Technische und organisatorische Maßnahmen gemäß Anlage zu § 9 BDSG

Verantwortliche Stelle:	Niedling & Partner Bürotechnik GmbH Grondahlsmühle 10 53881 Euskirchen
Leiter der verantwortlichen Stelle:	Peter Niedling, Geschäftsführender Gesellschafter Guido Niedling, Geschäftsführender Gesellschafter
Leiter der Datenverarbeitung:	Joachim Kontny
Datenschutzbeauftragter:	Reinhold Goetz
Stand:	1.9.2015

0. Organisationkontrolle

- ❑ Als externer Datenschutzbeauftragter wurde Herr Reinhold Goetz bestellt. Herr Goetz verfügt über eine Ingenieurausbildung im IT-Bereich hat seine datenschutzrechtliche Qualifikation über entsprechende Zertifikate nachgewiesen.
- ❑ Alle Mitarbeiter der verantwortlichen Stelle und alle externen Dienstleister bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann sind schriftlich auf das Datengeheimnis gem. § 5 BDSG verpflichtet.
- ❑ In internen Dienstanweisungen und IT-Nutzungsrichtlinien werden Regeln für den Umgang mit personenbezogenen Daten und die IT-Nutzung vorgegeben.
- ❑ Die Einhaltung der Dienstanweisungen wird durch den Leiter der verantwortlichen Stelle stichprobenartig überprüft.
- ❑ Die Mitarbeiter der verantwortlichen Stelle werden bei Bedarf, mindestens jedoch einmal jährlich durch den Datenschutzbeauftragten im Rahmen einer Präsenzschulung auf die datenschutzrechtlichen Anforderungen hingewiesen. Die Unterweisungen werden dokumentiert.
- ❑ Der Datenschutzbeauftrage überprüft bei Systemveränderungen die einen Einfluss auf die Verarbeitung personenbezogener Daten haben, spätestens jedoch nach Ablauf eines Jahres, im Rahmen einer Bestandsaufnahme die Einhaltung aktueller Datenschutzbestimmungen.
- ❑ Personenbezogene Datenverarbeitungen bei denen die Gefahr besteht, dass das Persönlichkeitsrecht eines Einzelnen verletzt wird, z.B. durch eine Videoüberwachung, GPS-Ortung etc., wird eine Vorabkontrolle durch den Datenschutzbeauftragten durchgeführt. Das Ergebnis der Vorabkontrolle wird dokumentiert.

1. Zutrittskontrolle

Lage der Betriebsstätte:

Die Betriebsstätte befindet sich in einem Mischgebiet in Euskirchen-Kuchenheim. Im Gebäude selber befindet sich auch die Privatwohnung eines Gesellschafters.

- ❑ Der Geschäftsbereich befindet sich im Erd- und Obergeschoss des Gebäudes
- ❑ Über die Gebäudezugänge (Haupt- und Nebeneingang) kann auch der Geschäftsbereich erreicht werden. Alle Zugangstüren zum Gebäude sind grundsätzlich verschlossen.
- ❑ Besucher nutzen die Klingel am Haupteingang. Die Türöffnung erfolgt manuell durch einen Mitarbeiter. Ein unbefugter oder unbemerkter Zugang zum Geschäftsbereich ist damit ausgeschlossen.
- ❑ Es befinden sich keine Schlüssel bei betriebsfremden Personen
- ❑ Alle Schlüsselinhaber werden in einer Schlüsselliste geführt. Die Schlüsselinhaber haben beim Schlüsselerhalt eine schriftliche Belehrung zur Aufbewahrung erhalten, d.h. keine Kennzeichnung der Schlüssel und unmittelbare Mitteilung an die Geschäftsleitung bei Schlüsselverlust
- ❑ Die Reinigung der Büroräume erfolgt während der Geschäftszeiten durch eine festangestellte Mitarbeiterin. Eine Vertretung ist intern organisiert, so dass keine betriebsfremden Reinigungskräfte die Büroräume betreten.
  Ausnahme: Fensterreinigung erfolgt während der Geschäftszeiten unter Aufsicht.
- ❑ Besucher betreten die Büroräume nur in Begeleitung eines Mitarbeiters
- ❑ Alle Mitarbeiter wurden im Rahmen einer Datenschutzunterweisung darauf hingewiesen, dass sie verpflichtet sind, personenbezogene und vertrauliche Daten vor unberechtigten Zugriff zu schützen und betriebsfremde Personen nicht unbeaufsichtigt zu lassen.
- ❑ Alle betriebsfremden Servicedienstleister (Fensterreinigung etc.) arbeiten nur bei Anwesenheit von min. einem Mitarbeiter und haben eine schriftliche Verpflichtungserklärung zum Datenschutz abgeben.

Sicherheitsmaßnahmen:

- ❑ Alle Türen und Fenster im Erdgeschoß sind vergittert
- ❑ Die Außentüren sind einbruchsicher und mit doppelten Schließzylindern ausgestattet, die Schließzylinder sind aufbohr- und ausziehsicher.
- ❑ Schlüsselkopien können nur unter Vorlage des Sicherheitszertifikats beim Hersteller erzeugt werden. Das Zertifikat befindet sich bei der Geschäftsleitung.
- ❑ Das eingezäunte Grundstück wird ganztags von zwei Wachhunden bewacht
- ❑ Im Gebäude sind verknüpfte Rauchmelder installiert, die einen Innenalarm auslösen.
- ❑ Die Zentralrechner (Server) befinden sich in einem verschlossenen und klimatisierten Schrank und sind nur einem autorisierten Personenkreis zugänglich, die Schlüsselinhaber werden in einer Schlüsselliste geführt.

2. Zugangskontrolle

- ❑ Die Systemnutzung ist hierarchisch aufgebaut. Jede Anmeldung, d.h. lokal, Domaine und CRM erfolgt über eine individuelle und geheime Anmeldung mit Name und verschiedenen Passwörtern. Die Passworte sind geheim und werden an keiner Stelle im Klartext gespeichert.
- ❑ Jeder Nutzer hat die Möglichkeit, sein Passwort in den einzelnen Systembereichen und Anwendungsprogrammen selbst zu ändern.
- ❑ Die Mitarbeiter werden regelmäßig im Rahmen einer Datenschutzunterweisung über die Notwendigkeit der Passwortkonventionen unterrichtet und sind angehalten, diese auch anzuwenden. Alle Passwörter bestehen aus Buchstaben, Zahlen und mind. einem Sonderzeichen und werden regelmäßig geändert.

- Die Passwortkonventionen, d.h. mindestens 10 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen und die Gültigkeit wird sofern möglich vom Betriebssystem bzw. von den Anwendungen eingefordert.
- Administrationspassworte sind nur dem zuständigen Mitarbeiter bekannt. Für den Notfall werden diese verschlüsselt gespeichert und können nur von der Geschäftsleitung entschlüsselt werden.
- Auf den fest installierten Arbeitsplätzen befinden sich keine schutzwürdigen oder personenbezogene Daten. Auf den Notebooks der Techniker befinden sich nur temporär Kundendaten. Aus diesem Grund sind die Notebooks alle vollständig verschlüsselt.
- Auf allen Arbeitsplätzen ist ein passwortgeschützter Bildschirmschoner aktiviert, der sich nach Ablauf einer Zeit, max. 15min., automatisch einschaltet. Damit wird eine unbefugte Nutzung bei Abwesenheit des Mitarbeiters verhindert.
- Der Internetzugang erfolgt über eine UTM mit integrierter Firewall, dynamischen Content-Filter und mehrstufigem Virenschutz.
- Die Konfiguration der lokalen Firewall ist nur einem autorisierten Personenkreis möglich.
- Die Aktualisierung der Sicherheitspatches für die Betriebssysteme erfolgt automatisch.
- Die Techniker bzw. Telearbeiter verfügen über eine Einwahlmöglichkeit in das Firmennetzwerk. Die Einwahl erfolgt über eine zertifikatsbasierte VPN-Verbindung.
- Die Telearbeiter haben eine schriftliche Vereinbarung zur Nutzung der Telearbeitsplätze unterzeichnet, darin sind alle Verhaltensregeln im Umgang mit schutzwürdigen und personenbezogenen Daten beschrieben.
- Alle von den Telearbeitern genutzten Geräte sind Eigentum der verantwortlichen Stelle und werden ausschließlich dienstlich genutzt.

Fernwartung:

Der Fernzugriff zu Wartungszwecken auf die Kundennetze erfolgt je nach Zweck auf unterschiedliche Weise:

- Fernzugriff auf die Routerkonfiguration

  Die Routerkonfiguration kann per Fernzugriff zu Wartungszwecken, beispielsweise für notwendige Sicherheitsupdates, Änderung des autorisierten Personenkreises, VPN-Zugänge etc., verändert werden. Die Berechtigung für die Änderung der Routerkonfiguration hat nur ein eingeschränkter Personenkreis (Leitung). Jede Änderung in der Routerkonfiguration wird mit Name und Zeitstempel protokolliert, so dass jederzeit nachvollziehbar ist, wer, wann, welche Änderungen an der Routerkonfiguration vorgenommen hat.

- Fernzugriff auf die Server

  Der Fernzugriff erfolgt ausschließlich über eine automatische und personalisierte Einwahlprotokollierung (Techniker bezogen). Jeder Techniker besitzt nur die Einwahlberechtigungen für die von ihm betreuten Kundennetzwerke. Die Zugangsdaten sind individuell und werden von einem eingeschränkten Personenkreis (Leitung) verwaltet. Jede Ein- und Auswahl in ein Kundennetzwerk wird mit Zeitstempel und Username automatisch per E-Mail an eine vom Kunden festgelegte E-Mailadresse gemeldet. Durch diese Maßnahme wird ein unbemerkter und unautorisierter Fernzugriff auf das Kundennetzwerk verhindert.

  Alle Techniker sind verpflichtet die gesamte Fernsteuersitzung als Videomitschnitt aufzuzeichnen und auf einem Zentralserver bei der *Niedling & Partner GmbH* abzulegen. Die Techniker haben nur die Befugnis auf Systemdaten zuzugreifen,

der Zugriff auf Anwendungs- oder Kundendaten ist untersagt. Die Überwachung erfolgt turnusmäßig in Stichproben durch einen externen Datenschutzbeauftragten. Der Videomitschnitt erfolgt revisionssicher und wird zwei Jahre lang aufbewahrt. Die Videoaufzeichnungen werden dem Kunden auf Wunsch zu Verfügung gestellt. Durch diese Maßnahme ist jeder Fernzugriff vollumfänglich für den Kunden nachvollziehbar.

- ❑ Fernsteuerung der Arbeitsplätze

  Eine Fernsteuerung der Arbeitsplätze erfolgt nur unter Aufsicht und Zustimmung des Kunden. Für die Fernsteuerung wird das Programm FastViewer eingesetzt. Für jede Fernsteuersitzung wird eine neue Sitzungs-ID durch den ferngesteuerten Arbeitsplatz vergeben. In diesem Falle erfolgt kein Mitschnitt, da der ferngesteuerte Arbeitsplatz alle Bedienungen am Bildschirm mitverfolgen kann und die Fernsteuersitzung jederzeit beenden kann.

Umgang mit Digitalkopierern beim Kunden:

- ❑ Die Administrationspasswörter werden bei der Ersteinrichtung auf ein individuelles Passwort abgeändert, dass nur den Technikern und dem Kunden bekannt ist
- ❑ Auf den netzwerkfähigen Digitalkopierern sind nur die notwendigen Dienste und Protokolle, in der Regel nur TCP/IP, aktiviert.
- ❑ Im Netzwerk angeschlossene Digitalkopierer werden im Rahmen der Wartung mit den sicherheitsrelevanten Updates des Herstellers ausgestattet, alle anderen Updates nur bei Bedarf bzw. auf Kundenwunsch.
- ❑ Nicht flüchtige Speicher (Flash oder Festplatten) in den Geräten werden vor der Entsorgung mechanisch zerstört oder datenschutzkonform formatiert, so dass eine Wiederherstellung der Daten ausgeschlossen ist.

3. Zugriffskontrolle

- ❑ Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Programme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.
- ❑ Das Kopieren von Daten ist nur im Rahmen der Datensicherung und für die besonders geregelten Fälle der Datenweitergabe erlaubt, z.B. notwendiger Datenaustausch mit Kunden.
- ❑ Alle Notebooks sind zum Schutz vertraulicher oder personenbezogener Daten vollständig verschlüsselt. Damit wird ein Zugriff Unbefugter auf die Daten verhindert.
- ❑ Schutzwürdige Daten auf USB-Sticks werden in einem verschlüsselten Bereich abgelegt (DataSafe auf myDentity-Sticks der DATEV)
- ❑ Die Administrationsrechte für das interne Firmennetz hat nur ein eingeschränkter Personenkreis
- ❑ Das Netzwerk ist vollständig dokumentiert.

4. Weitergabekontrolle

- ❑ Die Authentifizierung für das Online-Banking über eine HBCI-Karte, die auf einen Geschäftsführer ausgestellt ist.
- ❑ Jeder Mitarbeiter besitzt für seinen Email-Account eine SmartCard der DATEV mit Zertifikat, das für eine Verschlüsselung und digitale Signatur verwendet werden kann.

- ❑ Emails mit personenbezogenen oder anderen schutzwürdigen Inhalten werden verschlüsselt übertragen. Sofern der Empfänger über kein Zertifikat bzw. öffentlichen Schlüssel verfügt, wird die Email incl. der Anhänge in einen verschlüsselten PDF-Container gepackt, der nur über ein telefonisch übermitteltes Passwort entschlüsselt werden kann.
- ❑ Die Vernichtung von Akten und anderem vertraulichem Schriftgut wird mit einem Schredder der Sicherheitsstufe 3 nach DIN 32757 durchgeführt. Hierbei wird die Partikelbreite von 4mm und die Partikellänge von 80mm nicht überschritten.
- ❑ Nicht mehr benötigte Festplatten und Datensicherungsbänder, werden vor der Entsorgung mechanisch durch eine Bohrung zerstört. Diese Regelung trifft für interne, als auch für Kundengeräte zu.

5. Eingabekontrolle

- ❑ Das eingesetzte CRM-System, das von allen Mitarbeitern für die Kundenbeziehungen genutzt wird, protokolliert alle Änderungen mit Name und Zeitstempel revisionssicher.
- ❑ Alle Bedienhandlungen im Rahmen eine Fernwartungssitzung werden revisionssicher als Mitschnitt aufgezeichnet.

6. Auftragskontrolle

- ❑ Eine Auftragsdatenverarbeitung erfolgt nur zu Reparaturzwecken beim jeweiligen Hersteller oder Servicepartner. Dabei werden die Auftragnehmer in einer speziellen Vereinbarung zur Auftragsdatenverarbeitung zur Einhaltung aller datenschutzrechtlichen Bestimmungen verpflichtet.

7. Verfügbarkeitskontrolle

- ❑ Die Verantwortlichkeiten für die Datensicherung sind incl. einer Vertretung klar geregelt
- ❑ Es wird wöchentlich eine Vollsicherung und täglich eine Differenzsicherung aller Bewegungsdaten durchgeführt. Zusätzlich werden besonders geschäftskritische Daten mehrmals täglich gesichert.
- ❑ Zum Schutz gegen Feuer und Diebstahl werden immer die aktuellsten Datensicherungen außerhalb der Geschäftsräume aufbewahrt.
- ❑ Die Backups sind verschlüsselt
- ❑ Der Ausfall zentraler Systemkomponenten wird über ein zentrales Monitoring-System erfasst und führt zu einer automatischen Meldung per Mail/SMS an den Administrator.
- ❑ In einem Notfallszenario ist der genaue Ablauf der Rücksicherung bzw. die Wiederherstellung des Produktivsystems beschrieben.
- ❑ Das Netzwerk ist durch einen mehrstufigen Schutz gegen Schadsoftware abgesichert:
  1.) Network Protection
  2.) Enduser Protection
  3.) Server Protection
- ❑ Durch eine Advanced Threat Protection werden infizierte Rechner schnell entdeckt und isoliert und damit die Kommunikation mit bösartigen Command & Control Hosts verhindert.

- ❑ Die Signaturdateien werden automatisch aktualisiert. Veraltete Signaturen (älter 2 Tage) werden auf den Workstation/Notebooks mit einem Warnhinweis angezeigt.
- ❑ Erkannte Malware wird auf der Admin-Konsole gemeldet.
- ❑ Eingehende Mails werden über die interne Firewall auf Schadsoftware geprüft
- ❑ Die EDV unterliegt einer regelmäßigen Wartung

8. Trennungskontrolle

- ❑ Das Prinzip der Funktionstrennung wird konsequent eingehalten, dabei erfolgt eine strikte Trennung zwischen auftragsbezogenen und internen Verarbeitungen und zwar organisatorisch und datentechnisch.
- ❑ Dazu werden schutzwürdige Daten den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist.
- ❑ Es ist gewährleistet, dass Daten zu unterschiedlichen Zwecken und für unterschiedliche Ordnungsbegriffe (z. B. Personal- Kundennummer) erhobene bzw. gespeicherte Daten getrennt verarbeitet werden können.