JOHNSON CONTROLS COMPLIANCE-RICHTLINIEN	REIHE NR. 140	ABFOLGE NR. 401-00

AUSGEGEBEN: Januar 2015 ÜBERARBEITET: Juni 2017 ZULETZT ÜBERPRÜFT: Juni 2017	THEMA: Datenschutzrichtlinie	Seite **1** von **9**
ABTEILUNG: Rechtsabteilung	ANSPRECHPARTNER: Ann Marie Barry, Chief Privacy Officer	GENEHMIGT VON: Judy Reinsdorf

GELTUNGSBEREICH

Unternehmen .....Ja
Geschäftsbereiche und Tochtergesellschaften in den USA .....Ja
Geschäftsbereiche und Tochtergesellschaften außerhalb der USA .....Ja
Konsolidierte Joint Ventures und verbundene Unternehmen .....Ja
Nicht konsolidierte Joint-Venture-Kooperationen .....**
**** Entscheidung obliegt Leitung der Geschäftseinheit**

EINFÜHRUNG

Diese Datenschutzrichtlinie sowie das zugehörige weltweite Datenschutzprogramm legen die Rechte von Mitarbeitern, Bewerbern, Praktikanten, ehemaligen Mitarbeitern, Angehörigen, Begünstigten, Auftragnehmern, Beratern, Leiharbeitnehmern, Kunden, Anwendern, Lieferanten und Anbietern dar und beschreiben die Pflichten von Johnson Controls hinsichtlich der Verarbeitung personenbezogener Daten (einschließlich der Erfassung, Nutzung, Aufbewahrung, Offenlegung und Vernichtung) im Einklang mit den einschlägigen lokalen Rechtsvorschriften und den Verpflichtungen aus der Johnson Controls-Ethikrichtlinie. „Personenbezogene Daten“, manchmal auch „persönlich identifizierende Informationen (PII)“ genannt, bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Diese Datenschutzrichtlinie legt dar, wie Johnson Controls den Datenschutz gewährleistet, und legt eine Datenschutzvision und -mission fest, aus denen wir vier grundlegende Datenschutzprinzipien ableiten. Diese wiederum werden mithilfe von 13 Datenschutz-Managementprozessen verwaltet, die im weltweiten Datenschutzprogramm verankert und an unseren bindenden Unternehmensregeln ausgerichtet sind.

UMFANG

Diese Richtlinie gilt für alle Standorte und juristischen Personen weltweit, die der Kontrolle von Johnson Controls unterliegen und die personenbezogene Daten verarbeiten.

RICHTLINIE UND VERPFLICHTUNGEN

Vision und Mission

Das Datenschutz-Credo von Johnson Controls lautet:

Im Einklang mit den geschäftlichen Anforderungen werden wir angemessene Maßnahmen zur Minderung der Datenschutz- und Sicherheitsrisiken von Johnson Controls ergreifen, die mit der Erfassung, Verwendung, Absicherung, Aufbewahrung, Verbreitung und Löschung von personenbezogenen Daten einhergehen.

Dieses Credo trägt zum Erreichen der Datenschutzvision von Johnson Controls bei:

dem fairen und gesetzeskonformen Umgang mit personenbezogenen Daten in der Obhut des Unternehmens.

Zentrale Datenschutzprinzipien

Die Datenschutzprinzipien von Johnson Controls lauten: Transparenz, Verhältnismäßigkeit, Kontrollen und lokale Rechtsvorschriften.

1. Transparenz und Fairness

Im Rahmen unserer globalen Betriebsprozesse informieren wir Kunden, Mitarbeiter, Lieferanten und Anwender auf angemessene Weise über den Zweck der Erhebung ihrer personenbezogenen Daten, welche Daten erfasst werden, wer sie verarbeitet und wo. Außerdem erfahren die betroffenen Personen, welche Rechte sie in Bezug auf die Verarbeitung ihrer personenbezogenen Daten haben, und werden auch sonst hinreichend informiert, sodass eine faire Verarbeitung gewährleistet ist. Zudem haben wir Prozesse eingerichtet, die es betroffenen Personen ermöglichen, ihre Rechte hinsichtlich der Kontrolle über ihre personenbezogenen Daten auszuüben. Darüber hinaus stellen wir die Richtigkeit der personenbezogenen Daten sicher und aktualisieren sie bei Bedarf.

2. Legitimer Zweck, Endgültigkeit und Verhältnismäßigkeit

Im Rahmen unserer Betriebsprozesse gelangen personenbezogene Daten nur zu Beteiligten, die sie für legitime, ausdrücklich definierte Zwecke benötigen. Die Daten werden im Einklang mit einschlägigen Gesetzen, ordnungsgemäß und sorgfältig erfasst oder verwendet. Wir stellen sicher, dass die personenbezogenen Daten adäquat und relevant sind und nur in dem Umfang erfasst werden, der für den vorgesehenen Zweck erforderlich ist. Des Weiteren gewährleisten wir durch entsprechende Maßnahmen, dass personenbezogene Daten nur so lange in einem identifizierbaren Format vorliegen, wie es der Zweck erfordert, für den sie erfasst oder weiterverarbeitet wurden.

3. Kontrollen und Überwachung

Unsere globalen Bereichsrichtlinien und -standards definieren vorbeugende Kontrollen einschließlich relevanter Sensibilisierungsschulungen. Damit wird sichergestellt, dass die physische und/oder digitale Erfassung, der Umgang mit, die Übertragung und die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutzrichtlinie erfolgt. Unsere Prozesse sorgen dafür, dass personenbezogene Daten durch angemessene technische und organisatorische Maßnahmen vor Zerstörung, Verlust, Abänderung, unbefugter Freigabe, unbefugtem Zugriff sowie allen anderen Arten der ungesetzlichen Verarbeitung geschützt sind, unabhängig davon, ob das Vorstehende versehentlich oder vorsätzlich geschieht. Zu diesen Maßnahmen zählen Verfahrensweisen für das Melden und Bearbeiten von (i) möglichen Datenschutzproblemen; (ii) Beschwerden; und (iii) Vorfällen im Zusammenhang mit der Informationssicherheit. Die jeweiligen Kontrollen werden angemessen überwacht, beispielsweise durch regelmäßige Audits der Verarbeitung von personenbezogenen Daten und den zugehörigen Prozessen.

4. Lokale Rechtsvorschriften

Wir verpflichten uns, an all unseren Wirkungsstätten die dort geltenden Rechtsvorschriften zum Datenschutz einzuhalten. Das bedeutet, wir erfassen und verwenden personenbezogene Daten nur im Einklang mit den einschlägigen lokalen Gesetzen.

Vertrauliche personenbezogene Daten werden nur bei Bedarf und nötigenfalls mit dem Einverständnis der betreffenden Person verwendet. Darüber hinaus legen wir für bestimmte behördliche Administrationsabläufe den jeweils Datenverantwortlichen eindeutig fest.

Bindende Unternehmensregeln

Johnson Controls hat bindende Unternehmensregeln eingeführt, die an dieser Datenschutzrichtlinie ausgerichtet sind und die mithilfe einer konzerninternen Vereinbarung durchgesetzt werden. Die konzerninterne Vereinbarung gilt verpflichtend für alle juristischen Personen, über die Johnson Controls administrative Kontrolle hat. „Johnson Controls International SA/NV“ mit Sitz in Belgien hat die Verantwortung über die Einhaltung dieser bindenden Unternehmensregeln übernommen. Für die Abstimmung zu diesen Regeln mit den Datenschutzbehörden ist der Chief Privacy Officer zuständig.

Die bindenden Unternehmensregeln stehen auf der offiziellen Johnson Controls-Website sowie im Datenschutzportal für Mitarbeiter zur Verfügung.

Datenschutz-Managementprozesse

Die Aktivitäten im Rahmen des weltweiten Datenschutzprogramms gliedern sich in **13 Datenschutz-Managementprozesse**. Sie bilden die Grundlage zur Ermittlung des Reifegrads von Johnson Controls sowie zur Organisierung von Datenschutzprüfungen.

1. **Pflege einer Governance-Struktur für den Datenschutz und klare Verantwortlichkeiten:** Es sind für den Datenschutz verantwortliche Mitarbeiter und rechenschaftspflichtige Führungskräfte festzulegen sowie Verfahren zur Meldung an Vorgesetzte einzuführen. Die Verantwortlichkeiten sind nachstehend in dieser Richtlinie definiert.

2. **Führen eines Verzeichnisses über personenbezogene Daten:** Über den Speicherort wesentlicher personenbezogener Daten und sämtlichen Verkehr mit personenbezogenen Daten ist ein Verzeichnis zu führen. Dabei sind die personenbezogenen Daten in definierte Kategorien zu unterteilen.

3. **Pflege der Datenschutzrichtlinie:** Die Datenschutzrichtlinie muss den gesetzlichen Anforderungen entsprechen und das betriebliche Risiko berücksichtigen.

4. **Einbettung des Datenschutzes in betriebliche Richtlinien und Verfahren:** Die betrieblichen Richtlinien und Verfahren müssen im Einklang mit der Datenschutzrichtlinie, den gesetzlichen Vorschriften und den Zielen für das betriebliche Risikomanagement stehen.

5. **Organisierung von Datenschutzschulungen und Sensibilisierung für das Thema:** Es sind fortlaufend Schulungen bereitzustellen und Sensibilisierungsmaßnahmen zu ergreifen, um die Einhaltung der Datenschutzrichtlinie zu unterstützen und betriebliche Risiken zu minimieren.
6. **Management von Datensicherheitsrisiken:** Ein Datensicherheitsprogramm auf Grundlage der gesetzlichen Vorschriften ist zu erstellen. Darüber hinaus müssen fortlaufend Risikobewertungen vorgenommen werden.
7. **Management von Drittpartei-Risiken:** Mit Drittparteien und verbundenen Unternehmen sind Verträge und Vereinbarungen im Einklang mit der Datenschutzrichtlinie, den gesetzlichen Vorschriften und entsprechend der Toleranz für betriebliche Risiken zu schließen.
8. **Pflege von Mitteilungen:** Bei Mitteilungen an Personen müssen die Datenschutzrichtlinie, die gesetzlichen Vorschriften und die Toleranz für betriebliche Risiken berücksichtigt werden.
9. **Pflege von Anfrage- und Beschwerdeverfahren:** Es sind effektive Verfahrensweisen für Interaktionen mit Personen über ihre personenbezogenen Daten einzuführen.
10. **Prüfung auf neue betriebliche Verfahrensweisen:** Die betrieblichen Verfahrensweisen sind zu beobachten, um neue Prozesse oder wesentliche Änderungen an bestehenden Vorgehensweisen zu erkennen und die Einhaltung des Grundsatzes „eingebauter Datenschutz“ (Privacy by Design) zu gewährleisten.
11. **Pflege von Verfahren bei Datenschutzverletzungen:** Für Verstöße gegen die Datenschutzprinzipien müssen effektive Verfahren eingesetzt und gepflegt werden.
12. **Überwachung der betrieblichen Praxis im Umgang mit Daten:** Es ist zu prüfen, ob die betriebliche Praxis der Datenschutzrichtlinie sowie betrieblichen Richtlinien und Verfahrensweisen entspricht.
13. **Regelmäßige Prüfung externer Kriterien:** Es ist regelmäßig zu prüfen, ob neue Anforderungen, Erwartungen und Best Practices hinsichtlich der Compliance bestehen.

Verantwortungsbereiche

1. Der **Chief Ethics & Compliance Officer** (Leiter Ethik und Compliance) ist verantwortlich für das weltweite Datenschutzprogramm und fungiert dafür als Sponsor. Er hat das Datenschutzprogramm jährlich zu überprüfen, für kontinuierliche Verbesserungen zu sorgen und den Compliance-Fortschritt dem Executive Compliance Council sowie dem Governance Committee of the Board of Directors zu melden. Das weltweite Datenschutzprogramm ist Bestandteil des Ethik- und Compliance-Programms von Johnson Controls.

2. Das **Privacy Office** (Datenschutzbüro) ist für die Abläufe des weltweiten Datenschutzprogramms zuständig und hat sicherzustellen, dass die Ziele und betrieblichen Vorgaben des Programms erreicht werden und dass die Programminhalte effektiv innerhalb des Unternehmens kommuniziert werden. Darüber hinaus muss das Privacy Office dafür sorgen, dass die Mitglieder der Global Privacy Community (weltweite Datenschutzgemeinde) ordnungsgemäß in das weltweite Datenschutzprogramm eingebunden sind. Das Privacy Office hat angemessene Kommunikationsplattformen für die Global Privacy Community bereitzustellen, um den Austausch von Best Practices und den Zugriff auf datenschutzrelevante Ressourcen zu ermöglichen.
    a. Das Privacy Office setzt sich zusammen aus:
        i. dem Chief Privacy Officer;
        ii. dem Privacy Program Leader und den Privacy Program Managern; und
        iii. den Privacy Counsels.
    b. Der **Chief Privacy Officer** (Datenschutzbeauftragter) hat die Aufgabe, Orientierungshilfen zum weltweiten Datenschutzprogramm zu geben, für die Einhaltung geltender Vorschriften zu sorgen und organisatorische Anforderungen im Einklang mit geltenden lokalen und internationalen rechtlichen Vorschriften sowie dem weltweiten Datenschutzprogramm von Johnson Controls festzulegen. Der Chief Privacy Officer ist der konzernweite Leiter des weltweiten Datenschutzprogramms und in dieser Rolle verantwortlich für die Pflege der bindenden Unternehmensregeln und die Zusammenarbeit mit den zuständigen Behörden. Der Chief Privacy Officer muss den Chief Ethics & Compliance Officer und die obere Geschäftsführung regelmäßig über die Aktivitäten und die Wirksamkeit des Programms informieren.
    c. Die **Privacy Program Leader und Manager** (Leiter und Manager des Datenschutzprogramms) sind verantwortlich für die Organisation der Aktivitäten für das weltweite Datenschutzprogramm im Einklang mit den in Abschnitt 6 beschriebenen Datenschutz-Managementprozessen. Darüber hinaus werden sie auch als Projektmanager für das Programm fungieren.
    d. Die **Privacy Counsels** (Rechtsberater für den Datenschutz) sind verantwortlich für die rechtliche Beratung in Bezug auf die Datenschutzgesetze und -bestimmungen in ihren jeweiligen Regionen.
3. Die **Privacy Community** setzt sich zusammen aus den Mitgliedern des Privacy Office, den Data Privacy Officers (Datenschutzverantwortliche), den Local Data Privacy Coordinators (lokale Datenschutzkoordinatoren), den Subject Access Request Coordinators (Koordinatoren für den Antrag auf Offenlegung der gespeicherten Daten) und anderen Mitgliedern, die das Privacy Office bei Bedarf anfordert.
4. Die **Data Privacy Officers (DPO)** sind für die Einhaltung lokal geltender Datenschutzbestimmungen im Einklang mit dem weltweiten Datenschutzprogramm von Johnson Controls für eine bestimmte geografische Region, eine Geschäftseinheit und/oder eine Gruppe von juristischen Personen (nachfolgend „Geschäftsbereich“ genannt) verantwortlich, müssen entsprechende Maßnahmen koordinieren und über die Compliance Bericht erstatten.

Der DPO untersteht der Geschäftsführung der örtlichen Gesellschaften und dem Chief Privacy Officer (Dotted-Line-Prinzip). Zur Einhaltung lokaler gesetzlicher Anforderungen werden DPOs ernannt. Überall dort, wo DPOs keine Pflicht sind, kann Johnson Controls nach eigenem Ermessen DPOs ernennen. DPOs fungieren als Hauptansprechpartner für die örtliche Datenschutzbehörde. DPOs müssen über ausreichende Fachkenntnisse hinsichtlich der geltenden Datenschutzverordnung in ihrem Geschäftsbereich verfügen. Die DPO-Funktion kann zusätzlich zu einer anderen Rolle innerhalb von Johnson Controls ausgeübt werden, sofern durch beide Rollen kein Interessenkonflikt entsteht.

5. Die **Local Data Privacy Coordinators (LDPC)** sind für die Einhaltung lokal geltender Datenschutzbestimmungen im Einklang mit dem weltweiten Datenschutzprogramm von Johnson Controls für einen Geschäftsbereich verantwortlich, müssen entsprechende Maßnahmen koordinieren und über die Compliance Bericht erstatten. LDPCs sind Teil der Privacy Community und unterstützen das Privacy Office bei Datenschutz-Compliance-Aktivitäten in ihrem Geschäftsbereich. Eine solche LDPC-Rolle kann in Regionen eingesetzt werden, in denen die Ernennung eines offiziellen DPO nicht erforderlich ist.

6. Die **Subject Access Request Coordinators (SAR-Koordinatoren)** sind verantwortlich für den Empfang, die Koordination und die Beantwortung von Anträgen auf Offenlegung der gespeicherten Daten im Einklang mit lokalen Gesetzen und in Abstimmung mit dem zuständigen Privacy Counsel.

7. **Geschäftsleiter und Funktionsträger** haben sicherzustellen, dass ihre spezifischen Aktivitäten, Prozesse und Richtlinien innerhalb ihrer Geschäftseinheit(en), ihrer Region oder ihrem Zuständigkeitsbereich dem weltweiten Datenschutzprogramm einschließlich der Datenschutzrichtlinie und den bindenden Unternehmensregeln entsprechen.
    a. Der **Vice President Human Resources** (Vizepräsident Personal) ist verantwortlich für den Schutz von Mitarbeiterdaten und für mitarbeiterbezogene Prozesse.

    b. Der **Chief Information Technology Officer** (Leiter IT) hat die Aufgabe, Support für das weltweite Datenschutzprogramm zu liefern, und muss sicherstellen, dass die IT-Prozesse im Einklang mit dem weltweiten Datenschutzprogramm stehen.

    c. Der **Vice President of Internal Audit** (Vizepräsident interne Revision) ist dafür verantwortlich, Input und Ressourcen für das Programm zur Verfügung zu stellen und den Auditprozess des weltweiten Datenschutzprogramms zu unterstützen.

d. Der **Chief Information Security Officer** (Leiter Informationssicherheit) hat die Aufgabe, IT-Richtlinien und -Kontrollen im Einklang mit dem weltweiten Datenschutzprogramm zu erstellen.

Kontinuierliche Verbesserung

Das Privacy Office muss die Datenschutzrichtlinie regelmäßig überprüfen, um sicherzustellen, dass sie im Hinblick auf Änderungen der Datenschutzvorschriften und -gesetze, das Geschäft von Johnson Controls und neue Technologien auch weiterhin angemessen ist.

Datenschutzdokumentation

Das Privacy Office dokumentiert sämtliche Aktivitäten rund um das weltweite Datenschutzprogramm und übernimmt die Pflege von mit dem Programm zusammenhängenden Richtlinien und Verfahrensweisen und stellt sie den entsprechenden Zielgruppen zur Verfügung. Offizielle Dokumente werden auf der öffentlichen Website von Johnson Control veröffentlicht, interne Dokumente für Mitarbeiter werden im Datenschutzportal für Mitarbeiter zur Verfügung gestellt. Für die Privacy Community bestimmte Dokumente werden in einem strukturierten und sicheren Repository gespeichert.

Datenschutzaudits

Das Privacy Office unterstützt das Team der internen Revision bei der Einhaltung des Datenschutz-Auditprotokolls und bei der Durchführung jährlicher Datenschutzprüfungen gemäß dem vereinbarten Protokoll.

Die örtliche Führungsebene der überprüften Standorte, der lokale Ansprechpartner für den Datenschutz (DPO, LDPC, Datenverantwortliche der Personalabteilung), der Vice President of Internal Audit, der Chief Privacy Officer und der Chief Ethics & Compliance Officer werden über die Ergebnisse des Audits informiert. Sie sind dafür verantwortlich, gegebenenfalls notwendige Maßnahmen einzuleiten.

Nichteinhaltung

Alle Mitarbeiter von Johnson Controls müssen die in der Datenschutzrichtlinie beschriebenen Grundsätze, die entsprechenden Bestimmungen der bindenden Unternehmensregeln und die zugehörigen Richtlinien und Verfahrensweisen einhalten.

Die Nichteinhaltung der Datenschutzrichtlinie von Johnson Controls stellt einen Verstoß gegen die Ethikrichtlinie dar. Verstöße gegen die Ethikrichtlinie werden mit disziplinarischen Maßnahmen bis hin zur Kündigung geahndet.

Referenzen

a. Johnson Controls-Verhaltenskodex
b. Datenschutzerklärung zu personenbezogenen Daten für Mitarbeiter
c. Offizielle Datenschutzerklärung
d. Richtlinie zu den Datenschutzrechten der betroffenen Personen
e. Bindende Unternehmensregeln