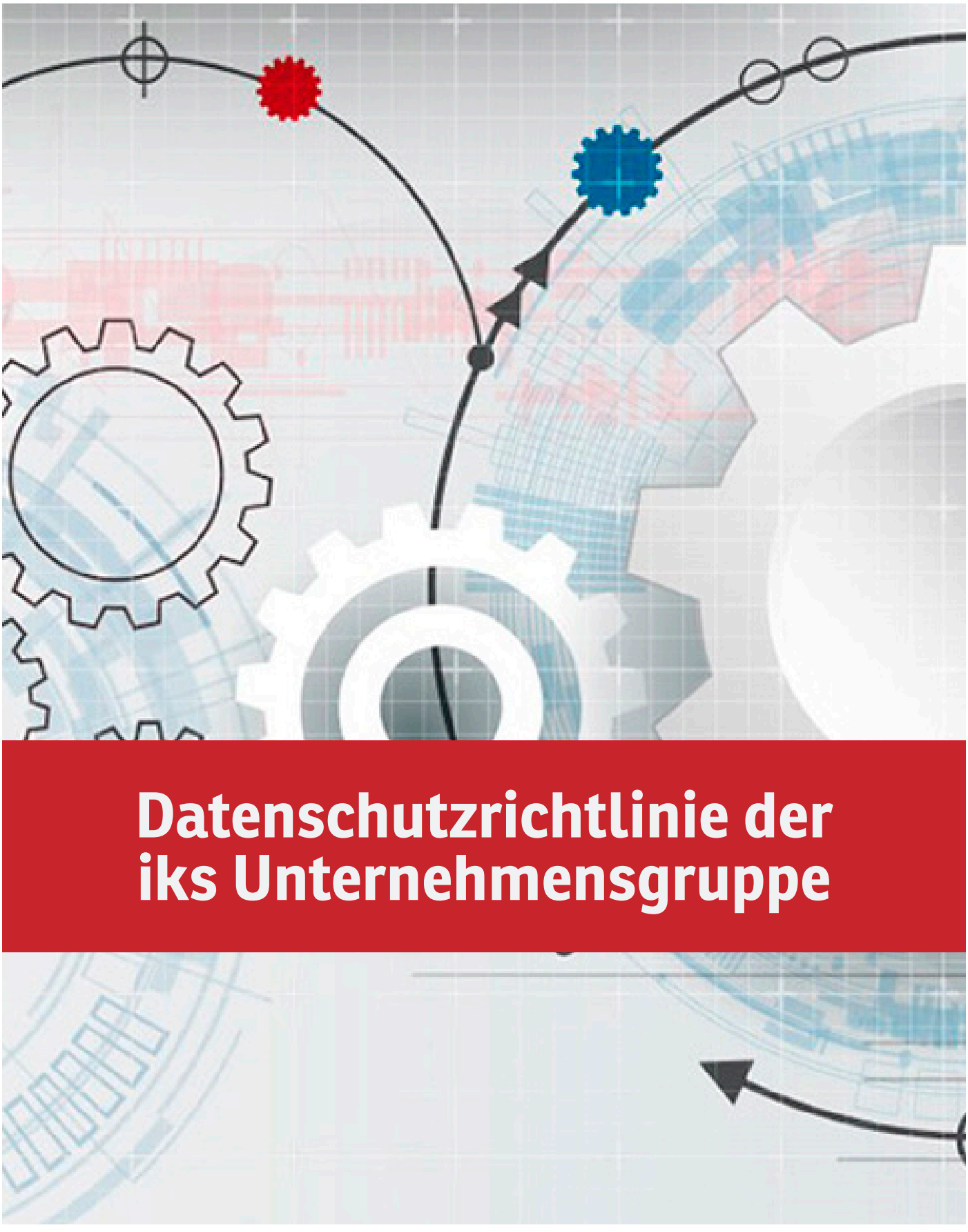

Datenschutzrichtlinie der iks Unternehmensgruppe

Inhalt

Vorwort

Wir freuen uns über Ihr Interesse an unseren Produkten und Dienstleistungen und möchten, dass Sie sich beim Besuch oder Kontakt zu unserem Unternehmen oder unseren Internetplattformen auch hinsichtlich des Schutzes Ihrer personenbezogenen Daten sicher fühlen.

In unserer Richtlinie zum Datenschutz haben wir strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Bewerbern und Mitarbeitern geregelt. Sie entspricht den Anforderungen der Europäischen Datenschutzrichtlinie und stellt die Einhaltung der Prinzipien der geltenden Datenschutzgesetze sicher. Dadurch setzen wir einen Datenschutz- und Datensicherheitsstandard in der iks Gruppe GmbH und ihren Töchtern, iks Engineering GmbH und TECnical Consulting GmbH (kurz iks Unternehmensgruppe) und regeln den Datenaustausch zwischen unseren Tochter¬gesellschaften.

Als Maßstab haben wir folgende Datenschutzgrundsätze festgelegt:

› Transparenz
› Datensparsamkeit
› Datensicherheit.

Unsere Führungskräfte und Mitarbeiter sind verpflichtet, diese Gruppenrichtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren. Als Datenbeauftragter trage ich dafür Sorge, dass die gesetzlichen Regelungen und Prinzipien zum Datenschutz bei der iks Unternehmensgruppe geachtet werden.

Meine Mitarbeiter und ich stehen Ihnen als Ansprechpartner bei Fragen zum Datenschutz und zur Datensicherheit gerne zur Verfügung.

Datenschutzbeauftragter

Ziel der Datenschutzrichtlinie

In dieser Richtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie wir diese Daten nutzen, mit wem wir sie teilen und welche Rechte und Wahlmöglichkeiten Personen im Zusammenhang mit unserer Nutzung ihrer personenbezogenen Daten haben. Des Weiteren beschreiben wir die Maßnahmen, die wir ergreifen, um die Datensicherheit zu gewährleisten, und wie Sie uns zu Fragen über unsere Datenschutzpraktiken und zur Ausübung Ihrer Rechte kontaktieren können.

Geltungsbereich

Diese Datenschutzrichtlinie gilt für alle Unternehmen der iks Unternehmensgruppe und deren Mitarbeiter. Die einzelnen Tochtergesellschaften der iks Unternehmensgruppe sind nicht berechtigt, von dieser Datenschutzrichtlinie abzuweichen. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

1 Prinzipien für die Verarbeitung personenbezogener Daten

1.1 Fairness und Rechtmäßigkeit

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

1.2 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.

1.3 Markt- und Meinungsforschung

Die Verarbeitung personenbezogener Daten zum Zwecke der Markt- und Meinungsforschung innerhalb der iks Unternehmensgruppe ist untersagt.

1.4 Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

› Die Identität der verantwortlichen Stelle
› Den Zweck der Datenverarbeitung
› Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

1.5 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 dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben.

1.6 Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäfts¬prozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

1.7 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten 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.

1.8 Vertraulichkeit und Datensicherheit

Für personenbezogene Daten 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.

2 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.

2.1 Kundendaten

2.1.1 Datenerhebung

Die Speicherung von personenbezogenen Kundendaten (Ansprechpartner: Name, E-Mail) erfolgt in der Regel bei nachfolgenden Kontaktaufnahmen.

2.1.1.1 Kontakt

Es finden folgende Kontaktaufnahmen von Kundenansprechpartner mit der iks Unternehmensgruppe statt:

› Telefon, Fax oder E-Mail (Nachweis: Dokument des Ansprechpartners)
› Persönliche Kontakte auf Messen, Kundenveranstaltungen, Schulungen, Symposien, usw. (Nachweis: Visitenkarten)
› Besuche durch iks Vertreter im Hause des Kunden (Nachweis: Visitenkarten)
› Vom Kunden veröffentliche Stellenausschreibungen

2.1.1.2 Internetplattform

Es finden folgende Kontaktaufnahmen von Kundenansprechpartnern mit der iks Unternehmensgruppe oder ihren Töchtern statt:

› Besuch auf Internetplattformen der iks, Homepage, Stem-p, usw.

2.1.1.3 Automatisierte Verfahren

Wenn Sie unsere Websites besuchen, können wir bestimmte Daten mittels automatisierter Verfahren erheben, z.B. durch die Verwendung von Cookies, Web Beacons und Server-Protokoll- Dateien. Zu den Daten, die wir auf diesem Wege erheben können, gehören IP-Adresse, eindeutige Gerätekennung (UDI), Browsermerkmale, Gerätemerkmale, Betriebssystem, sprachliche Präferenzen, verweisende URL, Informationen über Handlungen auf unseren Websites, Datum und Zeitpunkt des Besuchs unserer Websites und sonstige Nutzungsstatistiken. Ein Cookie ist eine Textdatei, die beim Besuch einer Internetseite an den Computer oder ein anderes mit dem Internet verbundenes Gerät des Besuchers verschickt wird, um dessen Browser eindeutig zu identifizieren oder um Informationen und Einstellungen im Browser zu speichern. Ein „Web Beacon“, auch als Internet-Tag, Pixel-Tag oder transparentes GIF bekannt, verlinkt Webseiten mit Webservern und deren Cookies und dient der Übermittlung von durch Cookies erfassten Daten zurück an einen Webserver. Durch diese automatisierten Erhebungsverfahren erhalten wir

„Clickstream- Daten“. Hierbei handelt es sich um Logdaten der Links und sonstiger Inhalte, die ein Besucher beim Browsen auf einer Website anklickt. Während der Besucher sich durch die Website klickt, kann eine Aufzeichnung seiner Zugriffe erfolgen und gespeichert werden. Wir verlinken bestimmte Datenelemente, die wir mittels automatisierter Verfahren erhoben haben, z.B. Ihre Browserinformationen, mit anderen Informationen, die wir über Sie erhalten haben, um bspw. zu erkennen, ob Sie eine von uns an Sie gesendete E-Mail geöffnet haben. Ihr Browser ist eventuell so eingestellt, dass Sie eine Benachrichtigung erhalten, wenn bestimmte Arten von Cookies an Sie gesendet werden, oder er informiert Sie darüber, wie Sie die Akzeptanz bestimmter Arten von Cookies einschränken oder diese deaktivieren können. Bitte beachten Sie jedoch, dass Sie ohne Cookies möglicherweise nicht alle Funktionen unserer Websites nutzen können. Soweit dies nach geltendem Recht erforderlich ist, holen wir Ihre Zustimmung ein, bevor wir Ihre personenbezogenen Daten mittels Cookies oder ähnlicher automatisierter Verfahren erheben. Die Drittanbieter von Apps, Tools, Widgets und Plug-ins auf unseren Websites, wie bspw. Social Media Sharing Tools, können ebenfalls automatisierte Verfahren zur Erhebung von Daten bezüglich Ihrer Interaktionen mit diesen Funktionen verwenden. Diese Daten werden unmittelbar von den Anbietern dieser Funktionen erhoben und unterliegen den Datenschutzrichtlinien oder -hinweisen dieser Anbieter

2.1.1.4 Einwilligung in die Datenverarbeitung

Die uns von gespeicherten Daten dienen dazu, mit Kunden in Kontakt zu treten und diesen aufrechtzuerhalten (z. B. Name, Postanschrift, E-Mail-Adresse und Telefonnummer), Benutzername und Passwort, wenn Kunden sich auf unseren Websites anmelden.

Standardmäßig enthalten Mails an unsere Kunden einen Link zu unserer Einwilligungsplattform. Damit sind unsere Kunden jederzeit in der Lage Ihre Einwilligung in die Datenverarbeitung zu erweitern oder einzuschränken. Die Löschung der Kundendaten erfordert einen schriftlichen Löschauftrag an den Datenschutzbeauftragten.

Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung wird dann schriftlich von Seiten der iks Unternehmensgruppe dokumentiert uns auf Wunsch per E-Mail bestätigt.

Im Falle des Besuchs einer unserer Internetplattformen erfolgt die Einwilligung über das Double-Opt-in-Verfahren. Hierbei erhält der Besucher nach Eingabe seiner E-Mail-Adresse eine BestätigungsE-Mail auf der er nochmals durch Betätigung eines Links die Einwilligung zur Verarbeitung seiner Daten bekundet.

2.1.1.5 Werbezwecke

Bei vorliegender Einwilligung in die Datenverarbeitung erhalten Kunden von uns Information über unsere Dienstleistungen, aktuelle Angebote und Aktionen (Tag der offenen Tür, Weiterbildung, Marketing, Projekte etc.)

2.1.2 Vertragliche Beziehung

Eine vertragliche Beziehung beginnt in der Regel mit der Beauftragung ein Angebot über unsere Dienstleistungen zu erstellen und dauert während der Projektabwicklung an. Die Dauer der Einwilligung zur Datenverarbeitung richtet sich nach den gesetzlichen Vorgaben zur Aufbewahrung der während der vertraglichen

Beziehung angefallenen Daten.

Eine Besonderheit stellen Projekte im Rahmen der Arbeitnehmerüberlassung dar. Hier schreibt der Gesetzgeber die Übermittlung von personenbezogenen Daten an den Entleiher vor. Bei der Übermittlung von personenbezogenen Daten sind die Standards der Auftragsdatenverarbeitung einzuhalten.

2.1.2.1 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.

2.1.2.2 Aufgrund von berechtigtem Interesse

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der iks Unternehmensgruppe 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.

2.1.3 Datenspeicherung

Die Speicherung von Kundendaten erfolgt ausschließlich im dafür vorgesehenen ERP - System (Landwehr L1). Nicht anonymisierte Kundendaten sind aus dem E-Mail-System (Outlook o.Ä.) oder den Fileservern zu entfernen. Bei Umsetzung einer Datenlöschung oder eines Auskunftsersuchen muss der Datenschutzbeauftragte dem vollumfänglich nachkommen können.

2.1.4 Datenübermittlung

Die Übermittlung von Kundendaten erfolgt im Rahmen der Auftragsabwicklung und Rechnungslegung. Zu Teilen ist diese Datenübermittlung vom Gesetzgeber vorgeschrieben. Darüber hinaus werden Kundendaten bei folgenden Gesellschaften verarbeitet: Warenkreditversicherungen, Banken, Versicherungen, Wirtschaftsprüfer und Ankäufer von Forderungen. Mit allen diesen Gesellschaften wurden Auftragsdatenverarbeitungsverträge geschlossen.

2.1.5 Auskunftsrecht

Der Kunde hat die Möglichkeit zu erfahren, welche personenbezogenen Daten über ihn in der iks Unternehmensgruppe verarbeitet werden. Anfrage hierzu werden unter der E-Mail-Adresse dsb@iks-gruppe.de von unserem Datenschutzbeauftragten entgegengenommen.

2.1.6 Datenlöschung

Der Kunde hat grundsätzlich das Recht den Auftrag an die iks Unternehmensgruppe zu erteilen, seine Daten zu löschen. Hiervon sind alle Daten die einer gesetzlichen Aufbewahrungspflicht unterliegen, nicht betroffen. Löschaufträge werden unter der E-Mail-Adresse dsb@iks-gruppe.de von Datenschutzbeauftragten entgegen genommen.

2.1.7 Automatisierte Einzelentscheidung

Es ist durch entsprechende Unternehmensprozesse sichergestellt, dass automatisierte Einzelentscheidungen, wie z.B. die automatisierte Auswertung von Kreditwürdigkeits-informationen, die zum Ausschluss von Kunden führt, einer letzten manuellen Entscheidungsprozedur zugeführt wird.

2.2 Bewerberdaten

2.2.1 Datenerhebung

Die Datenerhebung wird grundsätzlich vom Bewerber aus initiiert, sei es durch Zusendung oder Aushändigung von Bewerbungsunterlagen, Besuch unserer Website, Plattformen oder Social-Media-Kanäle, durch Teilnahme an von uns organisierten Veranstaltungen oder via Telefon, SMS und Telefax oder in Verbindung mit persönlich geführten Interviews.

Wir speichern personenbezogene Daten gemäß der europäischen Datenschutz-Grundverordnung (DSGVO).

2.2.1.1 Bewerberplattform

Die iks Unternehmensgruppe betreibt auf ihrer Internetseite einen Stellenmarkt. Hier besteht die Möglichkeit sich auf ausgeschriebene Stellen zu bewerben. Der Stellenmarkt wird von einem Drittanbieter innerhalb der Bundesrepublik Deutschland betrieben. Die iks Unternehmensgruppe hat mit diesem Auftragsdatenverarbeiter einen Vertrag geschlossen. Die erhobenen Daten werden durch einen weiteren Auftragsdatenverarbeiter in unsere zentrale Datenbank übermittelt. Auch mit diesem Auftragsdatenverarbeiter wurde ein Vertrag geschlossen.

2.2.1.2 Automatisierte Verfahren

Wenn Sie unsere Websites besuchen, können wir bestimmte Daten mittels automatisierter Verfahren erheben, z.B. durch die Verwendung von Cookies, Web Beacons und Server-Protokoll- Dateien. Zu den Daten, die wir auf diesem Wege erheben können, gehören IP-Adresse, eindeutige Gerätekennung (UDI), Browsermerkmale, Gerätemerkmale, Betriebssystem, sprachliche Präferenzen, verweisende URL, Informationen über Handlungen auf unseren Websites, Datum und Zeitpunkt des Besuchs unserer Websites und sonstige Nutzungsstatistiken. Ein Cookie ist eine Textdatei, die beim Besuch einer Internetseite an den Computer oder ein anderes mit dem Internet verbundenes Gerät des Besuchers verschickt wird, um dessen Browser eindeutig zu identifizieren oder um Informationen und Einstellungen im Browser zu speichern. Ein „Web Beacon“, auch als Internet-Tag, Pixel-Tag oder transparentes GIF bekannt, verlinkt Webseiten mit Webservern und deren Cookies und dient der Übermittlung von durch Cookies erfassten Daten zurück an einen Webserver. Durch diese automatisierten Erhebungsverfahren erhalten wir „Clickstream- Daten“.

Hierbei handelt es sich um Logdaten der Links und sonstiger Inhalte, die ein Besucher beim Browsen auf einer Website anklickt. Während der Besucher sich durch die Website klickt, kann eine Aufzeichnung seiner Zugriffe erfolgen und gespeichert werden. Wir verlinken bestimmte Datenelemente, die wir mittels automatisierter Verfahren erhoben haben, z.B. Ihre Browserinformationen, mit anderen Informationen, die wir über Sie erhalten haben, um bspw. zu erkennen, ob Sie eine von uns an Sie gesendete E-Mail geöffnet haben. Ihr Browser ist eventuell so eingestellt, dass Sie eine Benachrichtigung erhalten, wenn bestimmte Arten von Cookies an Sie gesendet werden, oder er informiert Sie darüber, wie Sie die Akzeptanz bestimmter Arten von Cookies einschränken oder diese deaktivieren können. Bitte beachten Sie jedoch, dass Sie ohne Cookies möglicherweise nicht alle Funktionen unserer Websites nutzen können. Soweit dies nach geltendem Recht erforderlich ist, holen wir Ihre Zustimmung ein, bevor wir Ihre personenbezogenen Daten mittels Cookies oder ähnlicher automatisierter Verfahren erheben. Die Drittanbieter von Apps, Tools, Widgets und Plug-ins auf unseren Websites, wie bspw. Social Media Sharing Tools, können ebenfalls automatisierte Verfahren zur Erhebung von Daten bezüglich Ihrer Interaktionen mit diesen Funktionen verwenden. Diese Daten werden unmittelbar von den Anbietern dieser Funktionen erhoben und unterliegen den Datenschutzrichtlinien oder -hinweisen dieser Anbieter

Vorbehaltlich des geltenden Rechts ist die iks Unternehmensgruppe nicht verantwortlich für die Datenschutzpraktiken dieser Anbieter.

2.2.1.3 Einwilligung in die Datenverarbeitung

Mit Erhalt der Bewerbungsunterlagen beginnt der Bewerbungsprozess. Nach einer Sichtung werden die Bewerberdaten in das ERP-System übernommen. Gleichzeitig erhält der Bewerber eine E-Mail mit einem Link zu der Einwilligungsplattform der iks Unternehmensgruppe. Hier hat der Bewerber die Möglichkeit explizit in die Verarbeitung seiner personenbezogenen Daten einzuwilligen, bzw. kann die Verwendung seiner Daten erweitern, einschränken oder untersagen.

Der Link zu der Einwilligungsplattform bleibt über das ganze Bewerbungsverfahren hinweg gültig. Eine Änderung der Einwilligung ist jederzeit möglich.

In der Regel ist das Bewerbungsverfahren in einem Zeitraum von 6 Monaten abgeschlossen. Sollten sich weitere Aspekte ergeben, die eine Speicherung über den Zeitraum von 6 Monaten hinaus erforderlich machen, wird vom Bewerber eine Einwilligung zur Datenspeicherung für weitere 6 Monate angefordert. Erfolgt von Seiten des Bewerbers keine Reaktion auf eine Anfrage zur Verlängerung der Einwilligung zur Datenspeicherung werden die Daten nach einer Wartezeit von längstens 4 Wochen gelöscht.

2.2.2 Datenverarbeitung

2.2.2.1 Für die Bewerbung um einen Arbeitsplatz

Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden.

Das Bewerbungsverfahren bezieht sich auf die Stellenausschreibung auf die sich der Bewerber beworben hat. Das Bewerbungsverfahren endet mit der Absage oder mit dem Wegfall der Stellenausschreibung.

Der Bewerber hat die Möglichkeit der iks Unternehmensgruppe die Einwilligung zur Speicherung der personenbezogenen Daten für einen späteren Auswahlprozess zu erteilen. Die Einwilligung gilt für längstens 6 Monate und kann auf Wunsch des Bewerbers verlängert werden.

Die Einwilligung kann auch auf die Verwendung der Daten für alle offenen Stellenausschreibungen der iks Unternehmensgruppe erweitert werden.

2.2.2.2 Besonders schutzwürdige Daten

Besonders schutzwürdige personenbezogene Daten 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 Art der zu besetzende Stelle kann es erforderlich machen, solche Daten über den Bewerber zu verarbeiten, bevor es zur Gründung eines Arbeitsverhältnisses komm.

Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Bewerber kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

2.2.2.3 Automatisierte Entscheidung

Soweit im Bewerbungsverfahren personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für die Ablehnung des Bewerbers 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. Dem betroffenen Bewerber muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden

2.2.3 Datenübermittlung

Im Rahmen der regulären Geschäftstätigkeit der iks Unternehmensgruppe werden personenbezogene Daten an Kunden übermittelt, um deren freie Stellen, bzw. Projekte zu besetzen. Bei diesen Daten handelt es sich in der Regel um Bewerberprofile mit deren Hilfe die Kunden geeignete Bewerber oder Mitarbeiter zur temporären Übernahme von Projekten auswählen. Der Empfänger der Daten wird darauf verpflichtet, diese nur zu den festgelegten Zwecken zu verwenden und diese gegebenenfalls nach Aufforderung der iks Unternehmensgruppe zu löschen.

Die Einwilligung zur Datenübermittlung ist Teil der Einwilligung zur Datenspeicherung und kann über die Einwilligungsplattform erweitert oder eingeschränkt werden.

Bei der Übermittlung der Daten an Kunden sind die Standards unter Ziffer 3 einzuhalten.

2.2.4 Datenspeicherung

Die Speicherung von Bewerberdaten erfolgt ausschließlich im dafür vorgesehenen ERP - System (Landwehr L1). Nicht anonymisierte Bewerberdaten sind aus dem E-Mail-System (Outlook o.Ä.) oder den Fileservern zu entfernen. Bei Umsetzung einer Datenlöschung oder eines Auskunftsersuchen muss der Datenschutzbeauftragte dem vollumfänglich nachkommen können.

2.2.5 Datenlöschung

Nach Beendigung des Bewerbungsverfahrens sind die Daten unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt.

Die Speicherung von Bewerberdaten unterliegt in der iks Unternehmensgruppe der Genehmigungspflicht durch den Bewerber. Ist diese Genehmigung abgelaufen werden die Daten sofort gelöscht. Das bei der Löschung eines Bewerbers erstellte Löschprotokoll wird so anonymisiert, dass ein Rückschluss auf den Bewerber nicht mehr möglich ist.

Der Bewerber hat jederzeit die Möglichkeit die iks Unternehmensgruppe zu beauftragen, seine Daten zu löschen. Die Löschung kann über die Einwilligungsplattform durch den Bewerber initiiert werden. Alternativ kann der Löschauftrag an folgende E-Mailadresse: dsb@iks-gruppe.de geschickt werden.

2.2.6 Auskunftsrecht

Der Bewerber hat jederzeit das Recht zu erfahren, ob und in welchem Umfang personenbezogene Daten über ihn gespeichert sind. Fordern Sie die Auskunft unter folgender E-Mail-Adresse an: dsb@iks-gruppe.de.

2.3 Mitarbeiterdaten

2.3.1 Datenverarbeitung

2.3.1.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. 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 im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen erforderlich sind die jeweiligen 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.

2.3.1.2 Aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten 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. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden. Siehe § 147 AO, § 257 HGB, § 107 GewO.

2.3.1.3 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.

2.3.1.4 Aufgrund von berechtigtem Interesse

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der iks Unternehmensgruppe erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. Bewertung von Unternehmen) 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.

2.3.1.5 Besonders schutzwürdige Daten

Besonders schutzwürdige personenbezogene Daten 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 Gewerkschaftszuge-

hörigkeiten 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. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

2.3.1.6 Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne 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. Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

2.3.2 Datenübermittlung

Im Rahmen der regulären Geschäftstätigkeit der iks Unternehmensgruppe werden personenbezogene Daten an Kunden übermittelt, um deren freie Stellen, bzw. Projekte zu besetzen. Bei diesen Daten handelt es sich zum einen um Mitarbeiterprofile oder aber um gesetzlich vorgeschriebene personenbezogene Daten die zur Gründung eines Arbeitnehmerüberlassungsvertrages erforderlich sind. Der Empfänger der Daten ist im Vorfeld darauf verpflichtet worden, diese nur zu den festgelegten Zwecken zu verwenden und sie gegebenenfalls nach Aufforderung durch die iks Unternehmensgruppe zu löschen. Vor der Übermittlung der Daten sind die Standards unter Ziffer 3 einzuhalten.

2.3.3 Datenspeicherung

Die Speicherung von Mitarbeiterdaten erfolgt ausschließlich im dafür vorgesehenen ERP - System (Landwehr L1). Für die Abteilungen Lohnbuchhaltung, Finanzbuchhaltung, Marketing, Personalabteilung und Geschäftsführung ist zusätzlich ein, für personenbezogene Daten freigegebener, Fileserver vorgesehen.

Nicht anonymisierte Mitarbeiterdaten sind aus dem E-Mail-System (Outlook o.Ä.) oder den Fileservern zu entfernen. Bei Umsetzung einer Datenlöschung oder eines Auskunftsersuchen muss der Datenschutzbeauftragte dem vollumfänglich nachkommen können.

2.3.4 Auskunftsrecht

Jeder Mitarbeiter hat das Recht umfänglich über seine, bei der iks Unternehmensgruppe gespeicherten personenbezogenen Daten Auskunft zu erhalten. Die Einsicht in die Daten beantragen Sie unter folgender E-Mail-Adresse: dsb@iks-gruppe.de.

2.3.5 Datenlöschung

Nach § 257 Abs. 1 Nr. 1 und 4 HGB sind Personalakten sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen zehn Jahre aufzubewahren.

Nach der 10-Jahres-Frist werden die personenbezogenen Daten gelöscht, oder soweit anonymisiert, dass eine Rückverfolgung nicht oder nur unter Einsatz eines enormen Aufwandes durchgeführt werden kann.

3 Telekommunikation und Internet

Telefonanlagen, EMailAdressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung 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 Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden. Eine generelle Überwachung der Telefon und EMailKommunikation bzw. der Intranet und InternetNutzung findet nicht statt. Zur Abwehr von Angriffen auf die ITInfrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das iksNetz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der EMailAdressen, des Intranets und Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der iks Unternehmensgruppe erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen.

4 Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung 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 iks Unternehmensgruppe eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen.
Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten 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:

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
- Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
- Die vom Datenschutzbeauftragten bereitgestellten Vertragsstandards müssen beachtet werden.
- 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.
› Bei einer grenzüberschreitenden Auftragsdatenverarbeitung 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 Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:

a) Vereinbarung der EUStandardvertragsklauseln zur Auftragsdatenverarbeitung 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 DatenschutzAufsichtsbehörden.

5 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.

1. 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.

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

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

4. 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.

5. 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.

Darüber hinaus kann jeder Betroffene die in Datenschutzrichtlinie eingeräumten Rechte als Drittbegünstigter geltend machen, wenn ein Unternehmen, das sich zur Einhaltung der Datenschutzrichtlinie verpflichtet hat, deren Vorgaben nicht beachtet und er dadurch in seinen Rechten verletzt ist.

6 Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. 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 NeedtoknowPrinzip: Mitarbeiter haben 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 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 unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

7 Sicherheit der Verarbeitung

Personenbezogene Daten 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 ITSysteme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Der verantwortliche Fachbereich muß dazu insbesondere seinen IT-Sicherheitsbeauftragten (ISB) und Datenschutzkoordinator zu Rate ziehen.

Die technischorganisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des iks-weiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden

8 Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Datenschutzbeauftragten, den Datenschutzkoordinatoren und weiteren, mit Auditrechten ausgestatteten Unternehmensbereichen oder beauftragten externen Prüfern.

Die Geschäftsführer der iks Unternehmensgruppe und der angeschlossenen Tochterunternehmen sind 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.

9 Datenschutzvorfälle

Jeder Mitarbeiter soll seinem jeweiligen Vorgesetzten, seinem Datenschutzkoordinator oder dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden. Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, den zuständigen Datenschutzkoordinator oder den Datenschutzbeauftragten umgehend über Datenschutzvorfälle zu unterrichten.

In Fällen von unrechtmäßiger Übermittlung personenbezogener Daten an Dritte, unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder bei Verlust personenbezogener Daten sind die im Unternehmen vorgesehenen Meldungen (Information Security Incident Management) unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

10 Verantwortlichkeiten und Sanktionen

Die Geschäftsführungen der iks Unternehmensgruppe und ihrer Töchter sind verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie 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 der Datenschutzbeauftragte umgehend zu informieren.

Die jeweiligen Geschäftsführungen müssen dem Datenschutzbeauftragten einen Datenschutzkoordinator benennen. Organisatorisch kann diese Aufgabe in Konzernen auch durch einen Datenschutzkoordinator für mehrere Gesellschaften wahrgenommen werden. Die Datenschutzkoordinatoren sind vor Ort Ansprechpartner für den Datenschutz. Sie können Kontrollen durchführen und haben die Mitarbeiter mit den Inhalten der Datenschutzrichtlinien vertraut zu machen. Die jeweiligen Geschäftsführungen sind verpflichtet, den Datenschutzbeauftragten und die Datenschutzkoordinatoren in ihrer Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen die Datenschutzkoordinatoren rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

11 Der Datenschutzbeauftragte

Der Datenschutzbeauftragte als internes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der Datenschutzvorschriften hin.

Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Der Datenschutzbeauftragte wird von der Geschäftsführung der iks Unternehmensgruppe bestellt.

Die Datenschutzkoordinatoren unterrichten den Datenschutzbeauftragten unverzüglich über Datenschutzrisiken.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten oder an den für ihn zuständigen Datenschutzkoordinator wenden.

Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Kann der zuständige Datenschutzkoordinator einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzrichtlinien nicht abstellen, muss er den Datenschutzbeauftragten einschalten. Die Entscheidungen des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung sind durch die jeweiligen Geschäftsführungen zu berücksichtigen.

Anfragen von Aufsichtsbehörden sind immer auch dem Datenschutzbeauftragten zur Kenntnis zu bringen.