

## **Zusammenfassung der Binding Corporate Rules des Giesecke + Devrient Konzerns**

### **1. Zweck**

Für ein innovatives, transnationales Unternehmen, wie den Giesecke + Devrient Konzern („G+D“), ist es von großer Wichtigkeit, Informationen zu haben und diese effektiv zu nutzen, um die Unternehmensziele in allen Unternehmensbereichen erreichen zu können. Wenn es um den Zugriff auf Informationen und ihre gemeinsame Nutzung geht, spielen moderne Informations- und Kommunikationstechnologien, wie das Internet, Intranet oder E-Mails, in unserem Konzern eine immer größere Rolle. Durch sie kann G+D Geschäftsentscheidungen schnell und effektiv treffen und umsetzen – und so den steigenden Kundenerwartungen gerecht werden.

Gleichzeitig birgt der technologische Wandel in Bezug auf den Informationsaustausch gewisse Risiken, die ein verantwortungsbewusstes Unternehmen wie G+D berücksichtigen muss. Belegschaft, Auftraggeber, Kunden und mögliche zukünftige Kunden haben ein berechtigtes Interesse daran, dass die Verarbeitung und Verwendung von personenbezogenen Daten keine Datenschutzrechte der Betroffenen Person verletzt.

### **2. Geltungsbereich**

Alle beigetretenen G+D-Konzerngesellschaften fallen in den Anwendungsbereich der BCR.

### **3. Beschreibung**

Im Zuge der Verpflichtung auf ein hohes Maß an Datenschutz hat der G+D-Konzern die Binding Corporate Rules eingeführt, um Sicherheiten und Garantien für ein angemessenes Datenschutzniveau gemäß der EU-Richtlinie 95/46/EG für jede die Verarbeitung personenbezogener Daten durch oder im Auftrag von den Unternehmen des G+D-Konzerns in seiner Rolle als Verantwortlicher, sowie jede Verarbeitung durch ein G+D-Konzernmitglied in seiner Rolle als Auftragsverarbeiter und insbesondere in Hinblick auf die Übermittlung personenbezogener Daten außerhalb des EWR sicherzustellen.

### **4. Schulungsprogramm**

Der G+D-Konzern hat ein umfassendes Schulungsprogramm für alle Mitarbeiter eingeführt, die im Rahmen der Ausführung ihrer Arbeit dauerhaften oder regelmäßigen Zugriff auf personenbezogene Daten haben und/oder in die Erhebung personenbezogener Daten oder die Entwicklung von Systemen zur Verarbeitung personenbezogener Daten involviert sind, und verpflichtet sich, dieses Schulungsprogramm aufrechtzuerhalten.

### **5. Auditprogramm**

Der G+D-Konzern hat, basierend auf einem risikoorientierten Auditprogramm, ein umfassendes Programm zur Überprüfung der Einhaltung der Binding Corporate Rules eingeführt und verpflichtet sich, dieses aufrechtzuerhalten. Das Auditprogramm umfasst alle Aspekte der Binding Corporate Rules und beinhaltet Methoden, mit denen die Umsetzung von Korrekturmaßnahmen sichergestellt wird.

### **6. Maßnahmen für den Fall, dass nationale Gesetzgebung, die Einhaltung der Binding Corporate Rules verhindern**

Die Mitglieder des G+D-Konzerns unterrichten den Kunden über jede rechtsverbindliche Anfrage auf Offenlegung der personenbezogenen Daten durch eine Strafverfolgungsbehörde, soweit dies nicht

gesetzlich, wie beispielsweise durch das strafrechtliche Verbot, die Wahrung der Vertraulichkeit einer Strafverfolgungsbehörde zu beeinträchtigen, untersagt ist.

## **7. Mechanismen für die Bearbeitung von Beschwerden**

Der G+D-Konzern hat ein System für die Bearbeitung von Beschwerden eingeführt und verpflichtet sich, dieses System aufrechtzuerhalten, durch das jede betroffene Person Beschwerde darüber einreichen kann, wenn ein Mitglied des G+D-Konzerns die Binding Corporate Rules nicht einhält.

Hierfür werden alle wichtigen Einzelheiten des Verfahrens für die Bearbeitung von Beschwerden und die zum Einreichen der Beschwerde benötigten Kontaktinformationen (E-Mail-Adresse und Postanschrift) auf der Unternehmenswebseite des G+D-Konzerns veröffentlicht.

## **8. Rechte und Rechtsmittel der Betroffenen Person**

Die betroffene Person hat als Drittbegünstigte das Recht der Binding Corporate Rules gegen jegliches Mitglied des G+D-Konzerns, welches die personenbezogenen Daten der betroffenen Person verarbeitet, durchzusetzen. Die Rechte als Drittbegünstigter beinhalten gerichtliche Rechtsbehelfe bei Verstoß gegen die garantierten Rechte und Schadensersatzansprüche. Zur Durchsetzung ihrer Rechte als Drittbegünstigte hat die betroffene Person das Recht, bei der zuständigen Datenschutzbehörde Beschwerde einzureichen und/oder innerhalb der gerichtlichen Zuständigkeit des Datenexporteurs oder vor dem für die Konzernmutter zuständigen Gericht Forderungen geltend zu machen. Die betroffene Person wird nachdrücklich ermutigt, vor dem Einreichen von Beschwerden und Forderungen zunächst die dieser Binding Corporate Rules aufgeführten Beschwerdeverfahren zu befolgen.

## **9. Rechte und Rechtsmittel der Kunden**

Jedes Mitglied des G+D-Konzerns haftet gegenüber dem Kunden für die Verletzung seiner Pflichten aus diesen Binding Corporate Rules oder soweit anwendbar nach dem Leistungsvertrag, wie es das anwendbare Recht bestimmt. Der Kunde ist darüber hinaus berechtigt, diese Binding Corporate Rules gegenüber einem Mitglied des G+D-Konzerns als drittbegünstigende Rechte geltend zu machen, das als Auftragsverarbeiter, bezüglich der personenbezogenen Daten, die der G+D-Konzern von dem Kunden erhalten hat, fungiert, sofern dieses Mitglied des G+D-Konzerns seine jeweiligen Pflichten aus diesen Binding Corporate Rules verletzt hat.

## **10. Haftung**

Die Mitglieder des G+D-Konzerns erkennen an, dass sie unter diesen Binding Corporate Rules für einen gegen drittbegünstigende Rechte gegenüber betroffenen Personen entsprechend den folgenden Bestimmungen dieses Abschnitts 19 haften. Betroffene Personen werden in der Wahrnehmung ihrer Rechte unterstützt und nicht benachteiligt oder in anderer Weise behindert.

## **11. Gegenseitige Unterstützung und Zusammenarbeit mit Aufsichtsbehörden**

Die Mitglieder des G+D-Konzerns verpflichten sich, angemessen zusammen zu arbeiten und sich gegenseitig zu unterstützen, bei der Sicherstellung der Einhaltung dieser Binding Corporate Rules sowie im Umgang mit einer Anfrage oder Beschwerde durch einen Kunden oder gegebenenfalls eine betroffene Person oder bei der Ermittlung oder Anfrage einer Aufsichtsbehörde.

Darüber hinaus stimmen die Mitglieder des G+D-Konzerns zu, mit den zuständigen Aufsichtsbehörden zusammenzuarbeiten und den Empfehlungen der Aufsichtsbehörden bei der Auslegung und Anwendung dieser Binding Corporate Rules Folge zu leisten.

## **12. Aktualisierung und Änderung der Binding Corporate Rules**

Diese Binding Corporate Rules können entsprechend den anwendbaren internen Richtlinien des G+D-Konzerns aktualisiert und/oder geändert werden, zum Beispiel wenn die Berücksichtigung von Änderungen der regulatorischen Rahmenbedingungen oder der Datenverarbeitungsprozesse innerhalb des G+D-Konzerns notwendig wird.

## **13. Verhältnis zwischen nationalem Recht und den Binding Corporate Rules**

Jede Verarbeitung personenbezogener Daten durch ein Mitglied des G+D-Konzerns unterliegt dem anwendbarem lokalem Recht. Diese Binding Corporate Rules gelten zusätzlich zu, und nicht anstelle von, anderen Rechten und Rechtsmitteln, die betroffene Personen gegebenenfalls nach anwendbarem lokalem Recht haben; alle diese Rechte und Rechtsmittel bleiben von den Binding Corporate Rules unberührt.

Schreibt das anwendbare lokale Recht ein höheres Schutzniveau für personenbezogene Daten vor als dies in diesen Binding Corporate Rules vorgesehen ist, hat das lokale Recht Vorrang vor diesen Binding Corporate Rules.

## **14. Pflichten der Mitglieder des G+D-Konzerns in ihrer Rolle als Verantwortliche**

### **Verarbeitungszwecke und Zweckbindung**

Personenbezogene Daten sollen nur dann verarbeitet werden, wenn dies für einen oder mehrere der im folgenden bestimmten Zwecke erforderlich oder nach dem jeweils anwendbarem Recht vorgeschrieben ist.

- Personenbezogene Daten, der Mitarbeiter der Unternehmen des G+D-Konzerns werden zum Zwecke des Personalmanagements einschließlich der allgemeinen Verwaltung des Arbeitsverhältnisses, der Arbeitnehmerverwaltung in der Matrixstruktur des G+D-Konzerns, der weltweiten Zusammenarbeit, der Schulungsprogramme, der Leistungs- und Entwicklungsplanung, der Nachfolgeplanung, der Gewährleistung eines zulänglichen Talentpools für Schlüsselpositionen innerhalb des G+D-Konzerns, der weltweiten Mobilität der Mitarbeiter und der Sicherstellung eines 24/7 IT-Supports zur Verfügung steht, verarbeitet. Besondere Kategorien personenbezogener Daten der Mitarbeiter des G+D-Konzerns werden nur verarbeitet, soweit dies notwendig ist, um ein Arbeitsverhältnis einzugehen und durchzuführen sowie die Pflichten und spezifischen Rechten auf dem Gebiet des Arbeitsrechts durch zu führen. Für andere Zwecke werden sie nur verarbeitet, wenn dies nach anwendbarem Recht vorgeschrieben ist oder die Mitarbeiter in die Verarbeitung ihrer Daten ausdrücklich eingewilligt haben.

- Personenbezogene Daten, die sich auf Mitarbeiter oder Kontaktpersonen von Geschäftspartnern beziehen, werden zur Durchführung und zur Verwaltung der Beziehungen mit den Geschäftspartnern verarbeitet sowie um Vertragsbeziehungen einzugehen, durchzuführen, weltweite Zusammenarbeit für Kundenprojekte zu ermöglichen, Kundenservice und -support bereitzustellen und die Einhaltung gesetzlicher Vorgaben sicherzustellen.

- Personenbezogene Daten dürfen nicht in einer mit den Zwecken, für die sie ursprünglich erhoben wurden, nicht zu vereinbarenden Weise weiterverarbeitet werden.

## **Datenqualität und Verhältnismäßigkeit**

Der G+D-Konzern stellt sicher, dass die verarbeiteten personenbezogenen Daten richtig, vollständig und soweit auf dem neuesten Stand sind, wie dies für den jeweiligen Zweck vernünftigerweise erforderlich ist. Der G+D-Konzern ergreift alle angemessenen Maßnahmen, um personenbezogene Daten, die unrichtig, unvollständig oder veraltet sind, unter Berücksichtigung des Zwecks, für den sie erhoben oder Verarbeitet wurden, zu berichtigen oder zu löschen.

Die Verarbeitung personenbezogener Daten ist zu beschränken auf Daten, die für den jeweiligen Zweck angemessen und erforderlich sind und darf nicht über die Zwecke, für die diese Daten erhoben und/oder weiterverarbeitet werden, hinausgehen. Werden personenbezogene Daten für die jeweiligen Zwecke nicht mehr benötigt, dürfen sie nicht weiter verarbeitet werden und müssen insoweit gelöscht oder vernichtet werden.

## **Rechtsgrundlage für die Verarbeitung Personenbezogener Daten**

Personenbezogene Daten sollen nur aus einem oder mehreren der folgenden Gründe verarbeitet werden:

- Die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich, bei dem die betroffene Person Vertragspartei ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen; oder
- die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; oder
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich; oder
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse oder in legitimer Ausübung hoheitlicher Befugnisse ausgeführt wird, die dem Verantwortlichen oder einem Empfänger, dem die Daten übermittelt werden, übertragen wurde; oder
- die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem Verantwortlichen oder von dem bzw. den Empfängern wahrgenommen wird, denen die Daten übermittelt werden, sofern diese Interessen nicht durch die überwiegenden Interessen an der Wahrung der Grundrechte und Grundfreiheiten der betroffenen Person außer Kraft gesetzt werden.

Trifft keiner der oben genannten Gründe zu, muss der G+D-Konzern die eindeutige Einwilligung der betroffenen Person einholen, bevor er ihre personenbezogenen Daten verarbeitet. Die betroffene Person kann ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen, sofern nicht durch anwendbares Recht anders vorgeschrieben. In diesem Fall stellt der G+D-Konzern jede weitere Verarbeitung ein, es sei denn, die Verarbeitung ist durch anwendbares Recht vorgeschrieben oder im Rahmen einer Vertragsbeziehung mit der betroffenen Person unbedingt notwendig.

## **Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten**

Der G+D-Konzern verpflichtet sich, Besondere Kategorien personenbezogener Daten nur zu verarbeiten, wenn einer oder mehrere der folgenden Gründe zutreffen:

- Die betroffene Person hat ausdrücklich in die Verarbeitung dieser besonderen Kategorien personenbezogener Daten eingewilligt; oder
- die Verarbeitung ist erforderlich, um den Pflichten und spezifischen Rechten des Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund der nationale Gesetzgebung erlaubt ist und angemessene Absicherungen vorgesehen werden; oder
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder

- die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die 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; oder
- die Verarbeitung bezieht sich auf Besondere Kategorien Personenbezogener Daten, die die betroffene Person offensichtlich öffentlich gemacht hat; oder
- die Verarbeitung der Besonderen Kategorien Personenbezogener Daten ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich; oder
- die Verarbeitung der Besonderen Kategorien Personenbezogener Daten ist für Zwecke der Gesundheitsvorsorge, für die medizinischen Diagnostik, der Versorgung oder Behandlung im Gesundheitsbereich oder für die Verwaltung von Gesundheitsdiensten erforderlich und die Verarbeitung dieser Besonderen Kategorien Personenbezogener Daten erfolgt durch ärztliches Personal, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

### **Informationen für betroffene Personen**

Die Mitglieder des G+D-Konzerns verpflichten sich, betroffenen Personen vor der Verarbeitung ihrer personenbezogenen Daten mindestens die folgenden Informationen zur Verfügung zu stellen, sofern die betroffenen Personen über diese nicht bereits verfügen:

- die Identität des Mitglieds des G+D-Konzerns, das als Verantwortlicher handelt, und seines Vertreters (falls zutreffend),
- die Zwecke der Verarbeitung, für die die Daten bestimmt sind, und
- alle weiteren Informationen, wie die Kategorien der betroffenen Personenbezogenen Daten, die Empfänger oder Kategorien der Empfänger der Daten und das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich der Daten der betroffenen Person, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten verarbeitet werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Betroffene Personen werden über die Verarbeitung und/oder Übermittlung ihrer personenbezogenen Daten auf der Unternehmenswebseite des G+D-Konzerns sowie gegebenenfalls, auch durch Verweise auf diese Webseite, in der Geschäftskommunikation und in Unternehmensbroschüren oder auf ähnliche, angemessene Weise informiert.

### **Recht auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch**

Betroffene Personen haben das Recht, frei und ungehindert in angemessenen zeitlichen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten eine Kopie aller sie betreffenden Personenbezogenen Daten zu erhalten, die vom jeweiligen Mitglied des G+D-Konzerns, das als Verantwortlicher in Bezug auf ihre Personenbezogenen Daten handelt, verarbeitet werden, darunter Informationen über die Zwecke der Verarbeitung, alle verfügbaren Informationen über die Herkunft der Personenbezogenen Daten sowie über die Empfänger beziehungsweise Empfängerkategorien, denen die Personenbezogenen Daten übermittelt werden.

Betroffene Personen haben außerdem je nach Fall das Recht, die Berichtigung, Löschung oder Sperrung ihrer Personenbezogenen Daten zu fordern, insbesondere, wenn die Personenbezogenen Daten unvollständig oder unrichtig sind, es sei denn, die Verarbeitung dieser Personenbezogenen Daten in ihrer unveränderten Form ist durch anwendbares Recht vorgeschrieben. Betroffene Personen haben das Recht,

vom Verantwortlichen zu verlangen, dass Empfängern, denen die Daten übermittelt wurden, jede Berichtigung, Löschung oder Sperrung mitgeteilt wird, es sei denn, dies erweist sich als unmöglich oder bedeutet einen unverhältnismäßigen Aufwand.

Betroffene Personen haben das Recht, jederzeit aus zwingenden und berechtigten, sich aus ihrer besonderen Situation ergebenden Gründen gegen die Verarbeitung ihrer Personenbezogenen Daten Widerspruch einzulegen, es sei denn, diese Verarbeitung ist durch anwendbares Recht vorgeschrieben. Bei berechtigtem Widerspruch verpflichtet sich der G+D-Konzern, die Verarbeitung einzustellen.

Darüber hinaus haben betroffene Personen das Recht, gegen die Verarbeitung ihrer Personenbezogenen Daten zu Zwecken der Direktwerbung (falls zutreffend) kostenfrei Widerspruch einzulegen.

Betroffene Personen können von ihren oben genannten Rechten Gebrauch machen, indem sie den für das jeweilige Mitglied des G+D-Konzerns, das in Hinblick auf ihre Personenbezogenen Daten als Verantwortlicher handelt, zuständigen Privacy Officer kontaktieren. Die Kontaktinformationen des zuständigen Privacy Officers jedes Mitglieds des G+D-Konzerns werden auf der Unternehmenswebseite des G+D-Konzerns veröffentlicht.

### **Sicherheit und Vertraulichkeit der Daten**

Alle Mitglieder des G+D-Konzerns haben angemessene technische und organisatorische Maßnahmen umgesetzt und verpflichten sich, diese aufrechtzuerhalten, um personenbezogene Daten vor ungewollter oder gesetzeswidriger Vernichtung und ungewolltem Verlust, Änderung, unberechtigter Offenlegung und unberechtigtem Zugriff, sowie vor jeder sonstigen Form der gesetzeswidrigen Verarbeitung zu schützen, insbesondere wenn im Rahmen der Verarbeitung personenbezogene Daten in einem Netzwerk übertragen werden.

### **Beziehungen zu Auftragsverarbeitern, die Mitglieder des G+D-Konzerns sind**

Mitglieder des G+D-Konzerns, die im Auftrag eines zum G+D-Konzern gehörenden Verantwortlichen personenbezogene Daten verarbeiten, sind in ihrer Funktion als Auftragsverarbeiter in dem für sie anwendbarem Umfang ebenfalls an diese Binding Corporate Rules gebunden.

### **Pflichten des Auftragsverarbeiter**

Mitglieder des G+D-Konzerns, die als Auftragsverarbeiter handeln, willigen ein, die von einem zum G+D-Konzern gehörenden Verantwortlichen erhaltenen Personenbezogenen Daten nur in dessen Auftrag und gemäß seinen Anweisungen zu verarbeiten sowie angemessene technische und organisatorische Maßnahmen umzusetzen, um diese Personenbezogenen Daten vor ungewollter oder gesetzeswidriger Vernichtung und ungewolltem Verlust, Änderung, unberechtigter Offenlegung und unberechtigtem Zugriff, sowie vor jeder sonstigen Form der gesetzeswidrigen Verarbeitung zu schützen, insbesondere wenn im Rahmen der Verarbeitung personenbezogene Daten in einem Netzwerk übertragen werden.

In ihrer Funktion als Auftragsverarbeiter sind diese Mitglieder des G+D-Konzerns darüber hinaus generell verpflichtet, zum G+D-Konzern gehörenden Verantwortlichen bei der Erfüllung ihrer Pflichten gemäß diesen Binding Corporate Rules (insbesondere in Bezug auf die Pflichten der Verantwortlichen in Hinblick auf die Wahrung der Rechte betroffener Personen) zu helfen und zu assistieren.

### **Pflichten des Verantwortlichen**

Zum G+D-Konzern gehörende Verantwortliche müssen einen Auftragsverarbeiter auswählen, der hinsichtlich der technischen und organisatorischen Sicherheitsvorkehrungen für die durchzuführende Verarbeitung ausreichende Gewähr bietet, und die Einhaltung dieser Maßnahmen sicherstellen.

Darüber hinaus können Verantwortliche diese Auftragsverarbeiter nur mittels schriftlichen Vertrags gemäß Artikel 16 und 17 der EU-Richtlinie 95/46/EG und anwendbarem lokalem Recht beauftragen. Insbesondere muss in dem Vertrag vorgesehen sein, dass der Auftragsverarbeiter nur auf Weisung des Verantwortlichen handelt und angemessene technische und organisatorische Sicherheitsmaßnahmen umsetzt, sofern diese nicht bereits gemäß diesen Binding Corporate Rules gelten.

### **Übermittlung und Weiterübermittlung Personenbezogener Daten an Verantwortliche außerhalb des G+D-Konzerns**

Wenn ein Mitglied des G+D-Konzerns in seiner Funktion als Verantwortlicher beabsichtigt, personenbezogene Daten an einen externen Verantwortlichen in einem Drittland ohne Angemessenes Datenschutzniveau zu übermitteln, verpflichtet es sich, angemessene Maßnahmen für die Erfüllung der Auflagen zu ergreifen, die sich aus den Artikeln 25 und 26 der Richtlinie 1995/46/EG ergeben, indem es beispielsweise die von der Europäischen Kommission mittels Beschluss Nr. 2004/915/EG verabschiedeten Standardvertragsklauseln (für die Übermittlung personenbezogener Daten an Drittländer) anwendet.

### **Übermittlung Personenbezogener Daten an Auftragsverarbeiter außerhalb des G+D-Konzerns**

Wenn ein Mitglied des G+D-Konzerns in seiner Funktion als Verantwortlicher beabsichtigt, einen externen Auftragsverarbeiter zu beauftragen, verpflichtet es sich, den diesen aus diesen Binding Corporate Rules ergebenden Pflichten nachzukommen, um die Anforderungen der Artikel 16 und 17 der EU-Richtlinie 95/46/EG und ihre anwendbare nationale Umsetzung zu erfüllen.

Wenn der Externe Auftragsverarbeiter seinen Sitz in einem Drittland ohne Angemessenes Datenschutzniveau hat, verpflichtet sich das Mitglied des G+D-Konzerns, das als Verantwortlicher handelt, zudem, angemessene Maßnahmen für die Erfüllung der Auflagen zu ergreifen, die sich aus den Artikeln 25 und 26 der EU-Richtlinie 95/46/EG ergeben, indem es beispielsweise die von der Europäischen Kommission mittels Beschluss Nr. 2010/87/EG verabschiedeten Standardvertragsklauseln (für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern) anwendet.

### **Maßnahmen im Falle nationaler Gesetzgebung, die die Einhaltung der Binding Corporate Rules verhindert**

Hat ein Mitglied des G+D-Konzerns Grund zu der Annahme, dass ihn die anwendbare Gesetzgebung an der Erfüllung seiner Pflichten gemäß diesen Binding Corporate Rules hindern könnten, und hat dies einen erheblichen Einfluss auf die durch die Binding Corporate Rules gewährten Sicherheiten, so informiert das Mitglied des G+D-Konzerns unverzüglich den Group Privacy Officer, es sei denn, dies wird ihm von einer Sicherheitsbehörde oder durch anwendbares Recht untersagt. Der Group Privacy Officer informiert die Geschäftsführung des G+D-Konzerns. Handelt das Mitglied des G+D-Konzerns als Auftragsverarbeiter gemäß diesen Binding Corporate Rules, so informiert es zusätzlich den Verantwortlichen des G+D-Konzerns, von dem er die Personenbezogenen Daten empfangen hat, es sei denn, dies wird ihm von einer Sicherheitsbehörde oder durch anwendbares Recht untersagt.

Wenn die Verpflichtungen aus den Binding Corporate Rules im Widerspruch zu nationalem Recht stehen, entscheidet die Geschäftsführung des G+D-Konzerns über die zu ergreifenden Maßnahmen und konsultiert im Zweifelsfall die zuständigen Datenschutzbehörden.

## **15. Pflichten der Mitglieder des G+D-Konzerns in ihrer Rolle als Auftragsverarbeiter**

Die Mitglieder des G+D-Konzerns sowie all deren Mitarbeiter verarbeiten personenbezogene Daten, die sie von Kunden erhalten haben, als Auftragsverarbeiter ausschließlich in dessen Auftrag und entsprechend dessen Weisungen.

Soweit ein Mitglied des G+D-Konzerns dies, gleich aus welchen Gründen, nicht gewährleisten kann, informiert es den Kunden hierüber unverzüglich. In einem solchen Fall ist der Kunde (entsprechend der Bestimmungen des Leistungsvertrages) dazu berechtigt, den Datentransfer einzustellen und/oder den Leistungsvertrag zu kündigen.

Soweit ein Mitglied des G+D-Konzerns Grund zu der Annahme hat, dass die, sich aus diesen Binding Corporate Rules ergebenden Pflichten, aufgrund der geltenden oder künftig anzuwendenden Rechtsvorschriften nicht erfüllt werden können und dies geeignet ist, die durch diese Binding Corporate Rules gewährleisteten Garantien wesentlich zu beeinträchtigen, informiert das Mitglied des G+D-Konzerns unverzüglich, ohne schuldhaftes Zögern, den Group Privacy Officer, den betroffenen Kunden (welcher in diesem Fall zur Einstellung des Datentransfers- oder unter Berücksichtigung der Regelungen des Leistungsvertrags - berechtigt ist jenen zu beenden) sowie die für den jeweiligen Kunden zuständige Aufsichtsbehörde. Der Group Privacy Officer informiert daraufhin die Geschäftsführung des G+D-Konzerns.

### **Mitwirkungs- und Unterstützungspflicht**

Die Mitglieder des G+D-Konzerns verpflichten sich, den Kunden bei der Einhaltung der gesetzlichen Bestimmungen zu unterstützen (wie beispielsweise bei der Pflicht die subjektiven Rechte der Betroffenen Person zu respektieren, bei der Pflicht Beschwerden zu beantworten oder einer Aufsichtsbehörde Rechenschaft ablegen zu können), die noch ausführlicher in diesen Binding Corporate Rules aufgeführt sind. Eine solche Unterstützung umfasst darüber hinaus beispielsweise, Verarbeitungs-Prozesse weiterer Auftragsverarbeiter transparent zu gestalten beziehungsweise offen zu legen, um dem Verantwortlichen eine korrekte Information gegenüber der Betroffenen Person zu ermöglichen. Insbesondere verpflichten sich die Mitglieder des G+D-Konzerns im Rahmen ihrer Möglichkeiten alle relevanten Informationen zur Verfügung zu stellen, um den Kunden bei der Erfüllung seiner Pflichten, wie etwa (a) die betroffene Person über die Verarbeitung ihrer Personenbezogenen Daten zu unterrichten, (b) die im Auftrag des Kunden verarbeiteten Personenbezogenen Daten auf Verlangen des Kunden und/oder einer Betroffenen Person oder nach dem gesetzlichen Bestimmungen zu korrigieren, zu löschen oder zu sperren und (c) auf Anfragen der Aufsichtsbehörden zu antworten. Der G+D-Konzern wird auf Verlangen des Kunden alle erforderlichen Maßnahmen zur Aktualisierung, Korrektur oder Löschung der Personenbezogenen Daten treffen, oder diese ab dem Zeitpunkt, ab dem das Identifikationsformular nicht mehr benötigt wird, zu löschen oder zu anonymisieren.

Jedes betroffene Mitglied des G+D-Konzerns informiert alle anderen Mitglieder des G+D-Konzerns, denen die personenbezogenen Daten übermittelt wurden, über jedwede Berichtigung, Löschung oder Anonymisierung.

Die Mitglieder des G+D-Konzerns unterstützen den Kunden und kommen jeder Anfrage bezüglich etwaiger Zusammenarbeit und Unterstützung innerhalb einer angemessenen Frist nach, soweit ihnen dies zumutbarer Weise möglich ist.



### **Rechte der Betroffenen Person**

Der Kunde ist für die Bearbeitung von Anfragen einer betroffenen Person hinsichtlich des Zugriffs, der Korrektur, der Löschung oder Sperrung der jeweiligen personenbezogenen Daten verantwortlich.

Soweit ein Mitglied des G+D-Konzerns eine direkte Anfrage der betroffenen Person bezüglich ihrer personenbezogener Daten erhält, leitet dieses Mitglied die Anfrage ohne deren Beantwortung an den Kunden weiter, es sei denn, im Leistungsvertrag ist etwas anderes vereinbart.

### **Technische und organisatorische Sicherheitsmaßnahmen**

Alle Mitglieder des G+D-Konzerns haben angemessene technische und organisatorische Sicherheitsmaßnahmen umgesetzt und verpflichten sich, diese aufrechtzuerhalten, um personenbezogene Daten vor ungewollter oder gesetzeswidriger Vernichtung und ungewolltem Verlust, Änderung, unberechtigter Offenlegung und unberechtigtem Zugriff, sowie vor jeder sonstigen Form der gesetzeswidrigen Verarbeitung zu schützen, insbesondere wenn im Rahmen der Verarbeitung personenbezogene Daten in einem Netzwerk übertragen werden.

Alle Mitarbeiter sowie Mitglieder des G+D-Konzerns halten sich an diese technischen und organisatorischen Sicherheitsmaßnahmen.

Die Mitarbeiter des G+D-Konzerns haben nur insoweit Zugriff auf personenbezogene Daten, wie dies für die Durchführung ihrer Aufgaben notwendig und für den jeweiligen anwendbaren Zweck vorgesehen ist. Alle Mitarbeiter, die Zugriff auf personenbezogene Daten haben, sind verpflichtet, diese personenbezogenen Daten mit angemessener Vertraulichkeit zu behandeln.

Diese technischen und organisatorischen Sicherheitsmaßnahmen müssen mindestens den Anforderungen des, für den Kunden im Leistungsvertrag angegebenen Rechts, sowie den im Leistungsvertrag festgelegten Sicherheits- und Vertraulichkeitsmaßnahmen entsprechen.

Durch diese technischen und organisatorischen Sicherheitsmaßnahmen wird ein Sicherheitsniveau gewährleistet, welches den, mit der Verarbeitung personenbezogener Daten einhergehenden, Risiken entspricht. Die Verarbeitung besonderer Kategorien personenbezogener Daten unterliegt erhöhten Sicherheitsmaßnahmen.

### **Anzeigepflicht bei Verstößen gegen die Datensicherheit**

Jedes Mitglied des G+D Konzerns informiert den Kunden unverzüglich über etwaige unbefugte Zugriffe, rechtswidrige Zerstörung, unbeabsichtigten Verlust oder die Veränderung personenbezogener Daten, die im Auftrag des Kunden verarbeitet wurden.

### **Verpflichtungen nach Beendigung des Leistungsvertrages**

Jedes Mitglied des G+D -Konzerns, das im Rahmen eines Leistungsvertrages und dieser Binding Corporate Rules personenbezogene Daten im Auftrag eines Kunden verarbeitet, ist, abhängig von den Bedingungen des Leistungsvertrages (z.B. hinsichtlich des Datenformats, der Vertragsdauer und der Preisgestaltung), an Wahl und Anfrage des Kunden für den Zeitraum nach Beendigung des Leistungsvertrages gebunden, wie sie im Leistungsvertrag Ausdruck finden kann, und sendet diesem die in seiner [der des Mitglieds des G+D-Konzerns] Kontrolle stehenden Personenbezogenen Daten entweder zurück oder löscht diese unwiderruflich und bestätigt dem Kunden, dass er dies getan hat.

Soweit das geltende Recht verbietet, dass die im Auftrag des Kunden verarbeiteten personenbezogenen Daten ganz oder teilweise zurückgegeben oder gelöscht werden, wird der Kunde durch das jeweilige Mitglied des G+D-Konzerns hierüber informiert und dieses sichert zu, dass es (a) die Vertraulichkeit der Personenbezogenen Daten garantiert und (b) es die Personenbezogenen Daten nicht mehr aktiv verarbeitet wird.