

## Technische und organisatorische Maßnahmen bei Auftragsdatenverarbeitung gemäß §§ 9, 11 Abs. 3 Nr. 3 Bundesdatenschutzgesetz (BDSG)

Die Daten werden in einem Rechenzentrum der Bisnode Informatics Deutschland GmbH, Havelstraße 9, Darmstadt (Schwestergesellschaft der Hoppenstedt360 GmbH), verarbeitet. Folgende Sicherungsmaßnahmen sind getroffen:

### I. Zutrittskontrolle

*Ziel: Unbefugten den räumlichen Zutritt verwehren*

Der Zutritt in das Gebäude wird durch spezielle Zugangschips, die individuell für jeden einzelnen Mitarbeiter frei geschaltet werden, geregelt. Zutritt erhalten nur Mitarbeiter, die zur Ausübung Ihrer Tätigkeit den Zutritt benötigen. Angelegt und frei geschaltet werden die Zutritte in der Personalabteilung. Für jeden Mitarbeiter gibt es eine Standard-Zutrittsberechtigung für die allgemeinen Eingänge zum Gebäude. Spezielle Berechtigungen (z.B. zum Rechenzentrum oder zum Druckerraum) werden ausschließlich nach Rücksprache mit und auf Weisung des entsprechenden Vorgesetzten des Mitarbeiters erteilt.

### II. Zugangskontrolle

*Ziel: Verhinderung des Eindringens Unbefugter in IT-Systeme*

Der Zugang zu Systemen erfolgt über Login-Name und Passwort. Einen Login zu den entsprechenden Systemen erhalten nur Mitarbeiter, die zur Ausübung Ihrer Tätigkeit diesen Zugang benötigen. Die Zugänge werden schriftlich beantragt und durch die verantwortliche Person für dieses System genehmigt. Erteilt werden die Zugänge durch die Systemadministratoren. Der schriftliche Antrag mit Genehmigung wird archiviert. Es finden regelmäßige Prüfungen statt, bei der die vorhandenen Zugänge eines jeden Mitarbeiters auf Notwendigkeit überprüft werden. Wenn ein Mitarbeiter einen bestimmten Zugang zur Ausübung seiner Tätigkeit nicht mehr benötigt (z.B. bei einem Abteilungswechsel oder Beendigung des Arbeitsverhältnisses), werden die entsprechenden Zugänge deaktiviert.

### III. Zugriffskontrolle

*Ziel: Verhinderung unerlaubter Tätigkeit in IT-Systemen außerhalb eingeräumter Berechtigungen*

Die Zugriffskontrolle erfolgt durch spezielle Passwörter und Berechtigungen, die individuell vergeben werden. Zugriff erhalten nur Mitarbeiter, die zur Ausübung Ihrer Tätigkeit diesen entsprechenden Zugriff auch benötigen. Antrags- und Prüfungsverfahren: wie unter Ziffer II (Zugangskontrolle) beschrieben.

### IV. Weitergabekontrolle

*Ziel: Gesicherte Weitergabe personenbezogener Daten (elektronische Übertragungen, Datentransport, Übermittlungskontrolle)*

Die Weitergabe (Empfang vom Kunden, Lieferung an Kunden) der Daten wird durch die Protokollierung der Datenverarbeitung gewährleistet. Des Weiteren werden die Daten, falls entsprechend vereinbart, mit einer verschlüsselten Datenübertragung gesichert. Die genaue Art der Datenübertragung wird in jedem Einzelfall mit dem Kunden vereinbart.

### V. Eingabekontrolle

*Ziel: Prüfbarkeit der eingegebenen, veränderten und entfernten Daten*

Eine Eingabe kann nur durch die Mitarbeiter erfolgen, die Zugriff auf die Daten haben (siehe Ziffer II, Zugangskontrolle). Je nach Funktion des Mitarbeiters werden die Zugriffe differenziert vergeben (z.B. nur Leserechte, nur Korrekturrechte usw.). Das Eingeben, Verändern und Entfernen wird automatisch protokolliert und kann im Einzelfall nachvollzogen werden.

### VI. Auftragskontrolle

*Ziel: Gewährleistung einer weisungsgemäßen Auftragsdatenverarbeitung*

Die Auftragskontrolle ist durch die automatischen Prozesse gewährleistet. Die Prozesse sind zwischen Auftraggeber und Auftragnehmer vereinbart und abgenommen. Alle Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind auf das Datengeheimnis nach § 5 BDSG verpflichtet. Änderungen und Neuerungen im Bereich des BDSG werden den Mitarbeitern in geeigneter Form mitgeteilt.

### VII. Verfügbarkeitskontrolle

*Ziel: Schutz der Daten gegen zufällige Zerstörung und Verlust*

Die Verfügbarkeitskontrolle wird durch regelmäßige Datensicherung und Backups der entsprechenden Datenbanken und Systeme gewährleistet. Für den Fall eines Stromausfalles besteht eine Notstromversorgung. Zum Schutz der Systeme existieren Firewalls, regelmäßige System-Updates und weitere Schutzmaßnahmen wie etwa Virens Scanner.

### VIII. Trennungsgebot

*Ziel: Gewährleistung getrennter Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten*

Alle gelieferten Datenpakete werden voneinander getrennt bearbeitet, so dass eine Überschneidung von Kundendaten ausgeschlossen ist. Hierzu sind entsprechende hardwaretechnische Vorkehrungen getroffen.

### IX. Datenschutzbeauftragte

*Als Beauftragte für den Datenschutz gemäß § 4f BDSG ist bei Hoppenstedt360 bestellt:*

Frau Désirée Giesen, c/o Bisnode Deutschland Holding GmbH, Havelstraße 9, 64295 Darmstadt, Telefon: 06151/380-821, Telefax: 06151/380-99821, E-Mail: datenschutz@bisnode.de.

Stand: 14. November 2011

Hoppenstedt360 GmbH | Havelstraße 9 | 64295 Darmstadt