datenschutzrecht, dem die HERMES-GRUPPE unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten;
   - mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

4.4. INTERNER BESCHWERDEMECHANISMUS

1. Wenn eine betroffene Person der Ansicht ist, dass ihre personenbezogenen Daten nicht in Übereinstimmung mit den BCRs oder dem maßgeblichen Datenschutzrecht verarbeitet werden, kann die betroffene Person gemäß dem BCR-Beschwerdeverfahren eine Beschwerde bei einem der folgenden Stakeholder (zum Beispiel beim lokalen Datenschutzbeauftragten) einreichen, deren Unabhängigkeit während der Wahrnehmung ihrer Aufgaben garantiert wird.
2. Konkrete Richtlinien und Verfahren müssen innerhalb der Gruppe auf lokaler Ebene vorhanden sein, um sicherzustellen, dass ein Beschwerdemechanismus einheitlich ist und dass den betroffenen Personen angemessene Informationen über diese Verfahren bereitgestellt werden. Wenn eine Beschwerde registriert wird, muss sie innerhalb einer angemessenen Frist bestätigt und gehandhabt werden (d. h. spätestens innerhalb eines Monats nach Erhalt des Antrags. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die HERMES-GRUPPE unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine solche Fristverlängerung, zusammen mit den Gründen für die Verzögerung).
3. Alle Vertreter und Mitarbeiter der HERMES-GRUPPE müssen auf lokaler Ebene größte Anstrengungen unternehmen, um den lokalen Datenverantwortlichen oder den lokalen CRM-Manager bei der Beilegung einer Beschwerde zu unterstützen. Alle von einem lokalen Datenverantwortlichen oder einem Mitarbeiter erhaltenen Datenschutzbeschwerden werden dem/den zuständigen Datenschutzkontakt(en) unverzüglich übermittelt.

4. Wenn die Vertreter der Hermes-Gruppe den Anspruch auf lokaler Ebene nicht lösen können, muss der Beschwerdeabwicklungsmechanismus das Problem an den globalen CRM-Manager oder das globale Datenschutzbüro weiterleiten, die innerhalb von höchstens einem Monat nach Erhalt des Antrags antworten müssen. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die HERMES-GRUPPE unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine solche Fristverlängerung, zusammen mit den Gründen für die Verzögerung.

5. Jedes Unternehmen der HERMES-GRUPPE, das diesen BCRs unterliegt, muss auf seiner Internetwebsite, sofern verfügbar, praktische Tools zur Verfügung stellen, die betroffenen Personen ermöglichen, ihre Beschwerden einzureichen, einschließlich mindestens eines der folgenden:
    a. E-Mail-Adresse
    b. Telefonnummer
    c. Postanschrift

6. Jeder lokale Datenverantwortliche und lokale CRM-Manager erstattet dem rechtlichen globalen CRM-Manager und dem globalen Datenschutzbüro regelmäßig über die auf lokaler Ebene beigelegten Beschwerden Bericht, um Korrekturmaßnahmen zu ergreifen und die innerhalb der Gruppe umgesetzten Richtlinien und Verfahren zu verbessern, sollten die Beschwerden „Lücken“ in Bezug auf die Einhaltung des Datenschutzes ergeben.

7. Um Zweifel auszuschließen, versteht sich, dass die betroffene Person das Recht hat, bei der zuständigen Aufsichtsbehörde (sofern die DSGVO anwendbar ist, bei der in dem EU-Mitgliedstaat ihres gewöhnlichen Aufenthalts, ihres Arbeitsplatzes oder des Ortes des mutmaßlichen Verstoßes) und/oder vor den zuständigen Gerichten (sofern die DSGVO anwendbar ist, vor dem Gericht des Mitgliedstaats, in dem der lokale Datenverantwortliche eine Niederlassung hat oder in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat) eine Beschwerde einzureichen, wenn die betroffene Person mit der Antwort der Vertreter der Hermes-Gruppe auf lokaler und globaler Ebene nicht zufrieden ist oder wenn die betroffene Person den verfügbaren internen Beschwerdemechanismus lieber umgehen möchte (siehe Absatz 5.3).
   Die betroffene Person wird über die Möglichkeit informiert, dass sie einen Anspruch, bevor sie einen Fall an die zuständige Aufsichtsbehörde oder ein zuständiges Gericht weiterleitet, auch über den oben beschriebenen internen Beschwerdemechanismus und das BCR-Beschwerdeverfahren lösen kann.

4.5. SICHERHEIT UND VERTRAULICHKEIT/BEZIEHUNG MIT AUFTRAGSVERARBEITERN, DIE MITGLIEDER DER GRUPPE SIND

4.5.1. Allgemeine Sicherheits- und Vertraulichkeitsgrundsätze

Die Gewährleistung, dass personenbezogene Daten vor Datenschutzverletzungen angemessen geschützt sind, ist eine der obersten Prioritäten der HERMES-GRUPPE. Daher gilt:

1. Jeder lokale Datenverantwortliche muss angemessene technische und organisatorische Maßnahmen umsetzen, um personenbezogene Daten vor Verletzungen zu schützen, wobei der Stand der Technik und die Kosten der Umsetzung, die Art, der Umfang, Kontext und Zweck der Verarbeitung sowie das Risiko unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden müssen.

   Darüber hinaus müssen die umgesetzten Maßnahmen (i) ein Sicherheitsniveau gewährleisten, das hinsichtlich der mit der Verarbeitung verbundenen Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist, beispielsweise gegebenenfalls die Pseudonymisierung und Verschlüsselung personenbezogener Daten; (ii) die Fähigkeit, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit von Verarbeitungssystemen und -diensten sicherstellen; (iii) die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls rechtzeitig wiederherzustellen sicherstellen; (iv) ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluation der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sicherstellen.

   Folglich müssen angemessene Richtlinien und Verfahren zur Informationssicherheit innerhalb der Gruppe entworfen und umgesetzt werden. Diese Sicherheitsrichtlinien legen alle angemessenen physischen und logischen Maßnahmen fest, um eine versehentliche Vernichtung, Änderung oder unbefugte Offenlegung oder unbefugten Zugriff auf personenbezogene Daten zu verhindern oder abzuwenden. Diese Richtlinien und Verfahren werden regelmäßig geprüft (siehe Absatz 4.9).

2. Besondere Kategorien personenbezogener Daten werden mit erweiterten und spezifischen Sicherheitsmaßnahmen verarbeitet.

3. Der Zugriff auf personenbezogene Daten ist auf die Empfänger beschränkt, die diesen ausschließlich benötigen, um ihre beruflichen Pflichten zu erfüllen. Disziplinarische Maßnahmen können vorkommen, wenn ein Mitarbeiter der HERMES-GRUPPE die entsprechenden Sicherheitsrichtlinien und -verfahren nicht einhält.

4. Im Falle einer Verletzung des Schutzes personenbezogener Daten müssen Sie:
    - jegliche Verletzung des Schutzes personenbezogener Daten dem zuständigen Datenschutzbeauftragten oder Datenschutzkontakt (z. B. dem lokalen CRM-Manager) melden, der dann unverzüglich den Hauptverantwortlichen, den globalen CRM-Manager und das globale Datenschutzbüro benachrichtigt;
    - jegliche Verletzung des Schutzes personenbezogener Daten (einschließlich der Fakten im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, deren Wirkung und der ergriffenen Abhilfemaßnahmen) dokumentieren und die Dokumentation auf Anfrage den Aufsichtsbehörden bereitstellen;

- die Verletzung des Schutzes personenbezogener Daten unverzüglich, jedoch möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, den zuständigen Aufsichtsbehörden melden, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen;
- die betroffenen Personen über jegliche Verletzung des Schutzes personenbezogener Daten, die sie erheblich beeinflussen könnte, sowie die Maßnahmen, die für ihre Lösung ergriffen wurden, informieren.

4.5.2. Beziehung zu Auftragsverarbeitern, die Mitglieder der HERMES-GRUPPE sind

Wenn ein lokaler Datenverantwortlicher verlangt, dass ein anderes Unternehmen der HERMES-GRUPPE in seinem Namen die Verarbeitung personenbezogener Daten übernimmt (zum Zwecke der Verarbeitung der Art der personenbezogenen Daten und der Kategorien der betroffenen Personen, wie in Anhang 4 der BCRs beschrieben, jedoch ausschließlich für die vom lokalen Datenverantwortlichen festgelegte(n) Themen und Dauer (die je nach Fall kurz oder lang sein kann)), sind die folgenden Sicherheitsvorkehrungen zu beachten:

1. Wenn die Verarbeitung durchgeführt wird, muss der lokale Datenverantwortliche einen Auftragsverarbeiter auswählen, der hinsichtlich der technischen und organisatorischen Maßnahmen, die die Verarbeitung regeln, ausreichende Garantien gewährleistet, und die Einhaltung dieser Maßnahmen sicherstellen. Jedes Unternehmen der HERMES-GRUPPE, das durch die Unterzeichnung der gruppeninternen BCR-Vereinbarung in Anhang 5 an die BCRs gebunden ist und im Auftrag eines lokalen Datenverantwortlichen als Auftragsverarbeiter fungiert, verpflichtet sich bei seiner Tätigkeit als Auftragsverarbeiter im Auftrag eines lokalen Datenverantwortlichen, diese ausreichenden Garantien in Bezug auf die geltenden technischen und organisatorischen Sicherheitsmaßnahmen für die durchzuführende Verarbeitung zu gewährleisten und alle hierin enthaltenen Sicherheitsvorkehrungen zu erfüllen, sowie die Einhaltung dieser Maßnahmen sicherzustellen. Lokale CRM-Manager können in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro Vorlagen der entsprechenden Datenverarbeiter-Klauseln an einen lokalen Datenverantwortlichen innerhalb der Gruppe übermitteln.

2. Das zuständige Unternehmen der HERMES-GRUPPE (Auftragsverarbeiter) darf die personenbezogenen Daten nur gemäß den Anweisungen des lokalen Datenverantwortlichen verarbeiten, es sei denn, es ist gesetzlich zu etwas anderem verpflichtet. In diesem Fall muss der Auftragsverarbeiter den lokalen Datenverantwortlichen unverzüglich benachrichtigen (es sei denn, dies ist gesetzlich verboten oder wichtiger Bestandteil des öffentlichen Interesses).

3. Das zuständige Unternehmen der HERMES-GRUPPE (Auftragsverarbeiter) verpflichtet sich:
   - zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
   - technische und organisatorische Sicherheitsmaßnahmen umzusetzen, um die personenbezogenen Daten vor jeglichen Datenschutzverletzungen ausreichend zu schützen;
   - die Bedingungen für die Beauftragung anderer Auftragsverarbeiter zu beachten (siehe unten);
   - den lokalen Datenverantwortlichen unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Absatz 5.2 oben genannten Rechte betroffener Personen nachzukommen;
   - den lokalen Datenverantwortlichen bei der Sicherstellung der Einhaltung seiner Verpflichtungen hinsichtlich der Sicherheit personenbezogener Daten, der Benachrichtigung über Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und der vorherigen Konsultation der lokalen Aufsichtsbehörde (sofern erforderlich) zu unterstützen;
   - nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des lokalen Datenverantwortlichen entweder zu löschen oder zurückzugeben sowie bestehende Kopien zu löschen, sofern nicht nach nationalem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
   - dem Datenverantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten zur Verfügung zu stellen und Prüfungen ihrer Verarbeitungstätigkeiten – einschließlich Inspektionen –, die vom lokalen Datenverantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und zu diesen beizutragen;
   - den lokalen Datenverantwortlichen zu informieren, wenn seiner Ansicht nach eine Anweisung die maßgeblichen Datenschutzvorschriften verletzt;
   - Verfahren zur Verwaltung von Datenschutzverletzungen und zur Benachrichtigung des lokalen Datenverantwortlichen, sobald eine Verletzung des Schutzes personenbezogener Daten festgestellt wird, sowie zur kontinuierlichen Unterstützung umzusetzen;
   - dem lokalen Datenverantwortlichen auf Anfrage zu erlauben, eine Prüfung seiner Verarbeitungstätigkeiten durchzuführen, um sicherzustellen, dass der Auftragsverarbeiter solche ausreichenden Sicherheitsmaßnahmen ergreift;
   - personenbezogene Daten ohne die vorherige ausdrückliche Einwilligung des lokalen Datenverantwortlichen nicht an Dritte außerhalb der HERMES-GRUPPE weiterzugeben (siehe auch Absatz 5.6 unten bezüglich der Übertragung von Daten außerhalb der HERMES-Gruppe). Im Falle einer erlaubten Offenlegung werden einem Dritten die oben dargelegten Datenschutzverpflichtungen vom zuständigen Unternehmen der HERMES-GRUPPE (Auftragsverarbeiter) über einen Vertrag auferlegt. Wenn ein solcher Dritter seine Datenschutzverpflichtungen nicht erfüllt, bleibt das zuständige Unternehmen der HERMES-GRUPPE (Auftragsverarbeiter) dem lokalen Datenverantwortlichen gegenüber für die Erfüllung der Verpflichtungen dieses anderen Dritten vollständig haftbar.

4. Der lokale Datenverantwortliche stimmt zu, dass ein Unternehmen der HERMES-GRUPPE, das als Auftragsverarbeiter agiert, ein anderes Unternehmen innerhalb der HERMES-GRUPPE für die Unterverarbeitung verwenden kann. In diesem Fall verpflichtet sich der Erstauftragsverarbeiter, den lokalen Datenverantwortlichen über alle beabsichtigten Änderungen in Bezug auf die Auftragsverarbeiter zu informieren, wodurch der lokale Datenverantwortliche die Möglichkeit erhält, dieser Änderung zu widersprechen.

5. Wenn der Auftragsverarbeiter die Zwecke und Mittel einer Verarbeitung festlegt, gilt der Auftragsverarbeiter als Datenverantwortlicher in Bezug auf diese Verarbeitung.

6. Das zuständige Unternehmen der HERMES-GRUPPE (Auftragsverarbeiter) muss im Auftrag des lokalen Datenverantwortlichen ein Verzeichnis der Verarbeitungstätigkeiten führen.

7. Der zuständige Auftragsverarbeiter haftet für Schäden, die durch die Verarbeitung verursacht werden, wenn er den Verpflichtungen der BCR, die speziell für den Auftragsverarbeiter gelten, nicht nachkommt oder wenn er gegen gesetzliche Anweisungen eines lokalen Datenverantwortlichen oder darüber hinaus handelt (es sei denn, er beweist, dass er für das Ereignis, das den Schaden verursacht hat, in keiner Weise verantwortlich ist).

8. Sind sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter (oder mehr als ein Verantwortlicher oder Auftragsverarbeiter) an derselben Verarbeitung beteiligt und sind sie für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, um eine wirksame Entschädigung der betroffenen Person zu gewährleisten. Hat ein Verantwortlicher oder Auftragsverarbeiter vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der ihrem Anteil an der Verantwortung für den Schaden entspricht.

4.6. BEZIEHUNG ZWISCHEN GEMEINSAM VERANTWORTLICHEN, DIE MITGLIEDER DER HERMES-GRUPPE SIND

Legen zwei oder mehr Verantwortliche innerhalb der HERMES-GRUPPE gemeinsam die Zwecke und Mittel der Verarbeitung fest, so sind sie gemeinsam Verantwortliche und verpflichten sich:

1. die Verarbeitungsvorgänge, die von jedem gemeinsam Verantwortlichen bei der Verarbeitung der betroffenen personenbezogenen Daten durchgeführt werden, eindeutig zu beschreiben und zu dokumentieren;

2. die Verarbeitung personenbezogener Daten in Übereinstimmung mit den DSGVO-Anforderungen und wie im Verzeichnis der Verarbeitungstätigkeiten und anderen Dokumenten im Zusammenhang mit der Verarbeitung personenbezogener Daten (wie zum Beispiel der Datenschutz-Folgenabschätzung) dargestellt, umzusetzen;

3. sich gegenseitig zu informieren, bevor Änderungen an der Verarbeitung personenbezogener Daten umgesetzt werden, um die Auswirkungen dieser Änderung auf die Einhaltung der Anforderungen für die Verarbeitung personenbezogener Daten zu analysieren und die Maßnahmen und Bedingungen der Umsetzung dieser Änderung (z. B. Änderung der Informationsmitteilung) zu vereinbaren, wo dies erforderlich ist;

4. den betroffenen Personen auf Anfrage den Kern dieser Vereinbarung zu vermitteln und sich auf die Mittel zu einigen, die für diese Kommunikation verwendet werden;

5. zu entscheiden, welcher gemeinsam Verantwortliche für die Bereitstellung der Informationsmitteilung an die betroffene Person und die Erhebung der Einwilligung (sofern erforderlich) der betroffenen Personen verantwortlich sein wird. In diesem Fall stimmen die gemeinsam Verantwortlichen zu, dass der gemeinsam Verantwortliche, der die Erhebung der Daten der betroffenen Person durchführt, diese Aufgabe übernehmen wird;

6. Im Falle eines Antrags oder einer Forderung von betroffenen Personen verpflichtet sich der gemeinsam Verantwortliche, der die Forderung erhalten hat, den anderen gemeinsam Verantwortlichen zu informieren und den Antrag im Namen des anderen gemeinsam Verantwortlichen wie in Absatz 4.4 (interner Beschwerdemechanismus) beschrieben zu handhaben sowie den anderen gemeinsam Verantwortlichen über die Antwort an die betroffene Person auf dem Laufenden zu halten. Der andere gemeinsam Verantwortliche verpflichtet sich, angemessene Hilfe und Zusammenarbeit zu leisten, um dem gemeinsam Verantwortlichen zu ermöglichen, auf Anträge oder Ansprüche von betroffenen Personen zu reagieren;

7. dass der gemeinsam Verantwortliche, der für die Erhebung der personenbezogenen Daten zuständig ist, verantwortlich ist, das Verzeichnis der Verarbeitungstätigkeiten im Auftrag aller gemeinsam Verantwortlichen zu erstellen und (falls notwendig) zu aktualisieren, und diese Unterlagen auf Anfrage an andere gemeinsam Verantwortliche zu übermitteln. Der andere gemeinsam Verantwortliche verpflichtet sich, angemessene Hilfe und Zusammenarbeit zu leisten, um die Erstellung der Unterlagen zu ermöglichen;

8. dass der gemeinsam Verantwortliche, der für die Erhebung der personenbezogenen Daten verantwortlich ist, zu bestimmen hat, ob eine Datenschutz-Folgenabschätzung erforderlich ist, und falls dies der Fall ist:
    a. den anderen gemeinsam Verantwortlichen darüber zu informieren und eine Datenschutz-Folgenabschätzung durchzuführen;
    b. den anderen gemeinsam Verantwortlichen i) über das Ergebnis der Datenschutz-Folgenabschätzung zu informieren; ii) über die geplante Aufgabenzuteilung zwischen den gemeinsam Verantwortlichen im Hinblick auf die umzusetzenden Maßnahmen zu informieren; und iii) darüber zu informieren, ob eine vorherige Konsultation mit der Aufsichtsbehörde erforderlich ist;

   Der andere gemeinsam Verantwortliche verpflichtet sich, angemessene Hilfe und Zusammenarbeit hinsichtlich der Durchführung der Datenschutz-Folgenabschätzung zu leisten und die Entscheidung/Ergebnisse der Datenschutz-Folgenabschätzung ausdrücklich zu validieren, einschließlich durch Konsultation einer Aufsichtsbehörde durch die gemeinsam Verantwortlichen;

9. dass der gemeinsam Verantwortliche, der für die Erhebung der personenbezogenen Daten zuständig ist, dafür verantwortlich ist, eine Konformitätsbewertung der Verarbeitung personenbezogener Daten durchzuführen (wo eine Datenschutz-Folgenabschätzung nicht erforderlich ist), und den anderen gemeinsam Verantwortlichen i) über das Ergebnis der Konformitätsbewertung; und ii) über die geplante Aufgabenzuteilung zwischen den einzelnen gemeinsam Verantwortlichen im Hinblick auf die umzusetzenden Maßnahmen zu informieren. Der andere gemeinsam Verantwortliche verpflichtet sich, angemessene Unterstützung und Zusammenarbeit bei der Durchführung der Konformitätsbewertung zu leisten und die Entscheidung/Ergebnisse in Bezug auf die Konformitätsbewertung des Datenschutzes einschließlich der anzuwendenden Speicherfristen explizit zu validieren;

10. die Sicherheit der Verarbeitung personenbezogener Daten zu wahren und Verletzungen des Schutzes personenbezogener Daten, wie in Absatz 4.5.1 vorgesehen, zu verhindern;

11. dass der gemeinsam Verantwortliche, dessen Informationssystem Opfer der Verletzung des Schutzes personenbezogener Daten geworden ist („die betroffene Partei"), den anderen gemeinsam Verantwortlichen informieren und sich verpflichten muss, Absatz 5.4.1 (z. B. Benachrichtigung des zuständigen Datenschutzbeauftragten usw.) zu befolgen. Die gemeinsam Verantwortlichen verpflichten sich, den Inhalt der Benachrichtigung, die an die Aufsichtsbehörde und die betroffenen Personen gesendet werden, innerhalb einer mit den DSGVO-Anforderungen kompatiblen Frist gemeinsam zu vereinbaren. Im Fall, dass die Verletzung des Schutzes personenbezogener Daten im Informationssystem eines Auftragsverarbeiters (innerhalb oder außerhalb der HERMES-GRUPPE) stattfindet, vereinbaren die Parteien, dass der gemeinsam Verantwortliche, der diesen Auftragsverarbeiter beauftragt hat, mit der Handhabung der Verletzung des Schutzes personenbezogener Daten beauftragt wird;

12. im Falle von Unteraufträgen innerhalb der HERMES-GRUPPE Artikel 4.5.2 zu befolgen. In diesem Fall müsste der gemeinsam Verantwortliche auch den anderen gemeinsam Verantwortlichen informieren;

13. im Fall von Übertragungen an Auftragsverarbeiter und Verantwortliche außerhalb der HERMES-GRUPPE Artikel 4.7 zu befolgen. In diesem Fall müsste der gemeinsam Verantwortliche die vorherige schriftliche Einwilligung der anderen Partei einholen. Im Falle einer Unterbeauftragung außerhalb der HERMES-GRUPPE ist der gemeinsam Verantwortliche, der den Auftragsverarbeiter beauftragt, außerdem für die Verhandlung der schriftlichen Vereinbarung mit dem Auftragsverarbeiter oder Verantwortlichen verantwortlich, der im Auftrag aller gemeinsam Verantwortlichen abgeschlossen wird (für weitere Einzelheiten siehe auch Absatz 4.7);

14. ihre jeweiligen Verpflichtungen im Zusammenhang mit der Verarbeitung personenbezogener Daten, wie in diesem Absatz beschrieben, zu dokumentieren und dem anderen gemeinsam Verantwortlichen auf Anfrage zur Verfügung zu stellen und die Informationen und anderen Dokumente, die erforderlich sind, um die Einhaltung der Verpflichtungen zu demonstrieren, auf Anfrage innerhalb einer angemessenen Frist zur Verfügung zu stellen;

15. vom anderen gemeinsam Verantwortlichen geprüft zu werden, um zu bestätigen, ob der andere gemeinsam Verantwortliche seine Verpflichtungen erfüllt;

16. Die gemeinsam Verantwortlichen sind gemeinsam für Schäden verantwortlich, die durch die Verarbeitung verursacht werden, und jeder gemeinsam Verantwortliche haftet für die gesamten Schäden, um eine wirksame Entschädigung der betroffenen Person zu gewährleisten. Wenn ein gemeinsam Verantwortlicher vollständigen Schadenersatz für die Schäden gezahlt hat, ist der gemeinsam Verantwortliche berechtigt, vom anderen gemeinsam Verantwortlichen, der an der gleichen Verarbeitung beteiligt ist, den Teil des Schadenersatzes, der seinem Teil der Verantwortung für den Schaden entspricht, zurückzufordern.

4.7. BESCHRÄNKUNGEN BEI DER ÜBERTRAGUNG UND WEITERLEITUNG AN EXTERNE AUFTRAGSVERARBEITER UND VERANTWORTLICHE

Wenn ein lokaler Datenverantwortlicher verlangt, dass ein Unternehmen, das nicht Teil der HERMES-GRUPPE ist, die Verarbeitung personenbezogener Daten als Auftragsverarbeiter oder Verantwortlicher durchführt (ein externer Auftragsverarbeiter oder ein externer Verantwortlicher), müssen folgende Sicherheitsmaßnahmen eingehalten werden:

1. **Externe Auftragsverarbeiter im EWR oder in einem Land, das von der EU-Kommission als ein Land mit angemessenem Schutzniveau anerkannt wird,** werden mit einer schriftlichen Vereinbarung gebunden, die festlegt, dass der Auftragsverarbeiter nur auf Anweisung des lokalen Datenverantwortlichen handelt und für die Umsetzung der angemessenen Sicherheits- und Vertraulichkeitsmaßnahmen verantwortlich ist (siehe Absatz 5.4.). Lokale CRM-Manager können in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro Vorlagen der entsprechenden Klauseln an einen lokalen Datenverantwortlichen innerhalb der Gruppe übermitteln.

2. **Bei jeglicher Übermittlung personenbezogener Daten an externe Datenverantwortliche außerhalb des EWR** in ein Land, das von der EU-Kommission nicht als ein Land mit angemessenem Schutzniveau anerkannt wird, müssen die europäischen Vorschriften für grenzüberschreitende Datenflüsse (Artikel 46 und 49 der DSGVO) eingehalten werden. Dies geschieht beispielsweise durch Verwendung der von der EU-Kommission genehmigten EU-Standardvertragsklauseln, der von einer Aufsichtsbehörde verabschiedeten und von der EU-Kommission genehmigten Standard-Datenschutzklauseln, eines genehmigten Verhaltenskodex, eines genehmigten Zertifizierungsmechanismus, Vertragsklauseln zwischen dem Unternehmen der HERMES-GRUPPE und dem externen Verantwortlichen, der der Genehmigung der zuständigen Aufsichtsbehörde oder Ausnahmeregelungen für bestimmte Situationen unterliegt. Darüber hinaus muss für die Beziehung zwischen den gemeinsam Verantwortlichen eine schriftliche Vereinbarung mit allen externen gemeinsam Verantwortlichen (innerhalb oder außerhalb des EWR) geschlossen werden, die festlegt, dass sie ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Verpflichtungen aus der DSGVO in transparenter Weise festlegen müssen. Dies betrifft insbesondere Verpflichtungen in Bezug auf die Ausübung der Rechte der betroffenen Person (siehe Absatz 4.2) und ihre jeweiligen Pflichten zur Bereitstellung der Informationen für diese betroffene Person durch eine Vereinbarung zwischen ihnen, es sei denn die jeweiligen Verantwortlichkeiten der Datenverantwortlichen werden nach dem Recht der Europäischen Union oder der Mitgliedstaaten, denen die Datenverantwortlichen unterliegen, festgelegt. Datenschutzkontakte (z. B. lokale CRM-Manager) und zuständige Datenschutzbeauftragte können in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro Vorlagen der entsprechenden Klauseln an einen lokalen Datenverantwortlichen innerhalb der HERMES-Gruppe übermitteln.

3. **Jegliche Übertragung personenbezogener Daten an externe Auftragsverarbeiter, die sich nicht im EWR befinden,** in ein Land, das von der EU-Kommission nicht als ein Land mit angemessenem Schutzniveau anerkannt wird, muss zusätzlich zu den Regeln der grenzüberschreitenden Datenflüsse (Artikel 46 und 49 der DSGVO) (siehe Klauseln 1 und 2 oben) den Regeln für Auftragsverarbeiter entsprechen (Artikel 28 und 49 der DSGVO).

4.8. SCHULUNGSPROGRAMME

Jeder Mitarbeiter der HERMES-GRUPPE, der personenbezogene Daten im Zusammenhang mit Kunden erhebt, verarbeitet oder Zugriff auf personenbezogene Daten hat, wird geschult, um seine praktischen Fähigkeiten und Kenntnisse in Bezug auf Datenschutzprobleme, vor allem die BCRs, zu verbessern.

1. Die BCRs und alle dazugehörigen Richtlinien, Verfahren oder Bestimmungen werden ins betriebliche Intranet der HERMES-GRUPPE hochgeladen und sind dauerhaft für jeden Mitarbeiter zugänglich.
2. Der Zugang zu den BCRs und allen dazugehörigen Richtlinien, Verfahren oder Bestimmungen wird jedem neuen Mitarbeiter der HERMES-GRUPPE gewährt. Interne Mitteilungen werden auch innerhalb der Gruppe übertragen, um das Bewusstsein für die BCRs zu schärfen.
3. Neue Mitarbeiter, die personenbezogene Daten erheben, verarbeiten oder Zugriff auf personenbezogene Daten haben, müssen ein Datenschutz-Schulungsprogramm absolvieren. Darüber hinaus müssen alle Mitarbeiter, die personenbezogene Daten erheben, verarbeiten oder Zugriff auf personenbezogene Daten haben, regelmäßig an einem solchen Programm teilnehmen. [Alle Mitarbeiter müssen nach Abschluss der Schulung eine Wissensprüfung (Zertifizierung) bestehen, um ihr Wissen und ihre Fähigkeiten in Bezug auf Datenschutzfragen zu bestätigen].
4. Auf lokaler Ebene steht es allen Datenverantwortlichen und/oder lokalen CRM-Managern frei, die oben beschriebenen Datenschutz-Schulungsprogramme durch die Ergänzung eventuell geeigneten Schulungsmaterials zu verbessern.
5. Datenschutz-Schulungsprogramme werden von erfahrenen Mitgliedern der HERMES-GRUPPE in Absprache mit dem lokalen Datenverantwortlichen, dem lokalen CRM-Manager, dem globalen CRM-Manager und dem globalen Datenschutzbüro koordiniert, überprüft und genehmigt. Verfahren im Zusammenhang mit Datenschutz-Schulungsprogrammen werden regelmäßig geprüft (siehe Absatz 5.8).

4.9. PRÜFUNGSPROGRAMM

Datenschutzprüfungen müssen regelmäßig (vorbehaltlich strengerer lokaler Gesetze mindestens alle drei Jahre) durch interne oder externe anerkannte Prüfungsteams durchgeführt werden, um sicherzustellen, dass die BCRs und alle dazugehörigen Richtlinien, Verfahren oder Bestimmungen aktualisiert und angewendet werden.

1. Die Datenschutzprüfungen müssen alle Aspekte der BCRs und alle dazugehörigen Richtlinien, Verfahren oder Bestimmungen abdecken, einschließlich Methoden zur Sicherstellung, dass Korrekturmaßnahmen stattfinden. Der Umfang der jeweiligen Prüfung kann jedoch auf begrenzte Aspekte der BCRs und/oder die damit verbundenen Richtlinien, Verfahren oder Bestimmungen fokussiert werden, einschließlich Methoden zur Sicherstellung, dass Korrekturmaßnahmen stattfinden.

2. Datenschutzprüfungen werden direkt durch die Compliance-Abteilung oder auf spezifische Anfrage des Hauptverantwortlichen, eines lokalen Datenverantwortlichen, eines lokalen CRM-Managers, des globalen CRM-Managers oder des globalen Datenschutzbüros festgelegt. Diejenigen, die für eine Prüfung verantwortlich sind, lassen bei der Ausübung ihrer Pflichten immer ein angemessenes Maß an Unabhängigkeit walten.

3. Die Ergebnisse aller Prüfungen werden dem Hauptverantwortlichen (insbesondere des Vorstands des höchsten Mutterunternehmens) und dem lokalen Datenverantwortlichen und/oder dem lokalen CRM-Manager und/oder dem globalen CRM-Manager und/oder dem globalen Datenschutzbüro mitgeteilt.

4. Die zuständigen Aufsichtsbehörden erhalten auf Anfrage eine Kopie dieser Prüfung. Jeder lokale Datenverantwortliche muss von einer Aufsichtsbehörde geprüft werden und bei jedem Problem im Zusammenhang mit den BCRs den Rat einer Aufsichtsbehörde befolgen.

5. Wie in Abschnitt 3 von Absatz 6.1 vorgesehen, erstatten lokale CRM-Manager in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro dem Hauptverantwortlichen jedes Jahr über alle Handlungen und Maßnahmen, die im Hinblick auf Datenschutzprobleme ergriffen werden (Schulungsprogramme, Status der erfolgenden Verarbeitung personenbezogener Daten, Handhabung von Beschwerden, usw.), Bericht. Darüber hinaus muss jeder lokale CRM-Manager alle notwendigen Schritte ergreifen, um sicherzustellen, dass lokale Datenverantwortliche die Bestimmungen der BCRs einhalten. Zu diesem Zweck wird eine „BCR-Compliance-Checkliste“ auf lokaler Ebene verwendet, um Compliance-Prüfungen durchzuführen.

6. Der globale CRM-Manager und das globale Datenschutzbüro müssen dem Hauptverantwortlichen auch regelmäßig über die Umsetzung der BCRs bei jedem lokalen Datenverantwortlichen Bericht erstatten.

7. Basierend auf den Ergebnissen der Prüfung und den oben erwähnten Berichten, wird/werden der Hauptverantwortliche (insbesondere des Vorstands des höchsten Mutterunternehmens) und/oder der globale CRM-Manager und/oder das globale Datenschutzbüro alle angemessenen rechtlichen, technischen oder organisatorischen Maßnahmen zur Verbesserung der Datenschutzverwaltung innerhalb der Gruppe sowohl auf globaler als auch auf lokaler Ebene festlegen.

5. DIE BCRs SIND BINDEND

5.1. DIE BCRs SIND INTERN BINDEND

Die vorliegenden BCRs binden alle Unternehmen der HERMES-GRUPPE, die die gruppeninterne BCR-Vereinbarung (Anhang 5) unterzeichnet und ihre Annahme der BCRs ausgedrückt haben.

Jedes Unternehmen der HERMES-GRUPPE, das das BCR-Vertragsformular unterzeichnet, ist für die Durchführung und Beaufsichtigung der Umsetzung dieser BCRs verantwortlich, einschließlich dafür, zu sorgen, dass die BCRs von den Mitarbeitern, die gemäß dieser dazu verpflichtet sind, eingehalten werden.

Gemäß geltenden lokalen Arbeitsgesetzen werden die BCRs für Mitarbeiter entweder über Arbeitsverträge, über kollektive Vereinbarungen oder durch entsprechende Unternehmensrichtlinien, in denen die BCRs aufgenommen wurden, verbindlich gemacht. Auch andere Mittel können genutzt werden, solange die Gruppe richtig erklären kann, wie die BCRs für die besagten Mitarbeiter verbindlich gemacht werden.

5.2. COMPLIANCE UND ÜBERWACHUNG DER COMPLIANCE

Die HERMES-GRUPPE hat ein Datenschutznetzwerk eingerichtet, das aus Datenschutzbeauftragten (wenn gemäß Artikel 37 gesetzlich vorgeschrieben) und/oder Datenschutzkontakten besteht, die auf globaler und lokaler Ebene zuständig sind.

Auf lokaler Ebene sind jeder zuständige Datenschutzbeauftragte (Data Protection Officer, DPO) und lokale CRM-Manager für die Umsetzung der BCRs verantwortlich. Daher gilt:

1. Der zuständige DPO und der lokale CRM-Manager haben die lokalen Datenverantwortlichen und die Mitarbeiter, die die Verarbeitung als eine ihrer Pflichten durchführen, zu informieren und zu beraten;

2. Jedes Unternehmen der HERMES-GRUPPE muss jeden notwendigen Schritt unternehmen, um sicherzustellen, dass lokale Datenverantwortliche die Bestimmungen der BCRs einhalten. Zu diesem Zweck wird eine „BCR-Compliance-Checkliste“ auf lokaler Ebene verwendet, um Compliance-Prüfungen durchzuführen. Datenschutzprüfungen, die durch die Compliance-Abteilung, den globalen CRM-Manager oder das globale Datenschutzbüro festgelegt werden, können sich darauf beziehen, wie diese Compliance-Prüfungen auf lokaler Ebene erfolgen.

3. Der DPO und der lokale CRM-Manager müssen in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro den lokalen Datenverantwortlichen und betroffenen Personen immer zur Verfügung stehen, um Hilfe hinsichtlich eines Datenschutzproblems zu leisten, insbesondere in Bezug auf die BCRs.

4. Der DPO und der lokale CRM-Manager stellen in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro für die Durchführung von Datenschutz-Folgenabschätzung und die Überwachung der entsprechenden Leistung gegebenenfalls Rat bereit.

5. Der DPO und die lokalen CRM-Manager erstatten in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro dem Hauptverantwortlichen jedes Jahr über alle Handlungen und Maßnahmen Bericht, die im Hinblick auf Datenschutzprobleme ergriffen werden (Schulungsprogramme, Status der umgesetzten Verarbeitung personenbezogener Daten, Handhabung von Beschwerden, usw.), insbesondere zur Umsetzung der BCRs.

6. Jeder lokale Datenverantwortliche, DPO und lokale CRM-Manager erstatten regelmäßig dem globalen CRM-Manager und dem globalen Datenschutzbüro über die Beschwerden Bericht, die auf lokaler Ebene abgewickelt werden, mit Fokus darauf, Korrekturmaßnahmen zu ergreifen und die in der Gruppe umgesetzten Richtlinien zu verbessern, wenn die Beschwerden in Bezug auf Datenschutz eine „Lücke“ enthüllt haben.

7. Der DPO und die lokalen CRM-Manager können in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro jedem lokalen Datenverantwortlichen innerhalb der Gruppe im Zusammenhang mit einem Datenschutzproblem entsprechende Vorlagen (d. h. Informationsmitteilung, Klauseln usw.) übermitteln.

8. Der DPO und die lokalen CRM-Manager kooperieren in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro mit den Aufsichtsbehörden und fungieren bei Problemen in Bezug auf die Verarbeitung für die Aufsichtsbehörde als Ansprechpartner.

Darüber hinaus müssen in Bezug auf die Überwachung der Compliance bestimmte Maßnahmen ergriffen werden, um die richtige Umsetzung der BCRs sicherzustellen:

1. Der globale CRM-Manager und das globale Datenschutzbüro müssen den Hauptverantwortlichen regelmäßig über die Umsetzung der BCRs bei jedem lokalen Datenverantwortlichen und jedem Auftragsverarbeiter, der Mitglied der HERMES-GRUPPE ist, informieren.

2. Datenschutzprüfungen müssen direkt durch die Compliance-Abteilung oder auf spezifische Anforderung eines lokalen Datenverantwortlichen, eines DPO, eines lokalen CRM-Managers, des globalen CRM-Managers oder des globalen Datenschutzbüros festgelegt werden. Die Ergebnisse aller Prüfungen oder Berichte werden dem Hauptverantwortlichen (vor allem des Vorstands des höchsten Mutterunternehmens) und dem lokalen Datenverantwortlichen und/oder dem DPO und/oder dem lokalen CRM-Manager und/oder dem globalen CRM-Manager und/oder dem globalen Datenschutzbüro mitgeteilt.

3. Basierend auf den Ergebnissen der Prüfung und den oben erwähnten Berichten entscheiden der Hauptverantwortliche (insbesondere der Geschäftsleitung des Hauptverantwortlichen), der globale CRM-Manager, das globale Datenschutzbüro, ein lokaler Datenverantwortlicher oder ein DPO oder ein lokaler CRM-Manager über die entsprechenden Maßnahmen, um das Datenschutzmanagement innerhalb der Gruppe zu verbessern, sowohl auf globaler als auch auf lokaler Ebene.

4. Wenn ein Verstoß gegen die BCRs festgestellt wird, können jegliche (rechtliche, technische oder organisatorische) Korrekturmaßnahmen sowie angemessene Sanktionen (gegen den lokalen Datenverantwortlichen oder, je nach lokalem Arbeitsrecht, einen lokalen Mitarbeiter), auf Initiative des Hauptverantwortlichen, des globalen CRM-Managers, des globalen Datenschutzbüros, des lokalen Datenverantwortlichen oder eines DPO oder eines lokalen CRM-Managers durchgeführt werden.

5. Datenschutz-Schulungsprogramme werden von erfahrenen Mitgliedern der HERMES-GRUPPE in Abstimmung mit dem globalen CRM-Manager, dem globalen Datenschutzbüro, dem DPO und den lokalen CRM-Managern überprüft und genehmigt. Verfahren im Zusammenhang mit Datenschutz-Schulungsprogrammen werden regelmäßig geprüft (siehe Absatz 4.9).

6. Der globale CRM-Manager, das globale Datenschutzbüro und der DPO arbeiten mit der leitenden Aufsichtsbehörde gemäß Artikel 56 der DSGVO zusammen.

5.3. DRITTBEGÜNSTIGTENRECHTE

1. Eine betroffene Person, die behauptet, als direkte Folge eines Verstoßes gegen die Bestimmungen der nachstehend aufgeführten BCRs und/oder Anhang 2 dieser BCRs einen Schaden erlitten zu haben, und die entweder mit der Lösung ihrer Beschwerde, wie in Absatz 4.4 beschrieben, nicht zufrieden ist oder den Wunsch hat, den internen Beschwerdemechanismus zu umgehen und ihre Beschwerde direkt bei der zuständigen Aufsichtsbehörde einzureichen, kann versuchen, ihre Rechte als Drittbegünstigte vor der zuständigen Aufsichtsbehörde oder vor den Gerichten gemäß den nachstehend aufgeführten Grundsätzen und Bedingungen durchzusetzen. Das Verfahren zur Beschwerdebearbeitung untermauert die Fähigkeit der betroffenen Person, eine Datenschutzbeschwerde intern einzureichen. Die betroffene Person ist jedoch berechtigt, wie durch lokale Gesetze vorgesehen, eine Beschwerde direkt bei der Aufsichtsbehörde oder den Gerichten einzureichen.

2. Eine betroffene Person hat das Recht, als Drittbegünstigte die Bestimmungen der BCRs in Bezug auf folgende Aspekte durchzusetzen:

- Zweckbegrenzung (siehe Absatz 2.2 und Anhang 2)
- Datenqualität und Datenminimierung (siehe Absatz 2.2 und Anhang 2)
- Grundsätze der Rechtmäßigkeit der Verarbeitung personenbezogener Daten und besonderer Datenkategorien (siehe Absatz 2.2 und Anhang 2)
- Grundsätze der Fairness und Transparenz, Recht auf Informationen und einfachen Zugriff auf BCRs (siehe Absätze 2.2 und .1 und Anhang 2)
- Recht auf Zugriff, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und Recht auf Datenübertragbarkeit (siehe Absatz .2)
- Rechte im Falle einer automatisierten Entscheidung im Einzelfall (einschließlich Profiling) (siehe Absatz .3)
- Grundsätze der Sicherheit und Vertraulichkeit (siehe Absatz 4.5)
- Beschränkungen bei Weiterleitung außerhalb der Unternehmensgruppe (siehe Absatz 4.7.)
- Nationale Gesetzgebung, die die Einhaltung der BCRs verhindert (siehe Absatz 6.2.)
- Recht auf Beschwerde über den internen Beschwerdemechanismus (siehe Absatz 4.4.)
- Verpflichtung zur Kooperation mit Aufsichtsbehörden (siehe Absatz 5.6)
- Haftung und Zuständigkeit (siehe Absätze 4.4. und 5.4)

In der Regel hat jede betroffene Person das Recht, ihren Fall, je nach Zweckmäßigkeit, entweder an die zuständigen Aufsichtsbehörden (sofern die DSGVO anwendbar ist, in dem EU-Mitgliedstaat ihres gewöhnlichen Aufenthalts, am Arbeitsort oder Ort der mutmaßlichen Verletzung) weiterzuleiten oder vor einem Gericht des lokalen Datenexporteurs oder des lokalen Datenimporteurs (sofern die DSGVO anwendbar ist, vor dem Gericht des EU-Mitgliedstaats, in dem der lokale Datenverantwortliche oder -auftragsverarbeiter eine Niederlassung hat oder wo die betroffene Person ihren gewöhnlichen Aufenthalt hat) einzureichen.

3. Gemäß den einschlägigen Bestimmungen in Absatz 4.3.1 ist jede betroffene Person, die Schäden erlitten hat, berechtigt, eine Entschädigung (z. B. gerichtliche Abhilfe) zu erhalten, deren Höhe vom zuständigen Gericht oder der Aufsichtsbehörde bestimmt oder ggf. gemäß dem internen Beschwerdemechanismus festgelegt wird.

4. Die BCRs werden jeder betroffenen Person unter den in Absatz 4.1 beschriebenen Bedingungen stets zur Verfügung stehen.

5. Die an die BCRs gebundenen Unternehmen der HERMES-GRUPPE müssen sich an eine Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde halten (sofern dieses Gericht ein Gericht des EU-Mitgliedstaats ist, in dem der lokale Datenverantwortliche oder -auftragsverarbeiter eine Niederlassung hat oder in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat oder eine solche Behörde, die sich im EU-Mitgliedstaat des gewöhnlichen Aufenthalts, des Arbeitsortes der betroffenen Person oder des Ortes der mutmaßlichen Verletzung befindet), die endgültig ist und gegen die kein weiterer Rechtsbehelf möglich ist.

5.4. HAFTUNG

Jedes Unternehmen der HERMES-GRUPPE innerhalb der EU, das gegen die BCRs verstößt, und betroffenen Personen Schäden verursacht, ist haftbar und muss die notwendigen Abhilfemaßnahmen ergreifen, sofern die betreffende HERMES-GRUPPE nicht nachweisen kann, dass diese Schäden ihr und ihren Anbietern wegen einer Verletzung der BCRs nicht zugeschrieben werden können.

HERMES INTERNATIONAL übernimmt die Verantwortung dafür und stimmt zu, die notwendigen Maßnahmen zu ergreifen, um die Handlungen anderer Unternehmen der HERMES-GRUPPE außerhalb der EU zu berichtigen und Schadenersatz für wesentliche oder unwesentliche Schäden zu zahlen, die sich aus Verletzungen der BCRs durch solche Unternehmen der HERMES-GRUPPE ergeben, es sei denn, HERMES INTERNATIONAL kann nachweisen, dass diese Schäden einem Unternehmen der HERMES-GRUPPE außerhalb der EU oder ihren Anbietern nicht zugeschrieben werden können.

Wenn ein Unternehmen der HERMES-GRUPPE außerhalb der EU gegen die BCRs verstößt, sind die Gerichte und anderen zuständigen Behörden in der EU so zuständig und haben die betroffenen Personen so Anspruch auf Rechte und Rechtsbehelfe gegen HERMES INTERNATIONAL, als ob die Verletzung durch ein Unternehmen der HERMES-GRUPPE innerhalb der EU verursacht worden wäre.

HERMES INTERNATIONAL behält sich das Recht vor, gegen Unternehmen der HERMES-GRUPPE, die sich außerhalb der EU befinden und gegen die BCRs verstoßen, Rechtsmittel zu ersuchen.

Alle Unternehmen der HERMES-GRUPPE haben ausreichende finanzielle Ressourcen zur Deckung von Schadenersatz für eine Verletzung der BCRs zur Verfügung. Die Haftung zwischen den Parteien ist auf tatsächliche Schäden beschränkt. Indirekte (d. h. Folgeschäden wie Rufschädigungen) oder Strafschadensersatz (d. h. Schadensersatz, der dazu vorgesehen ist, eine Partei für ihr empörendes Verhalten zu bestrafen) werden ausdrücklich ausgeschlossen.

Die oben genannten Verbindlichkeiten werden nicht von Maßnahmen berührt, die die HERMES-GRUPPE gegen ihre Anbieter oder andere Dritte ergreifen kann, die möglicherweise an der Verarbeitung von Informationen beteiligt sind.

5.5. SANKTIONEN

Wird ein Verstoß gegen die BCRs entweder durch Vertreter des lokalen Datenverantwortlichen oder durch Mitarbeiter festgestellt, können auf Initiative des Hauptverantwortlichen, des globalen CRM-Managers, des globalen Datenschutzbüros, des lokalen Datenverantwortlichen, des DPO oder des lokalen CRM-Managers, geeignete Disziplinar- oder gerichtliche Maßnahmen in Übereinstimmung mit dem örtlichen Arbeitsrecht ergriffen werden.

Daher muss jeder lokale Datenverantwortliche, DPO und lokale CRM-Manager den Prüfungsergebnissen (siehe Absatz 5.8) besondere Aufmerksamkeit widmen, um Verstöße gegen Vertreter oder Mitarbeiter festzustellen, insbesondere im Falle der Nichteinhaltung der Datenschutzgrundsätze und der geltenden Bestimmungen, Richtlinien und Verfahren im Zusammenhang mit der Umsetzung der BCRs.

5.6. GEGENSEITIGE UNTERSTÜTZUNG UND ZUSAMMENARBEIT MIT AUFSICHTSBEHÖRDEN

Alle Mitglieder der HERMES-GRUPPE, die an die BCRs gebunden sind, verpflichten sich zu einer vollständigen Zusammenarbeit mit den zuständigen EWR-Aufsichtsbehörden. Daher gilt:

- Die zuständigen Aufsichtsbehörden erhalten auf Anfrage innerhalb einer angemessenen Frist eine aktualisierte Kopie der BCRs oder aller dazugehörigen Verfahren, Richtlinien oder Bestimmungen.
- Der lokale Datenverantwortliche antwortet innerhalb einer angemessenen Frist auf jede Anfrage, die von einer zuständigen Aufsichtsbehörde gestellt wird, in Bezug auf ihre Anforderungen bezüglich der Auslegung und Anwendung der BCRs.
- Der lokale Datenverantwortliche muss jede relevante Empfehlung oder Beratung von einer zuständigen Aufsichtsbehörde bezüglich der Umsetzung der BCRs in die Tat umsetzen.
- Die an die BCRs gebundenen Unternehmen der HERMES-GRUPPE verpflichten sich, Prüfungen von den zuständigen EWR-Aufsichtsbehörden anzunehmen.

- Der lokale Datenverantwortliche hält sich im Zusammenhang mit der Umsetzung der BCRs an Entscheidungen der zuständigen Aufsichtsbehörden, gegen die vor den zuständigen Gerichten kein weiterer Rechtsbehelf möglich ist.
- Der globale CRM-Manager sowie das globale Datenschutzbüro und der DPO stehen den zuständigen Aufsichtsbehörden für alle Fragen im Zusammenhang mit der Umsetzung der BCRs zur Verfügung.

Darüber hinaus kooperieren und unterstützen Mitglieder der HERMES-GRUPPE sich gegenseitig, um Anfragen oder Beschwerden von einer Person (siehe Absatz .4) oder Anfragen durch die Aufsichtsbehörden zu bearbeiten.

6. SCHLUSSBESTIMMUNGEN

6.1. BEZIEHUNG ZWISCHEN NATIONALEN GESETZEN UND DEN BCRs

Die HERMES-GRUPPE verpflichtet sich, dass entsprechende Unternehmen und Mitarbeiter der HERMES-GRUPPE die Bestimmungen der BCRs sowie der DSGVO, der EU-Richtlinie 2002/50 und der geltenden lokalen Gesetze einhalten.

Wenn die lokale Gesetzgebung ein höheres Maß an Schutz für personenbezogene Daten erfordert, hat dieses immer Vorrang gegenüber den BCRs. Im Zweifelsfall können die betroffenen Unternehmen der HERMES-GRUPPE die zuständigen Aufsichtsbehörden und/oder die leitende Aufsichtsbehörde konsultieren.

6.2. MAßNAHMEN IM FALLE NATIONALER GESETZE, DIE DIE EINHALTUNG DER BCRs VERHINDERN

Wenn ein lokaler Datenverantwortlicher Grund zu der Annahme hat, dass die für den lokalen Datenverantwortlichen geltenden Rechtsvorschriften die Erfüllung seiner Verpflichtungen aus den BCRs durch den lokalen Datenverantwortlichen verhindern und erhebliche Auswirkungen auf die von den BCRs gewährten Garantien haben, wird der lokale Datenverantwortliche den globalen CRM-Manager oder das globale Datenschutzbüro unverzüglich informieren (außer wenn dies von einer Strafverfolgungsbehörde verboten ist, z. B. strafrechtliches Verbot zur Wahrung der Vertraulichkeit einer Strafverfolgungsuntersuchung).

Bei Konflikten zwischen nationalem Recht und den Verpflichtungen in den BCRs konsultieren der DPO, der lokale CRM-Manager und der lokale Datenverantwortliche im Zweifelsfall in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro die zuständigen Aufsichtsbehörden und sind dafür verantwortlich, eine Entscheidung bezüglich des Konflikts zu treffen.

Wenn eine gesetzliche Anforderung, der ein lokaler Datenverantwortlicher in einem Drittland unterliegt, die von den BCRs gewährten Garantien erheblich beeinträchtigen kann, sollte das Problem zudem den zuständigen Aufsichtsbehörden gemeldet werden. Dies umfasst eine rechtlich bindende Anforderung zur Offenlegung der personenbezogenen Daten durch eine Strafverfolgungsbehörde oder eine staatliche Sicherheitsstelle. In einem solchen Fall sollten die zuständigen Aufsichtsbehörden unmissverständlich über die Anfrage informiert werden, einschließlich darüber, welche Informationen angefordert werden, über die ersuchende Stelle und die Rechtsgrundlage für die Offenlegung (sofern nicht anderweitig verboten, wie z. B. durch ein strafrechtliches Verbot zur Wahrung der Vertraulichkeit einer Strafverfolgungsermittlung).

Wenn in bestimmten Fällen die Aussetzung und/oder Benachrichtigung verboten ist, bemüht sich der kontaktierte lokale Datenverantwortliche nach besten Kräften, das Recht zu erhalten, dieses Verbot außer Kraft zu setzen, um so bald wie möglich so viele Informationen wie möglich zu übermitteln und nachweisen zu können, dass er dies getan hat.

Wenn der kontaktierte lokale Datenverantwortliche in den oben genannten Fällen trotz größter Bemühungen nicht in der Lage ist, die zuständigen Aufsichtsbehörden zu benachrichtigen, verpflichtet er sich, den zuständigen Aufsichtsbehörden jährlich allgemeine Informationen zu den eingegangenen Anfragen zur Verfügung zu stellen (z. B. Anzahl der Anträge auf Offenlegung, Art der angeforderten personenbezogenen Daten, Antragsteller, falls möglich usw.).

In jedem Fall darf die Übertragung personenbezogener Daten durch einen lokalen Datenverantwortlichen an eine Behörde nicht massiv, unverhältnismäßig und wahllos sein und über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist.

6.3. AKTUALISIERUNG DER BCRs

Falls beispielsweise Änderungen der Gesetze oder Verfahren der HERMES-GRUPPE vorgenommen werden, können die Bedingungen der BCRs auf Initiative des Hauptverantwortlichen in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro aktualisiert werden.

Globaler CRM-Manager

Jede Änderung der BCRs muss von der HERMES-GRUPPE unverzüglich an alle Mitglieder der HERMES-GRUPPEN-BCRs und die zuständigen Aufsichtsbehörden über die leitende Aufsichtsbehörde gemeldet werden.

Darüber hinaus können Aktualisierungen der BCRs oder der Liste der Mitglieder der HERMES-GRUPPE ohne erneute Beantragung der Bestätigung vorgenommen werden, wenn die HERMES-GRUPPE sich zu Folgendem verpflichtet:

- Der globale CRM-Manager und das globale Datenschutzbüro führen eine aktualisierte Liste der Mitglieder der HERMES-GRUPPE und dokumentieren alle Aktualisierungen der Regeln;
- Die HERMES-GRUPPE stellt die notwendigen Informationen über alle Aktualisierungen der Regeln an die betroffenen Personen und anderen relevanten Datenschutzbehörden auf Anfrage zur Verfügung.
- Eine Übertragung an ein neues Unternehmen der HERMES-GRUPPE darf erst vorgenommen werden, wenn dieses neue Unternehmen effektiv an die BCRs gebunden ist und die Einhaltung von Vorschriften gewährleistet;
- Änderungen an den BCRs oder der Liste der Mitglieder der HERMES-GRUPPE werden einmal jährlich der leitenden Aufsichtsbehörde gemeldet;
- Alle Änderungen, die das von den BCRs gebotene Schutzniveau beeinträchtigen oder die BCRs erheblich beeinflussen (d. h. Änderungen am bindenden Charakter), werden den zuständigen Aufsichtsbehörden über die leitende Aufsichtsbehörde mitgeteilt.

6.4. MAßGEBLICHES RECHT/ZUSTÄNDIGKEIT/KÜNDIGUNG/AUSLEGUNG VON BEDINGUNGEN

Die BCRs werden vom Hauptverantwortlichen in Abstimmung mit dem globalen CRM-Manager und dem globalen Datenschutzbüro übernommen.

Die BCRs werden an dem Datum wirksam, an dem jedes Unternehmen der HERMES-GRUPPE diese BCR-Vereinbarung unterzeichnet hat und als Folge rechtlich gebunden ist.

Jedes Unternehmen der HERMES-GRUPPE erkennt in Bezug auf andere Unternehmen der HERMES-GRUPPE, die bereits ab dem Datum ihrer Unterzeichnung gebunden sind oder kurz davor stehen, gebunden zu werden, ab dem Datum der Unterzeichnung der BCR-Vereinbarung ohne weitere Formalitäten an, an die BCRs gebunden zu sein, dies ungeachtet des Datums und des Ortes der Unterzeichnung einer BCR-Vereinbarung durch jedes andere Unternehmen der beteiligten HERMES-GRUPPE, vorausgesetzt, dass die Bedingungen der BCRs untereinander strikt identisch sind,. Außer wenn ein Unternehmen der HERMES-GRUPPE nachweisen kann, dass die unterzeichnete BCR-Vereinbarung nicht strikt mit den von anderen Unternehmen unterzeichneten BCRs übereinstimmt, lehnt sie ausdrücklich und unwiderruflich ab, den Nachweis anzufechten, dass sie an die Bestimmungen der BCRs gebunden ist.

Für den Fall, dass ein lokaler Datenexporteur oder ein lokaler Datenimporteur einen wesentlichen oder anhaltenden Verstoß gegen die Bestimmungen der BCRs begeht, kann der Hauptverantwortliche die Übertragung personenbezogener Daten vorübergehend aussetzen, bis der Verstoß behoben ist. Sollte der Verstoß nicht rechtzeitig behoben werden, wird der Hauptverantwortliche die Initiative ergreifen, die BCR-Vereinbarung in Bezug auf diesen spezifischen lokalen Datenexporteur oder lokalen Datenimporteur zu kündigen. In diesem Fall muss der lokale Datenexporteur oder der lokale Datenimporteur alle notwendigen Schritte ergreifen, um die europäischen Regeln zu grenzüberschreitenden Datenflüssen (Artikel 46 der DSGVO) zu befolgen, beispielsweise durch die Verwendung der EU- Standardvertragsklauseln, die von der EU-Kommission genehmigt wurden.

Die Bestimmungen der BCRs unterliegen dem maßgeblichen Datenschutzrecht. Zuständig sind die Gerichte des lokalen Datenimporteurs oder des lokalen Datenexporteurs.

Im Falle von Widersprüchen zwischen den BCRs und den Anhängen ist stets der Hauptteil der BCRs maßgeblich. Im Falle von Widersprüchen zwischen den BCRs und anderen globalen oder lokalen Richtlinien, Verfahren oder Bestimmungen sind stets die BCRs maßgeblich. Im Falle von Widersprüchen oder Unstimmigkeiten werden die Bedingungen der BCRs immer entsprechend der der DSGVO und der EU-Richtlinie 2002/58 ausgelegt und geregelt.

[Von jedem Unternehmen der HERMES-GRUPPE zu unterzeichnen, das gemäß dem Vertragsformular, das in Anhang 5 festgelegt ist, an die BCRs gebunden ist]

ANHÄNGE

- Anhang 1 – Begriffsbestimmungen
- Anhang 2 – Datenschutzgrundsätze
- Anhang 3 – Liste der an die BCRs gebundenen Unternehmen der HERMES-GRUPPE
- Anhang 4 – Art und Zweck der personenbezogenen Daten, die im Rahmen der BCRs übertragen werden
- Anhang 5 – Vertragsformular

ANHANG 1: BEGRIFFSBESTIMMUNGEN

Die in den BCRs verwendeten Begriffe und Ausdrücke werden in diesem Anhang definiert, sofern diese Begriffe und Ausdrücke immer gemäß den EU-Richtlinien 95/46 und 2002/58 ausgelegt werden.

„**Aufsichtsbehörde**" bezeichnet eine unabhängige Stelle, die zuständig ist für: (i) die Überwachung der Verarbeitung personenbezogener Daten in ihrem Zuständigkeitsbereich (Landes-, Regions- oder internationale Organisation); (ii) die Beratung der zuständigen Stellen in Bezug auf gesetzliche und administrative Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten; und (iii) die Anhörung von Beschwerden der Bürger zum Schutz ihrer Datenschutzrechte.

„**Auftragsverarbeiter**" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„**Automatisierte Entscheidungen im Einzelfall**" bezeichnet eine Entscheidung, die rechtliche Auswirkungen hervorruft oder Einfluss auf eine betroffene Person hat und sich zur Evaluierung dieser Person ausschließlich auf die automatisierte Verarbeitung personenbezogener Daten stützt.

„**Besondere Kategorien personenbezogener Daten**" bezeichnet personenbezogene Daten, die direkt oder indirekt die Hautfarbe oder ethnische Herkunft, politischen Meinungen, philosophischen oder religiösen Überzeugungen, Gewerkschaftszugehörigkeit, genetischen Daten, biometrischen Daten, die zum Zwecke der eindeutigen Identifizierung einer natürlichen Person verarbeitet werden, oder Daten in Bezug auf die Gesundheit oder Sexualität von Einzelpersonen offenlegen.

„**Betroffene Person**" bezeichnet eine identifizierte oder identifizierbare Person, auf die sich spezifische personenbezogene Daten beziehen. Diese ist jemand, der direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf eine Kennung wie einen Namen, eine Kennnummer, Standortdaten, eine Online-Kennung oder einen oder mehrere Faktoren, die für die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle, oder soziale Identität dieser natürlichen Person spezifisch sind.

„Datenschutz-Grundverordnung" (oder „DSGVO") 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, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

„**Datenübertragung**" bezeichnet eine Übertragung personenbezogener Daten von einem Unternehmen an ein anderes Unternehmen. Eine Übertragung kann über jede Kommunikation, Kopie, Übertragung oder Offenlegung personenbezogener Daten über ein Netzwerk erfolgen, einschließlich durch Fernzugriff auf eine Datenbank oder Übertragung von einem Medium auf ein anderes, unabhängig von der Art des Mediums (z. B. von einer Computerfestplatte auf einen Server).

„**Dritter**" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten.

„**Einwilligung"** der betroffenen Person bezeichnet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Erklärung oder bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

„**Empfänger**" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der die Daten offengelegt werden, ob es sich um Dritte handelt oder nicht, wobei Behörden, die im Rahmen einer bestimmten Untersuchung Daten erhalten können, jedoch nicht als Empfänger gelten.

„**EWR oder Europäischer Wirtschaftsraum**" bezeichnet die Länder der Europäischen Union und Mitgliedsländer der EFTA (European Free Trade Association – Europäische Freihandelsassoziation).

„Gemeinsam Verantwortliche" bezeichnet zwei oder mehr Verantwortliche, die gemeinsam den/die Zweck(e) und Mittel der Verarbeitung festlegen.

„**Gesundheitsdaten**" bezeichnet personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

„**Globaler CRM-Manager**" bezeichnet den Senior-Level-Manager, der innerhalb der Gruppe auf globaler Ebene für das Management von Geschäftsbewusstsein und -angemessenheit in Bezug auf maßgebliches Datenschutzrecht und die Datenschutzrichtlinie, Verfahren und Richtlinien der HERMES-GRUPPE, insbesondere die BCRs, verantwortlich ist.

„**Globales Datenschutzbüro**" bezeichnet die Abteilung innerhalb des Büros des Hauptverantwortlichen, die innerhalb der Gruppe auf weltweiter Ebene für die Verwaltung des Geschäftsbewusstseins und die Einhaltung des maßgeblichen Datenschutzrechts und der Datenschutzrichtlinien, Verfahren und Bestimmungen der HERMES-GRUPPE, insbesondere der BCRs, verantwortlich ist.

„**Hauptverantwortlicher**" bezeichnet den Hauptsitz der HERMES-GRUPPE in Frankreich, der allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt und für die formelle Übernahme von BCRs verantwortlich ist, die innerhalb der HERMES-GRUPPE umgesetzt werden sollen.

„**Hermes-Gruppe**" bezeichnet HERMES INTERNATIONAL selbst und/oder ein Unternehmen der HERMES-GRUPPE, das direkt oder indirekt von HERMES INTERNATIONAL gemäß Artikel L. 233-3 des französischen Handelsgesetzbuchs verwaltet wird.

„**Leitende Aufsichtsbehörde**“ bezeichnet die französische Aufsichtsbehörde („CNIL“).

„**Lokaler CRM-Manager**“ bezeichnet einen erfahrenen leitenden Angestellten der HERMES-GRUPPE bei einem lokalen Datenverantwortlichen, der für die Verwaltung des Geschäftsbewusstseins und der -angemessenheit in Bezug auf das maßgebliche Datenschutzrecht und die Datenschutzrichtlinien, Verfahren und Bestimmungen der HERMES-GRUPPE, insbesondere die BCRs, verantwortlich ist.

„**Lokaler Datenexporteur**“ bezeichnet das Unternehmen der HERMES-GRUPPE, das sich innerhalb des EWR befindet und die personenbezogenen Daten außerhalb des EWR überträgt.

„**Lokaler Datenimporteur**“ bezeichnet das Unternehmen der HERMES-GRUPPE, das sich außerhalb des EWR befindet und zustimmt, vom Datenexporteur personenbezogene Daten für die weitere Verarbeitung zu empfangen.

„**Lokaler Datenverantwortlicher**“ bezeichnet die juristische Person der HERMES-GRUPPE, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt; wenn die Zwecke und Mittel der Verarbeitung durch nationale oder EU-Gesetze oder -Vorschriften bestimmt werden, können der Verantwortliche oder die spezifischen Kriterien für seine Nominierung durch nationale oder EU-Gesetze bestimmt werden.

„**Maßgebliches Datenschutzrecht**“ bezeichnet die Gesetze, die die grundlegenden Rechte und Freiheiten von Einzelpersonen schützen, insbesondere ihr Recht auf Datenschutz in Bezug auf die Verarbeitung personenbezogener Daten, das für einen Datenverantwortlichen in einem Land gilt, in dem die HERMES-GRUPPE und der lokale Datenexporteur ansässig sind.

„Mitarbeiter“ bezeichnet die Person oder alternativ alle Personen, die als Untergebene Aufgaben für die HERMES-GRUPPE im Austausch gegen Löhne oder Gehälter im Rahmen eines Arbeitsvertrags (sofern zutreffend oder gesetzlich vorgeschrieben) oder einer anderen ähnlichen Vereinbarung (wie eines Praktikumsvertrags) erfüllen oder in der Vergangenheit erfüllt haben. Dazu gehören auch Vorstandsmitglieder, Auszubildende, Lehrlinge, Zeitarbeitskräfte und ähnliche Personen.

Verarbeitung „**personenbezogener Daten**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person“).

„**Profiling**“ bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

„**Pseudonymisierung**“ bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, sodass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

„**Technische und organisatorische Sicherheitsmaßnahmen**“ für die Verarbeitung bezeichnet Maßnahmen zum Schutz personenbezogener Daten vor versehentlicher oder rechtswidriger Vernichtung oder versehentlichem/r Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff, insbesondere wenn die Verarbeitung die Übertragung von Daten über ein Netzwerk umfasst, und vor allen anderen rechtswidrigen Formen der Verarbeitung. **„EU-Richtlinie 2002/58“** bezeichnet Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (in ihrer jeweils gültigen Fassung).

„**Verarbeitung von personenbezogenen Daten**“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, Erfassen, Organisieren, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übertragung, Verbreiten oder eine andere Form der Bereitstellung, des Abgleichs oder der Verknüpfung, Sperrung, Löschung oder Vernichtung.

„Verletzung des Schutzes personenbezogener Daten“ bezeichnet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten beziehungsweise zum unbefugten Zugang zu diesen führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

„**Verzeichnis der Verarbeitungstätigkeiten**“ bezeichnet die Unterlagen aller in Artikel 30 der DSGVO dargelegten Informationen, die jeder einzelne Verantwortliche oder sein Vertreter und jeder Auftragsverarbeiter in Bezug auf alle Verarbeitungstätigkeiten unter seiner Verantwortung aufbewahren muss.

ANHANG 2: DATENSCHUTZGRUNDSÄTZE

Im Rahmen der BCRs muss jede Übertragung personenbezogener Daten an ein Drittland, das kein angemessenes Schutzniveau gewährleistet, stets den folgenden Datenschutzgrundsätzen entsprechen, die von der DSGVO festgelegt wurden.

FAIRNESS UND TRANSPARENZ

Die Fairness macht es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird.

Alle Informationen und Mitteilungen im Zusammenhang mit der Verarbeitung der personenbezogenen Daten der betroffenen Personen werden in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form in klarer und deutlicher Sprache bereitgestellt, insbesondere alle Informationen, die speziell an ein Kind gerichtet sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden.

Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

RECHTMÄßIGKEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN

Personenbezogene Daten dürfen nur verarbeitet werden, wenn:

- die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat;
- die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung offizieller Befugnis erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten oder einer Partei, der die Daten offengelegt werden, erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

RECHTMÄßIGKEIT DER VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

Besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, werden nur verarbeitet, wenn:

- die betroffene Person ihre ausdrückliche Einwilligung zur Verarbeitung für einen oder mehrere bestimmte Zwecke erteilt hat, außer wenn die geltenden Gesetze es verbieten;
- die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Recht der Europäischen Union oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung, die geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist;
- die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;
- die Verarbeitung auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;
- die Verarbeitung sich auf besondere Kategorien personenbezogener Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat;
- die Verarbeitung besonderer Kategorien personenbezogener Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;
- die Verarbeitung der besonderen Kategorien personenbezogener Daten zum Zwecke der Präventiv- oder Arbeitsmedizin, zur Beurteilung der Arbeitsfähigkeit des Mitarbeiters, zur medizinischen Diagnose, zur Bereitstellung von Gesundheits- oder Sozialleistungen oder zur Behandlung oder zur Verwaltung von Gesundheitsleistungen, Pflege- oder Sozialpflegesystemen und -diensten auf der Grundlage des nationalen Rechts oder gemäß einem Vertrag mit einer Fachkraft aus dem Gesundheitswesen und nach nationalem Recht oder nach Vorschriften, die von den zuständigen nationalen Stellen der Verpflichtung zum Berufsgeheimnis oder einer anderen Person unterworfen sind, die ebenfalls einer gleichwertigen Geheimhaltungspflicht unterliegen, erforderlich ist.

Andere besondere Datenkategorien (wie z. B. vor allem Daten zu strafrechtlichen Verurteilungen) unterliegen den lokalen Datenschutzanforderungen, die durch nationale Gesetze vorgesehen sind. Insbesondere darf die Verarbeitung von Daten im Zusammenhang mit Straftaten, strafrechtlichen Verurteilungen oder Sicherheitsmaßnahmen nur unter der Kontrolle einer behördlichen Stelle erfolgen oder wenn die Verarbeitung nach nationalem Recht genehmigt ist, sofern dies angemessen ist, um angemessene Schutzmaßnahmen für die Rechte und Freiheiten von betroffenen Personen zu gewährleisten.

Außerdem kann das nationale Recht näher bestimmen, unter welchen spezifischen Bedingungen eine nationale Kennnummer oder andere Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen. In diesem Fall darf die nationale Kennnummer oder das andere Kennzeichen von allgemeiner Bedeutung nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person gemäß diesem Verordnungsrecht verwendet werden.

ZWECKBEGRENZUNG

Personenbezogene Daten werden für festgelegte, ausdrückliche und legitime Zwecke erhoben und nicht auf eine Weise weiterverarbeitet, die nicht mit diesen Zwecken kompatibel ist.

Die Weiterverarbeitung von Daten für Archivierungszwecke, im öffentlichen Interesse, für wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke gilt nicht als inkompatibel, sofern angemessene Schutzmaßnahmen für die Rechte und Freiheiten der betroffenen Personen – insbesondere technische und organisatorische Maßnahmen – umgesetzt werden, um die Datenminimierung sicherzustellen.

DATENMINIMIERUNG, BEGRENZTE SPEICHERFRISTEN UND DATENQUALITÄT

Personenbezogene Daten haben dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Erhebung und/oder Verarbeitung notwendige Maß beschränkt zu sein („Datenminimierung“);

Personenbezogene Daten müssen korrekt sein und gegebenenfalls auf dem neuesten Stand gehalten werden (Richtigkeit). Es sind alle angemessenen Schritte zu unternehmen, um sicherzustellen, dass Daten, die falsch oder unvollständig sind, unter Berücksichtigung der Zwecke, für die sie erhoben oder für die sie weiterverarbeitet werden, gelöscht oder berichtigt werden.

Personenbezogene Daten werden in einer Form aufbewahrt, die es ermöglicht, betroffene Personen nicht länger zu identifizieren, als dies für die Zwecke erforderlich ist, für die die Daten erhoben oder für die sie weiterverarbeitet werden. Personenbezogene Daten können für längere Zeiträume gespeichert werden, solange sie ausschließlich zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden, sofern die entsprechenden technischen und organisatorischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person eingehalten werden (begrenzte Speicherfristen).

DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Datenschutz durch Technikgestaltung: Der lokale Datenverantwortliche muss sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst geeignete technische und organisatorische Maßnahmen (wie Pseudonymisierung) umsetzen, um die Datenschutzgrundsätze (wie Datenminimierung) auf effektive Weise umzusetzen und um die erforderlichen Sicherheitsvorkehrungen in die Verarbeitung zu integrieren.

Datenschutz durch datenschutzfreundliche Voreinstellungen: Der lokale Datenverantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

SICHERHEIT PERSONENBEZOGENER DATEN

Angemessene technische und organisatorische Maßnahmen müssen umgesetzt werden, um personenbezogene Daten vor versehentlichem/r oder unrechtmäßigem/r Vernichtung oder Verlust, Veränderung, unbefugter Offenlegung oder Zugriff und alle anderen rechtswidrigen Formen der Verarbeitung zu schützen (siehe Absatz 4.5).

WEITERLEITUNG AN ORGANISATIONEN, DIE NICHT AN BCRS GEBUNDEN SIND

Wenn personenbezogene Daten an ein Unternehmen, das nicht Teil der HERMES-GRUPPE ist, übertragen werden sollen, müssen angemessene Sicherheitsmaßnahmen umgesetzt werden (siehe Absatz 4.7).

VERANTWORTLICHKEIT

Der lokale Datenverantwortliche ist für die Einhaltung der vorliegenden Datenschutzgrundsätze verantwortlich und muss diese nachweisen können (Verantwortlichkeit).

Um die Compliance nachzuweisen, müssen BCR-Mitglieder ein Verzeichnis der Verarbeitungstätigkeiten gemäß den in Artikel 30 der DSGVO dargelegten Anforderungen führen. Gegebenenfalls muss der lokale Datenverantwortliche angemessene Datenschutzrichtlinien umsetzen.

Um die Compliance zu verbessern und wenn erforderlich, müssen Datenschutz-Folgenabschätzungen für die Verarbeitungsvorgänge durchgeführt werden, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen (Artikel 35 der DSGVO). Wenn eine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung zu einem hohen Risiko führen würde und der lokale Datenverantwortliche keine Maßnahmen zur Risikominderung ergreift, sollte die zuständige Aufsichtsbehörde vor der Verarbeitung konsultiert werden (Artikel 36 der DSGVO).

ANHANG 3: LISTE UND STANDORTE DER UNTERNEHMEN DER HERMES-GRUPPE, DIE AN DIE BCRS GEBUNDEN SIND

1. Unternehmen der HERMES-GRUPPE im EWR

HEAD CONTROLLER

France:

HEAD CONTROLLER	HERMES INTERNATIONAL
Form	Société en commandite par actions
Registered address	24, rue du Faubourg Saint-Honoré 75008 Paris (France)
TVA communautaire	FR
Legal representative	Axel DUMAS
Global CRM Manager	Bénédicte REVOL
Global Privacy Office	Legal Department - DPO
Local CRM Manager	Armelle Laurent

LOCAL DATA CONTROLLER

France:

LOCAL DATA CONTROLLER	COMPAGNIE DES ARTS DE LA TABLE ET DE L'EMAIL (LA TABLE HERMES)
Form	Société par actions simplifiée à associé unique
Registered address	Route de Piégut 24300 Nontron (France)

LOCAL DATA CONTROLLER	COMPTOIR NOUVEAU DE LA PARFUMERIE (HERMES PARFUMS)
Form	Société anonyme
Registered address	23, rue Boissy d'Anglas 75008 Paris (France)

LOCAL DATA CONTROLLER	COMPAGNIE DES CRISTALLERIES DE SAINT-LOUIS
Form	Société par actions simplifiée
Registered address	57620 Saint-Louis-lès-Bitche (France)

LOCAL DATA CONTROLLER	CREATIONS METAPHORES
Form	Société par actions simplifiée
Registered address	21, rue Cambon 75001 Paris (France)

LOCAL DATA CONTROLLER	HERMES SELLIER
Form	Société par actions simplifiée
Registered address	24, rue du Faubourg Saint-Honoré 75008 Paris

LOCAL DATA CONTROLLER	PUIFORCAT

Form	Société par actions simplifiée à associé unique
Registered address	48 AV GABRIEL 75008 PARIS

LOCAL DATA CONTROLLER	John Lobb
Form	Société par actions simplifiée
Registered address	23 RUE BOISSY D'ANGLAS 75008 PARIS

Belgium / Luxemburg:

LOCAL DATA CONTROLLER	HERMES BENELUX NORDICS
Form	Société anonyme de droit belge
Registered address	50, Boulevard de Waterloo, 1000 Bruxelles

Denmark :

LOCAL DATA CONTROLLER	HERMES DENMARK
Form	Anpartsselskab (ApS)
Registered address	c/o NJORD Law Firm, Pilestrade 58, 1112 Copenhagen K

Germany:

LOCAL DATA CONTROLLER	HERMES GmbH
Form	Société à responsabilité limitée de droit allemand
Registered address	Marstallstrasse 8, 80539 Munich

United Kingdom:

LOCAL DATA CONTROLLER	HERMES GB Ltd
Form	Société à responsabilité limitée de droit anglais
Registered address	1 Bruton Street W1J 6TL London

LOCAL DATA CONTROLLER	**JL & Co. Ltd - *(John Lobb)***
Form	Limited Liability Company
Registered address	Westminster Works, 1 Oliver Street Northampton NN2 7JL England

Spain:

LOCAL DATA CONTROLLER	HERMES IBERICA
Form	Société anonyme de droit espagnol
Registered address	Calle Ortega y Gasset 28006 Madrid

Sweden:

LOCAL DATA CONTROLLER	HERMES SWEDEN AB
Form	AB (Private Limited Company)

Registered address	NK 243, 111 77 Stockholm

Italy:

LOCAL DATA CONTROLLER	HERMES Italie SPA
Form	Société anonyme de droit italien
Registered address	Via Serbelloni 1, 20122 Milan

Greece:

LOCAL DATA CONTROLLER	HERMES GRECE
Form	Société anonyme de droit grec
Registered address	Rue Stadiou 4 et Rue Voukourestiou 1, 10564 Athènes

Czech Republic:

LOCAL DATA CONTROLLER	HERMES PRAGUE
Form	Société anonyme de droit tchèque
Registered address	Parizka 12 :120, 110000 Prague

Portugal:

LOCAL DATA CONTROLLER	HERMES INTERNATIONAL PORTUGAL
Form	Société de droit portugais
Registered address	Largo do Chiado 9, 1200-108 Lisbonne

Poland:

LOCAL DATA CONTROLLER	HERMES POLOGNE SP. Z O.O
Form	limited liability company
Registered address	ul. Krakowskie Przedmieście 13 00-071 Warszawa

2. HERMES GROUP entities located outside the EEA

Turkey:

LOCAL DATA CONTROLLER	HERMES ISTANBUL
Form	
Registered address	Abdi Ipekçi Cad N°79 Nisantasi Sisli Istanbul

Monaco:

LOCAL DATA CONTROLLER	HERMES MONTE CARLO
Form	Société Anonyme de droit monégasque

Registered address	11.13.15 avenue de Monte-Carlo 98000 Monaco (Principauté de Monaco)

Russia:

LOCAL DATA CONTROLLER	HERMES RUS
Form	SARL
Registered address	Nizhniy Kiselny Pereulok 4, 107 031 MOSCOW

Switzerland:

LOCAL DATA CONTROLLER	HERMES (SUISSE)
Form	Société Anonyme de droit Suisse
Registered address	4, rue de la Tour de l'Ile 1204 Genève

ZONE AMERIQUES

United States :

LOCAL DATA CONTROLLER	CREATIONS METAPHORES
Form	Société anonyme de droit américain
Registered address	55 east 59th Street – NYC 10022 - USA

LOCAL DATA CONTROLLER	HERMES OF PARIS Inc
Form	Société anonyme de droit américain
Registered address	55 East 59th Street – NYC 10022 - USA

Canada:

LOCAL DATA CONTROLLER	HERMES CANADA INC
Form	Société de droit canadien
Registered address	130 Bloor Street West, Toronto, Ontario M5S 1N5 (Canada)

Mexico:

LOCAL DATA CONTROLLER	BOISSY MEXICO
Form	
Registered address	Avenida Presidente Mazaryk 422, Local A Col Polanco, 11560 Mexico DF (Mexique)

Argentina:

LOCAL DATA CONTROLLER	HERMES ARGENTINA
Form	Sarl de droit argentin
Registered address	Avenida Alvear 1981 – 1129 Buenos Aires (Argentine)

Brazil:

LOCAL DATA CONTROLLER	H BRASIL COMERCIO IMPORTACAO E EXPORTACAO Ltda
Form	L.T.D.A
Registered address	Avenida Magalhaes de Castro, n°12.000 Loja 32, Piso Terreo, Jardim Panarama, CEP 05502-001, Sao Paulo, Brazil

ZONE ASIA - PACIFIC

Singapore:

LOCAL DATA CONTROLLER	HERMES MIDDLE EAST SOUTH ASIA
Form	Private Limited Company
Registered address	1 Marina Bld 2800/018989 Singapour

LOCAL DATA CONTROLLER	HERMES SOUTH EAST ASIA (HSEA)
Form	Ltd
Registered address	1 Marina Bld 2800/018989 Singapour

LOCAL DATA CONTROLLER	HERMES SINGAPORE RETAIL
Form	Private Limited Company
Registered address	1 Marina Bld #2800/018989 Singapour

LOCAL DATA CONTROLLER	BOISSY SINGAPOUR (TR Singapore)
Form	Private Limited Company
Registered address	One Marina Boulevard #28-00 Singapour 018989 (Singapour)

Hong-Kong:

LOCAL DATA CONTROLLER	HERMES ASIA PACIFIC
Form	Ltd
Registered address	25F, Chinachem Leighton Plaza, 29 Leighton Road – Causeway Bay – Hong-Kong (RPC)

LOCAL DATA CONTROLLER	HERLEE LIMITED (TR HK)
Form	Ltd
Registered address	25/F Chinachem Leighton Plaza, 29 Leighton Road, Causeway Bay, Hong Kong

China:

LOCAL DATA CONTROLLER	HERMES (CHINA) CO LTD
Form	Ltd
Registered address	Room 3010, 3011 – Westgate Mall Tower

	1038 Nanjing Xi Road, Shanghai 2000141 (Chine)

LOCAL DATA CONTROLLER	HERMES (CHINA) TRADING CO. LTD
Form	Ltd
Registered address	Building N°12, N° 211, 213, 215 et 227 Middle Huaihai Road, Shanghai PRC

LOCAL DATA CONTROLLER	SHANG-XIA
Form	A Chinese company
Registered address	233, Huaihai Middle Road, Shanghai, 200021, PRC

Thailand:

LOCAL DATA CONTROLLER	SAINT HONORE BANGKOK
Form	Ltd
Registered address	2 Sukhumvit Road, Kwaeng Klagton Khet Kiongtoey – Bangkok – Thaïlande

Malaysia:

LOCAL DATA CONTROLLER	HERMES RETAIL (MALAYSIA)
Form	Private Limited Company
Registered address	Level 16, Memara TM Asia Life, 189 Jalan Inn Razan 50400 Kuala Lumpur (Malaisie)

India:

LOCAL DATA CONTROLLER	HERMES INDIA RETAIL AND DISTRIBUTORS
Form	Private Limited Company de droit indien
Registered address	G/5 – Shopping Arcade, The Oberoi – Dr Zakir Hussain Marg. 110003 New Delhi (Inde)

Japan:

LOCAL DATA CONTROLLER	HERMES JAPON CO LTD
Form	Kabushiki Kaisha
Registered address	4-3 Ginza 5-Chome Chuo-Ku Tokyo 104-0061 (Japon)

Australia:

LOCAL DATA CONTROLLER	HERMES AUSTRALIA PTY LTD
Form	Ltd
Registered address	Level 11, 70 Castlereagh Street NSW 2000 Sydney (Australie)

Taiwan:

LOCAL DATA CONTROLLER	HERMES ASIA PACIFIC -TAIWAN
Form	Ltd
Registered address	Basement 1st Floor, n°3, Lane 39, Sec 2, Chang-Chan North Road TAIPEI

South Korea:

LOCAL DATA CONTROLLER	HERMES KOREA LIMITED
Form	Ltd
Registered address	630-26, Shinsa-Dong Gangnam-gu, 135-895 SEOUL

Guam:

LOCAL DATA CONTROLLER	Faubourg Guam Inc (TR Guam)
Form	Inc
Registered address	Suite 331, Tumon Sands Plaza, 1082 Pale San Vitores Road, Tumon, Guam 96913

Saipan:

LOCAL DATA CONTROLLER	Boissy Singapore Pte Ltd , Saipan Branch
Form	
Registered address	Suite 331, Tumon Sands Plaza, 1082 Pale San Vitores Road, Tumon, Guam 96913

ANHANG 4: ART UND ZWECK DER PERSONENBEZOGENEN DATEN, DIE IM RAHMEN DER BCRs ÜBERTRAGEN WERDEN

Zwecke	Art der übertragenen Daten	Empfänger in Drittländern
► Customer Relationship Management (CRM) d. h.: - Bereitstellung der angeforderten Produkte an Kunden und/oder Erbringung der angeforderten Dienstleistungen für sie (einschließlich Bearbeitung ihrer Zahlung); - Durchführung von Prüfungen, um Kunden zu identifizieren und ihre Identität zu bestätigen; - Versand von Marketing-Mitteilungen mit vorheriger Einwilligung des Kunden; - Erbringung von Dienstleistungen nach dem Verkauf; - Beantwortung von Anfragen, Fragen und Vorschlägen von Kunden; - Verwaltung der Ereignisse, für die Kunden registriert sind und/oder an denen sie teilgenommen haben; - Aufdeckung, Verhinderung und Bekämpfung betrügerischer oder illegaler Aktivitäten, einschließlich des Schutzes von Kundentransaktionen vor Zahlungsbetrug, um gegen Fälschungen und gegen den Weiterverkauf von Hermès-Produkten vorzugehen, die gegen die Verkaufsbedingungen von Hermès verstoßen und außerhalb des Vertriebsnetzes liegen; - Verwaltung der Lagerbestände bestimmter Arten seltener Produkte, um für eine faire Zuteilung der von uns verkauften Produkte zu sorgen; - Durchführung von statistischen Analysen, Marktforschung, Kundenzufriedenheits- und Qualitätssicherungsumfragen; - Verbesserung unserer Produkte und Leistungen; - Weiterleitung von Informationen an Aufsichtsbehörden, wenn dies nach geltendem Recht vorgeschrieben ist. - Verwaltung der allgemeinen Aufzeichnungen.	► *Identitäts- und Kontaktinformationen (Name, Nachname, Geschlecht, private Kontaktdaten, Telefonnummer, Position, Datum und Ort der Geburt, E-Mail-Adresse usw.);* ► *gekaufte Waren und/oder Dienstleistungen (einschließlich Ort des Kaufs, besonderer Anfragen, Beobachtungen über Service-/Produktpräferenzen usw.);* ► *Rechnungsdetails (Kaufmenge, Zahlungsart, Kredit-/Debitkartendetails usw.);* ► *alle Informationen, die in Bezug auf Marketingpräferenzen oder im Verlauf der Teilnahme an Umfragen oder Werbeangeboten oder im Zusammenhang mit der Anfrage eines Kunden (einschließlich Kommentaren oder anderen Mitteilungen) bereitgestellt werden.*	► *CRM-Abteilungen und Abteilungen, die für Kundenbeziehung, Einzelhandel, E-Commerce, Kommunikation, rechtliche und interne Prüfung zuständig sind.*

ANHANG 5: VERTRAGSFORMULAR

HERMES INTERNATIONAL

Binding Corporate Rules (BCRs) for intra-group Transfers of personal data to non-EEA countries

to be completed

The following entity of the HERMES group:

undertakes to comply with the provisions of the BCRs of the HERMES Group.

This undertaking will be relevant for:

the version dated to be completed

and for any updated BCRs that would have been notified by the HEAD CONTROLLER and/or the Global CRM Manager and/or the Global Privacy Office, 30 days prior the effective date of such new BCRs and according to articles 6.3 and 6.4 of the BCRs

On: _____ (date)

At: _____ (place of signature)

For
Name:
Surname:
Quality: