Datenschutzerklärung

für

Heinrich Wietholt GmbH

Änderungshistorie

Zuständig	Datum/Version	Bezeichnung
Olbring	15.03.2018	Dokumenterstellung unter Berücksichtigung der Anforderungen der DSGVO

Inhaltsverzeichnis

1 Datenschutz & Datensicherheit – unsere Verantwortung

In nun mehr als sieben Dekaden haben wir uns vom Ein-Mann-Handwerksbetrieb zum bundesweit agierenden, mittelständischen Unternehmen der Bürobranche entwickelt. Handelte und reparierte unser Gründer und Namensgeber Heinrich Wietholt anfangs ausschließlich lokal mit Schreib- und Büromaschinen, sind wir heute schon zum ständigen Begleiter Ihres Büroalltags avanciert - und das in ganz Deutschland. Wietholt/Bresser passt sich den Bedürfnissen der Zeit und seiner Kunden an, sodass wir mit all unseren Produkten und Dienstleistungen immer eine maßgeschneiderte Lösung für jedes Problem bieten können.

Unser Team bietet neben einer hochwertigen Produktauswahl vieler namhafter Hersteller & Partner eine kompetente Beratung. Mit über 70 Jahren Branchenerfahrung (gegr. 1945) stehen unsere Mitarbeiter/-innen mit einer durchschnittlichen Betriebszugehörigkeit von 14 Jahren wie kaum ein anderes Unternehmen der Bürobedarfsbranche für Fachwissen, Erfahrung und Nachhaltigkeit.

Dieses Dokument repräsentiert zusammenfassend die umfangreichen Maßnahmen zum Datenschutz und ist Bestandteil des nachhaltigen Datenschutzmanagements. Ziel des Dokumentes ist die Gewährung eines Einblickes in die transparenten Prozesse zum Datenschutz- und zur Datensicherheit für Kunden, Partner und Interessenten.

Die verantwortliche Stelle hat ihren Sitz in Velen (Dieks Wall 17, 46342 Velen) und wird vertreten durch die Geschäftsführer Mario Damm, Martin Osterkamp, Markus Steinkamp. Ein Büromarkt wird in Coesfeld (Dülmener Straße 52, 48653 Coesfeld) betrieben.

2 Datenschutzmanagement

Nachfolgende Übersicht gewährt einen Einblick in die getroffenen Maßnahmen zum Datenschutz:

- Alle Mitarbeiter wurden schriftlich zur Verschwiegenheit verpflichtet. Die Verschwiegenheitsverpflichtung berücksichtigt folgende Anforderungen:
  - Datengeheimnis gem. Bundesdatenschutzgesetz (BDSG)
  - Verletzung von Privatgeheimnissen gem. Strafgesetzbuch (StGB)
  - Verrat von Geschäfts- und Betriebsgeheimnissen gem. Gesetz gegen den unlauteren Wettbewerb (UWG)
- Ein Datenschutzbeauftragter wurde schriftlich ernannt
- Durch Schulung und Informationsbereitstellung zu Datenschutz und Datensicherheit werden die Mitarbeiter laufend zu wichtigen und aktuellen Themen geschult und sensibilisiert
- Umfangreiche, aber dennoch einfache, Richtlinien und Verfahrensanweisungen stellen den verantwortungsvollen Umgang unserer Mitarbeiter mit Daten und Geräten der Informations- und Telekommunikationstechnik sicher
- Lösungen zu Virenschutz und Datensicherung stellen die Verfügbarkeit der Systeme sicher
- Datenträger (Papier, CDs, Festplatten usw.) werden datenschutzkonform vernichtet
- Der Zugriff auf IT-Systeme und Anwendungen ist durch Benutzername und Kennwort geschützt

3 Bestellung eines Datenschutzbeauftragten

Das Unternehmen ist verpflichtet einen Datenschutzbeauftragten zu bestellen.

Für die Heinrich Wietholt GmbH ist ein externer Datenschutzbeauftragter bestellt:

Markus Olbring
comdatis it-consulting
Deventer Weg 8
48683 Ahaus
Telefon: 02561-7569986
Mobil: 0173-9799897
E-Mail: datenschutz@wietholt.de

Nachfolgend die Bestellungsurkunde:

Bestellung zum Datenschutzbeauftragten

Gemäß § 4f Bundesdatenschutzgesetz (BDSG), § 38 BDSG (neu) und Art. 37 DSGVO wird Markus Olbring mit sofortiger Wirkung zum externen Datenschutzbeauftragten für das Unternehmen Heinrich Wietholt GmbH bestellt.

Herr Olbring ist in seiner Funktion als externer Datenschutzbeauftragter der Geschäftsleitung direkt unterstellt und in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

Die Aufgaben ergeben sich aus dem Bundesdatenschutzgesetz sowie der Datenschutzgrundverordnung.

Empfehlungen, erforderliche Maßnahmen oder Organisationsanweisungen werden der Geschäftsleitung vorgeschlagen.

Velen, 1. Januar 2018

Heinrich Wietholt GmbH
Geschäftsführung

comdatis it-consulting
Markus Olbring
Deventer Weg 8 - D-48683 Ahaus
Telefon: 02561-7569986
www.comdatis.de
Markus Olbring
comdatis it-consulting

4 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten ist die Aufzeichnung der Geschäftsprozesse innerhalb des Unternehmens, in denen personenbezogene Daten verarbeitet werden. Die Anforderungen an die Erstellung des Verfahrensverzeichnisses ergeben sich aus Artikel 30 der Datenschutz-Grundverordnung (DS-GVO).

Jeder Verantwortliche und ggf. sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält folgende Angaben (Art. 30 DSGVO):

- den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO

Ein Verzeichnis der Verarbeitungstätigkeiten liegt im Unternehmen vor. Die Anforderungen aus Art. 30 Abs. 2 DSGVO für Auftragsverarbeiter sind im erforderlichen Umfang berücksichtigt.

5 Sicherheit der Verarbeitung

Durch technische und organisatorische Maßnahmen (Art. 32 Abs.1 DSGVO) sind die Anforderungen an die IT-Sicherheit zu definieren, um einen angemessenen Schutz der personenbezogenen Daten zu erreichen. Es sind Maßnahmen zu ergreifen, die ein ausreichendes Maß an Sicherheit und Schutz für die Daten bieten. In diesem Kapitel werden die technischen und organisatorischen Maßnahmen für die IT-Infrastruktur beschrieben.

5.1 Wahrung der Vertraulichkeit (Art. 32. Abs. 1 lit. b DSGVO)

5.1.1 Zutrittskontrolle

Der räumliche Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, ist Unbefugten zu verwehren.

Folgende Maßnahmen sind implementiert:

- Alarmsicherung des Gebäudes durch Alarmanlage
- Schließsystem mit codierten Schlüsseln (BKS)
- Technikräume sind separat verschlossen und berechtigte Mitarbeiter haben Zutritt
- Gäste haben ausschließlich in Begleitung Zutritt zu den Technikräumen
- Technikräume können nicht als solche erkannt werden
- Einbruchsichere Verglasung der Technikräume

5.1.2 Zugangskontrolle

Die IT muss so geschaffen sein, dass diese nicht von Unbefugten genutzt werden kann. Unter Zugang wird der konkrete Zugang zu Datenverarbeitungsanlagen verstanden. Es ist sicherzustellen, dass Unbefugte nicht mit personenbezogenen Daten in einem System umgehen.

Folgende Maßnahmen sind implementiert:

- Benutzerauthentifizierung mit Benutzernamen und Kennwort für Clients
- Benutzerauthentifizierung mit Benutzernamen und Kennwort für Anwendungen
- Sichere, toolgestützte Löschung sensitiver Daten von IT-Systemen, wenn diese außer Haus gegeben werden
- Hohe Kennwortkomplexität mit Buchstaben, Zahlen und Sonderzeichen

5.1.3 Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen und das unerlaubte Verarbeiten personenbezogener Daten sind durch die bedarfsorientierte Ausgestaltung von Berechtigungskonzepten auszuschließen. Jedem Benutzer sollten ausschließlich die Zugriffsrechte eingeräumt werden, die zur Aufgabenerledigung notwendig sind.

Folgende Maßnahmen sind implementiert:

- Aufgabenbezogene Berechtigungsverwaltung
- Schaffung der Möglichkeit einer differenzierten Berechtigungsvergabe (Profile, Rollen)
- Datenschutzgerechte Entsorgung von Datenträgern

5.1.4 Trennungsgebot

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden.

Folgende Maßnahmen sind implementiert:

- Systemtrennung zwischen Softwareprodukten (z.B. Technikerlösung, Warenwirtschaft, Archiv)
- Trennung zwischen Test- und Produktivumgebung für wesentliche Anwendungen

5.2 Wahrung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

5.2.1 Weitergabekontrolle

Bei einer Weitergabe personenbezogener Daten ist sicherzustellen, dass die Daten während der Übertragung oder des Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Folgende Maßnahmen sind implementiert:

- Zugriff auf die IT-Systeme von außen über VPN
- Zugriff auf die IT-Systeme über eine verschlüsselte Verbindung (https für Technikersoftware)
- Verschluss vertraulicher Unterlagen und IT-technischer Datenträger
- Verschlüsselte Backupdatenträger
- Definierte Maßnahmen zum Datenträgertransport sowie bei auftretenden Fehlern

5.2.2 Eingabekontrolle

Eingaben personenbezogener Daten müssen nachvollziehbar sein. Es muss erkennbar sein, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt wurden.

Folgende Maßnahmen sind implementiert:

- Einsatz systemseitiger Protokollierungsmöglichkeiten
- Definierte Benutzerprofile und Zuständigkeiten

5.3 Wahrung der Verfügbarkeit und Belastbarkeit (Art. 32. Abs. 1 lit. b DSGVO)

5.3.1 Verfügbarkeitskontrolle

Personenbezogene und weitere schützenswerte Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, um somit deren Verfügbarkeit sicherzustellen.

Folgende Maßnahmen sind implementiert:

- Definierte Backup-Verfahren einschl. Auslagerung von Datensicherungen
- Unterbrechungsfreie Stromversorgung
- Viren- und Firewallschutz (bitdefender / Sophos)
- Kontrollmaßnahmen zur Prüfung und Überwachung von Datensicherungen

5.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32. Abs. 1 lit. d DSGVO)

5.4.1 Auftragskontrolle

Die Verarbeitung personenbezogener Daten im Auftrag darf nur nach Anweisung des Auftraggebers erfolgen.

Folgende Maßnahmen sind implementiert:

- Vertragliche Verpflichtung von Subunternehmern
- Möglichkeit zum Abschluss einer standardisierten Vereinbarung zur Auftragsvereinbarung mit Kunden

5.4.2 Datenschutzmanagement

Ein nachhaltiges und dokumentiertes Datenschutzmanagement gewährleistet die Möglichkeit zur kontinuierlichen Verbesserung und regelmäßigen Überprüfung, Bewertung und Evaluierung.

Folgende Maßnahmen sind implementiert:

- Benennung eines Datenschutzbeauftragten
- Nachvollziehbares Datenschutzmanagement
- Dokumentation der datenschutzrechtlichen Vorgaben
- Schulung / Sensibilisierung der Mitarbeiter
- Selbstkontrolle & kontinuierliche Verbesserung