GMC INSTRUMENTS

DATEN-SCHUTZ-LEITLINIE

DER GMC-INSTRUMENTS GMBH

Inhaltsverzeichnis

1 Ziel dieser Datenschutzleitlinie

- Die GMC-Intruments Gruppe (GMC-I Gruppe) verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur internationalen Einhaltung von Datenschutzrechten. Diese Datenschutzleitlinie beruht auf global akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der Unternehmensgruppe.

- Diese Datenschutzleitlinie schafft eine der notwendigen Rahmenbedingungen für weltweite Datenübermittlungen personenbezogener Daten zwischen den Unternehmen der GMC-I Gruppe. Sie gewährleistet das von der Europäischen Datenschutzgrundverordnung (DSGVO) und den nationalen Gesetzen verlangte angemessene Datenschutzniveau für den innerdeutschen und grenzüberschreitenden Datenverkehr auch in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau (Drittländer) besteht.

2 Definitionen

- Ein angemessenes Datenschutzniveau von Drittstaaten wird von der EU Kommission dann anerkannt, wenn der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schließt die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Standesregeln und Sicherheitsmaßnahmen ein.

- Anonymisiert sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

- Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass 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.

- Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

- Betroffener im Sinne dieser Datenschutzleitlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.

- Datenschutzvorfälle sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten (pbD) rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Mitarbeiter beziehen.

- Dritter ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle.

- Auftragsdatenverarbeiter bzw. Auftragsverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

- Drittstaaten im Sinne der Datenschutzleitlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.

- Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

- Datenschutzbeauftragter (DSB): Der Datenschutzbeauftragte im Unternehmen unterstützt die Selbstkontrolle des Unternehmens („interne Kontrolle“). Die einschlägigen gesetzlichen Regelungen zur Benennung sowie die Rechte und Pflichten des DSB sind in den Artikeln 37 bis 39 DSGVO und national (Deutschland) in § 38 BDSG beschrieben.

- Erforderlich ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.

- Der Europäische Wirtschaftsraum (EWR) ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.

- Personenbezogene Daten (personenbezogene Daten (pbD)) sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

- Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

- Verarbeitung personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

- Verantwortliche Stelle oder Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

3 Geltungsbereich und Änderung der Datenschutzleitlinie

- Diese Datenschutzleitlinie gilt für alle Unternehmen der GMC-I Gruppe.

- Die Datenschutzleitlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten (pbD) geschützt werden, gilt diese Datenschutzleitlinie auch in gleicher Weise für Daten juristischer Personen. Anonymisierte Daten, z. B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzleitlinie.

- Die einzelnen Gesellschaften der GMC-I Gruppe sind nicht berechtigt, von dieser Datenschutzleitlinie abweichende Regelungen zu treffen, es sei denn diese sind vor Inkraftsetzung von der Holding der GMC-I Gruppe, der GMC-Intruments GmbH (GMC-I), freigegeben.

4 Geltung staatlichen Rechts

- Diese Datenschutzleitlinie beinhaltet grundlegende Datenschutzprinzipien, ohne dass bestehendes staatliches Recht ersetzt wird. Sie ergänzt das jeweilige nationale Datenschutzrecht. Das jeweilige staatliche Recht geht vor, wenn es Abweichungen von dieser Datenschutzleitlinie erfordert oder weitergehende Anforderungen stellt. Die Inhalte dieser Datenschutzleitlinie sind auch dann zu beachten, wenn es kein entsprechendes staatliches Recht gibt. Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen müssen beachtet werden.

- Jedes Unternehmen der GMC-I Gruppe ist für die Einhaltung dieser Datenschutzleitlinie und der gesetzlichen Verpflichtungen verantwortlich. Hat es Grund zu der Annahme, dass gesetzliche Verpflichtungen im Widerspruch zu den Pflichten aus dieser Datenschutzleitlinie stehen, hat das betroffene Unternehmen unverzüglich die Unternehmensleitung der GMC-I Gruppe zu informieren. Im Falle einer Kollision zwischen nationaler Rechtsvorschrift und der Datenschutzleitlinie wird die GMC-I Gruppe gemeinsam mit dem betroffenen Unternehmen nach einer praktikablen Lösung im Sinne der Ziele der Datenschutzleitlinie suchen.

5 Prinzipien für die Verarbeitung personenbezogener Daten

5.1 Fairness und Rechtmäßigkeit

- Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten (pbD) müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

5.2 Zweckbindung

- Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

5.3 Transparenz

- Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten (pbD) bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss bei Erhebung der Daten der Betroffene mindestens Folgendes erkennen können oder zum Zeitpunkt der Erhebung entsprechend informiert werden über:
  - Die Identität der verantwortlichen Stelle
  - Den Zweck der Datenverarbeitung
  - Kontaktdaten des Datenschutzbeauftragten
  - Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden
  - Speicherdauer bzw. Kriterien für die Löschung
  - Recht auf Beschwerde bei einer Aufsichtsbehörde
  - Recht auf Auskunft, Berichtigung, Einschränkung, Widerruf
  - Herkunft der Daten (Wenn die Daten nicht beim Betroffenen erhoben wurden)

5.4 Datenvermeidung und Datensparsamkeit

- Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten (pbD) dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

5.5 Löschung

- Personenbezogene Daten (pbD), die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht bzw. vernichtet werden, es sei denn es besteht im Einzelfall ein schutzwürdiges Interesse an deren darüberhinausgehenden Speicherung.

5.6 Sachliche Richtigkeit und Datenaktualität

- Personenbezogene Daten (pbD) sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

5.7 Vertraulichkeit und Datensicherheit

- Für personenbezogene Daten (pbD) gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

6 Zulässigkeit der Datenverarbeitung

- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

6.1 Kunden- und Partnerdaten

6.1.1 Datenverarbeitung für eine vertragliche Beziehung

- Personenbezogene Daten (pbD) des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten. Für darüberhinausgehende Werbemaßnahmen müssen die unten folgenden Voraussetzungen beachtet werden.

6.1.2 Datenverarbeitung zu Werbezwecken

- Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen der GMC-I Gruppe (z. B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

- Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen soll eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden.

- Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke sind zu beachten.
-
-

6.1.3 Einwilligung in die Datenverarbeitung

- Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß 5.3. dieser Datenschutzleitlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z. B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

6.1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

- Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

6.1.5 Datenverarbeitung aufgrund berechtigten Interesses

- Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der GMC-I Gruppe erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z. B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z. B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen. Die Begründung für berechtigte Interessen ist von der Leitung der Unternehmensgruppe freizugeben.

6.1.6 Verarbeitung besonders schutzwürdiger Daten

- Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragen der Unternehmensgruppe im Vorfeld zu informieren.

6.1.7 Automatisierte Einzelentscheidungen

- Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z. B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden.

- Solche automatisierten Verarbeitungen dürfen in der GMC-I Gruppe nicht durchgeführt werden.

- Sollte dies im Einzelfall notwendig sein, sind diese vor Einführung von der Geschäftsführung der GMC-Intruments GmbH zu genehmigen.

6.1.8 Nutzerdaten und Internet

- Wenn auf Webseiten oder in Apps personenbezogene Daten (pbD) erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

- Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out).

- Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten (pbD) ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird. Sofern in einzelnen Gesellschaften Richtlinien zum Identitäts- und Authentifizierungs-Management existieren, müssen sie dementsprechend ausgestaltet sein und sind verbindlich zu beachten.

6.2 Beschäftigtendaten

6.2.1 Datenverarbeitung für das Arbeitsverhältnis

- Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten (pbD) von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Konzerngesellschaften erforderlich.

- Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.
- Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

- Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

6.2.2 Kollektivregelungen für Datenverarbeitungen

- Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.

6.2.3 Einwilligung in die Datenverarbeitung

- Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß 5.3 dieser Datenschutzleitlinie informiert werden.

6.2.4 Datenverarbeitung aufgrund berechtigten Interesses

- Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der GMC-I Gruppe erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z. B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z. B. Qualifikationsnachweise) begründet.

- Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

- Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z. B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z. B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

6.2.5 Verarbeitung besonders schutzwürdiger Daten

- Besonders schutzwürdige personenbezogene Daten (pbD) dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

- Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.

- Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

6.2.6 Automatisierte Entscheidungen

- Soweit im Beschäftigungsverhältnis personenbezogene Daten (pbD) automatisiert verarbeitet werden, durch die einzelnen Persönlichkeitsmerkmale bewertet werden (z. B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein. Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist.

6.2.7 Telekommunikation und Internet

- Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden im Rahmen der betrieblichen Aufgabenstellung und nur für betriebliche Zwecke durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden.

- Im Ausnahmefall kann die Nutzung für private Zwecke in eingeschränktem Umfang erlaubt sein. Die setzt jedoch eine entsprechende schriftliche Unternehmens-Richtlinie oder eine schriftliche Genehmigung im Einzelfall voraus. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden.

- Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der GMC-I Gruppe bzw. der jeweiligen Gesellschaft erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Konzernregelungen.

7 Übermittlung personenbezogener Daten

- Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb oder innerhalb der GMC-I Gruppe unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 6. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

- Im Falle einer Datenübermittlung an einen Empfänger außerhalb der GMC-I Gruppe in einem Drittstaat (außerhalb des Europäischer Wirtschaftsraum) muss dieser ein zu dieser Datenschutzleitlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche gesetzliche Verpflichtung kann sich aus dem Recht des Sitzlandes der Konzerngesellschaft, welche die Daten übermittelt, ergeben oder das Recht des Sitzlandes der Konzerngesellschaft erkennt das mit der gesetzlichen Verpflichtung eines Drittstaats verfolgte Ziel der Datenübermittlung an.

- Im Falle einer Datenübermittlung von Dritten an Unternehmen der GMC-I Gruppe muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

- Werden personenbezogene Daten (pbD) von einer Konzerngesellschaft mit Sitz im Europäischen Wirtschaftsraum an eine Konzerngesellschaft mit Sitz außerhalb des Europäischen Wirtschaftsraums (Drittstaat) übermittelt, so ist die datenimportierende Gesellschaft verpflichtet, bei allen Anfragen der für die datenexportierende Gesellschaft zuständigen Aufsichtsbehörde mit dieser zu kooperieren und die Feststellungen der Aufsichtsbehörde im Hinblick auf die übermittelten Daten zu beachten. Entsprechendes gilt für Datenübermittlungen durch Konzerngesellschaften aus anderen Staaten. Nehmen sie an einem internationalen Zertifizierungssystem für verbindliche Unternehmensregelungen zum Datenschutz teil, müssen sie die dort vorgesehene Kooperation mit den entsprechenden Prüfungsstellen und Behörden sicherstellen. Die Teilnahme an derartigen Zertifizierungssystemen ist von der Leitung der GMC-I Gruppe zu genehmigen.

- Im Fall eines von einem Betroffenen behaupteten Verstoßes gegen diese Datenschutzleitlinie durch eine datenimportierende Konzerngesellschaft mit Sitz in einem Drittstaat verpflichtet sich die datenexportierende Konzerngesellschaft mit Sitz im Europäischen Wirtschaftsraum, den Betroffenen, dessen Daten im Europäischen Wirtschaftsraum erhoben worden sind, sowohl bei der Sachverhaltsaufklärung zu unterstützen als auch die Durchsetzung seiner Rechte gemäß dieser Datenschutzleitlinie gegenüber der datenimportierenden Konzerngesellschaft sicherzustellen. Darüber hinaus ist der Betroffene berechtigt, seine Rechte auch gegenüber der datenexportierenden Konzerngesellschaft geltend zu machen. Bei einem behaupteten Verstoß muss die datenexportierende Gesellschaft gegenüber dem Betroffenen den Nachweis erbringen, dass der datenimportierenden Konzerngesellschaft in einem Drittland bei einer Weiterverarbeitung der erhaltenen Daten ein Verstoß gegen diese Datenschutzleitlinie nicht zuzurechnen ist.

8 Auftragsverarbeitung

- Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb der GMC-I Gruppe eine Vereinbarung über eine Auftragsverarbeitung abzuschließen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten (pbD) nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
3. Die vom Datenschutzbeauftragen der Unternehmensgruppe bereitgestellten Vertragsstandards müssen beachtet werden.
4. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.
5. Bei einer grenzüberschreitenden Auftragsverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzleitlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:

a) Vereinbarung der EU-Standardvertragsklauseln zur Auftragsverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.
b) Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus.
c) Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

9 Rechte des Betroffenen

- Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

- Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z. B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

- Werden personenbezogene Daten (pbD) an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

- Sollten personenbezogene Daten (pbD) unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

- Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

- Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

- Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet oder gesetzliche Aufbewahrungsfristen das Speichern der personenbezogene Daten (pbD) erforderlich machen.

- Darüber hinaus kann jeder Betroffene die in den Ziffern 5., 6., 7., 10., und 11 eingeräumten Rechte als Drittbegünstigter geltend machen, wenn ein Unternehmen, das sich zur Einhaltung der Datenschutzleitlinie verpflichtet hat, deren Vorgaben nicht beachtet und er dadurch in seinen Rechten verletzt ist.

10 Vertraulichkeit der Verarbeitung

- Personenbezogene Daten (pbD) unterliegen dem Datengeheimnis und der Vertraulichkeit. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

- Mitarbeiter dürfen personenbezogene Daten (pbD) nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.
- Vorgesetze müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses und der Vertraulichkeit unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

11 Sicherheit der Verarbeitung

- Personenbezogene Daten (pbD) sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Der verantwortliche Fachbereich kann hierzu den Verantwortlichen für die IT und den Datenschutzbeauftragten der Unternehmensgruppe zu Rate zu ziehen. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des gruppenweiten Datenschutzmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

12 Datenschutzkontrolle

- Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Datenschutzbeauftragen der Unternehmensgruppe oder beauftragten externen Prüfern. Die Ergebnisse der Datenschutzkontrollen sind dem Datenschutzbeauftragen der Unternehmensgruppe mitzuteilen. Die Unternehmensleitung der GMC-I Gruppe ist im Rahmen der jeweiligen Berichtspflichten über wesentliche Ergebnisse zu informieren. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

13 Datenschutzvorfälle

- Jeder Mitarbeiter hat seinem jeweiligen Vorgesetzten, dem IT-Verantwortlichen und dem Datenschutzbeauftragen der Unternehmensgruppe unverzüglich Fälle von Verstößen gegen diese Datenschutzleitlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) zu melden. Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, den Datenschutzbeauftragen der Unternehmensgruppe umgehend über Datenschutzvorfälle zu unterrichten.

  In Fällen von
  - ➡ unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
  - ➡ unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten (pbD), oder
  - ➡ bei Verlust personenbezogener Daten

  sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

14 Verantwortlichkeiten

- Die Geschäftsführungen der Konzerngesellschaften sind verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzleitlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z. B. nationale Meldepflichten). Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist die Geschäftsführung der GMC-Intruments GmbH umgehend zu informieren.

- Die Geschäftsführungen der Konzerngesellschaften können für ihre Gesellschaft einen Datenschutzbeauftragten benennen, wenn dies für die Umsetzung der nationalen Datenschutzbelange sinnvoll ist.

- Sind Kriterien zur verpflichtenden Benennung eines Datenschutzbeauftragten nach nationalen gesetzlichen Regelungen oder der DSGVO geben, hat der Geschäftsführer der betreffenden Konzerngesellschaft einen Datenschutzbeauftragten festzulegen.

- Benennt eine Einzelgesellschaft einen Datenschutzbeauftragten, ist die Geschäftsführung der GMC-Intruments GmbH umgehend zu informieren.

- Die Aufgaben des Datenschutzbeauftragten richten sich nach den jeweiligen gesetzlichen Regelungen.

Nürnberg, den 01.01.2024
GMC-Intruments GmbH

Joachim Czabanski
Vors. der Geschäftsführung

Matthias Wist
Geschäftsführer

GMC INSTRUMENTS

GMC-Intruments GmbH
Südwestpark 15 ■ 90449 Nürnberg ■ Deutschland
Tel.: +49 911 252661-0 ■ Fax: +49 911 252661-881

www.gmc-instruments.com ■ info@gmc-i.com

Gedruckt in Deutschland • Änderungen vorbehalten • 2/01.24 • 3-336-015-01