Kundeninformation
Köln, 25.05.2018

Verzeichnis der Datenverarbeitungstätigkeit Der Firma Der Kölner GassiKönig

Prolog:

Nach dem aktuellen EU-Datenschutzgesetz DSGVO müssen wir als Verantwortliche ein sogenanntes Verzeichnis der Datenverarbeitungstätigkeiten führen (Art. 30 DSGVO). Dieses kann jederzeit bearbeitet und ergänzt werden. Auch hier gibt es bis dato kein verbindliches Muster. Erst die Praxis wird in den kommenden Jahren zeigen, wie die Anforderungen konkret auszusehen haben. Deshalb erhebt das hier vorliegende Verzeichnis keinen Anspruch auf Vollständigkeit. Vielmehr muss und wird es individuell angepasst und ggf. ergänzt werden.

Wir haben entsprechend dieser neuen Rechtsnorm, die ab 25.05.2018 in Kraft tritt, bereits 3 Jahre vor der gesetzlichen Vorgabe technische und organisatorische Maßnahmen ergriffen, die seitdem in vollem Umfang arbeiten.

Unsere Datenverarbeitungsgeräte (wie PC, Tablets, Smartphones etc.) wurden nun daraufhin genau überprüft und es wurde sichergestellt, dass Datenschutz entsprechend der EU-Vorschrift gewährleist ist bzw. bleibt.
Denn Art. 32 DSGVO, § 64 BDSG-neu verpflichtet jeden Gewerbetreibenden, geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Daten seiner Kunden zu gewährleisten.
Es gibt hierbei jedoch keinen standardisierten Katalog. Die Maßnahmen müssen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignet und angemessen sein, um das Schutzniveau zu gewährleisten.
Bei unserer Art der Dienstleistung ist der Einsatz von eigenen Servern, Personal und

anderer technischer Maßnahmen nur in geringem Umfang und wenig komplex vorhanden, andere als etwa bei einer großen Firma, wie z.B. Volkswagen, die tausende Datensätze, wechselndes Personal und Subunternehmer oder Subdienstleister beschäftigt. Trotzdem gibt es für uns bestimmte Vorgaben, die wir hiermit vorstellen möchten:

Folgende Voraussetzungen sind erforderlich:

1. Anforderung: ZUGANGSKONTROLLE:

Anforderung:
Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

2. Anforderung: DATENTRÄGERKONTROLLE:

Anforderung:
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern durch Dritte bzw. Unbeteiligte.

3. Anforderung: SPEICHERKONTROLLE:

Anforderung:

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten durch Dritte bzw. Unbeteiligte.

4. Anforderung: BENUTZERKONTROLLE:

Anforderung:
Verhinderung der Nutzung automatisierter Verarbeitungs-systeme durch Unbefugte mithilfe von Einrichtungen zur Datenübertragung .

5. Anforderung: ZUGRIFFSKONTROLLE:

Anforderung:
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Unsere Umsetzung (Punkt 1-5):
Unsere Arbeitsstätte ist unser Privathaus, zumindest für die HundeHerberge.
Dieses ist seit Jahren besonders gegen Diebstahl und Einbruch gesichert.
Die Daten unseres Gewerbes sind weder auf unseren Rechnern, noch in Papierform zu

finden, sondern werden elektronisch und digital an einem sicheren Ort physisch und auch aushäusig virtuell sicher gelagert und sind für Unbefugte nicht auffindbar. Überdies werden alle Daten in virtuellen Safes (Softwarelösung durch Steganos) verschlüsselt gelagert und ebenso verschickt.

6. Anforderung: ÜBERTRAGUNGSKONTR.:

Anforderung:
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

7. Anforderung: EINGABEKONTROLLE:

Anforderung:
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

8. Anforderung: TRANSPORTKONTROLLE:

Anforderung:
Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Unsere Umsetzung (Punkt 6-8):
Daten werden grundsätzlich nicht als offene Dateien verschickt, sondern der Kunde erhält einen Link zu einer Stelle auf unserem Internetseitenserver.
Dort ruft er/sie die Datei durch einen Klick auf, lädt sie herunter oder liest sie. Er/sie benötigt dafür ein ihm vorab ausgehändigtes Kennwort, das nur ihm/ihr und uns bekannt ist.
Nach Ansicht erhalten wir eine Nachricht, dass die Datei gelesen wurde und der Linkinhalt wird vom Server gelöscht. Ein Zugriff durch Dritte ist ausgeschlossen, insbesondere durch den Umstand, dass die Daten kennwortgeschützt sind.
Die Kontrolle der Übertragung ist durch die Speicherung der E-Mail-Protokolle gewährleistet. Die Inhalte der Übertragung werden jedoch anschließend regelmäßig jeden Tag gelöscht, so dass von der Übertragung selbst nur die E-Mail-Bestätigung übrig bleibt, der Schutz der

Übertragungsdaten ist gewährleistet, der Akt der Übertragung selbst ist protokolliert.
Der Handelnde im Bereich Übertragung ist immer die selbe Person und dem Kunden bekannt.

9. Anforderung: WIEDERHERSTELLBARKEIT:

Anforderung:
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Unsere Umsetzung (Punkt 9):
Daten werden grundsätzlich mehrfach auf unterschiedlichen Datenträgern, wie z.B. USB-Sticks, DVD-ROMs, Festplatten (SSD), in einer Cloud usw. gesichert und dies IMMER safe- und kennwortgeschützt.
Eine Wiederherstellung im Störfalle ist deshalb zu jeder Zeit gewährleistet, insbesondere auch deshalb, weil die Rechnersysteme keine Daten enthalten, da sie ausgelagert sind.

10. Anforderung: ZUVERLÄSSIGKEIT:

Anforderung:
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Unsere Umsetzung (Punkt 10):
Alle im Gebrauch stehende Systeme sind immer in Funktion und werden im Falle eines Ausfalls oder einer Störung durch vorhandene Backupsysteme sofort ersetzt. Die gespeicherten Daten sind davon in jedem Falle nie betroffen.

11. Anforderung: DATENINTEGRITÄT:

Anforderung:
Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Unsere Umsetzung (Punkt 11):
Alle im Gebrauch stehende Systeme sind immer in Funktion und werden im Falle eines Ausfalls oder einer Störung durch vorhandene Backupsysteme sofort ersetzt.
Die Daten sind mehrfach gesichert und sind zu jeder Zeit von Extern her im Zugriff, unabhängig von der Funktionalität von Systemen.

12. Anforderung: AUFTRAGSKONTROLLE:

Anforderung:

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Unsere Umsetzung (Punkt 12):
Alle im Gebrauch stehende Daten werden nur punktuell im Falle einer Auftragsverarbeitung ihren virtuellen Safes entnommen, verarbeitet und werden nach Abschluss der Verarbeitung wieder rückstandsfrei im jeweiligen virtuellen Safe verschlossen. Ein Zugriff ist danach nicht mehr erforderlich. Die Daten liegen also für Dritte und "Außenstehende" (Hacker z.B.) unsichtbar und extern in virtuellen Safes, die nicht sichtbar bzw. nicht auf den laufenden Systemen vorhanden sind.

13. Anforderung: VERFÜGBARKEITSK.:

Anforderung:
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Unsere Umsetzung (Punkt 13):
Alle Daten werden mehrfach auf unterschiedlichen Datenträgern gesichert bzw. lagermäßig vorgehalten, wobei diese Datenträger einen virtuellen Safe enthalten.

Dieser Safe muss durch ein Kennwort gesichert geöffnet werden und ist ansonsten nicht nutzbar.
Zudem sind die Datenträger immer physisch in einem eigens dafür gemieteten Banksafe dupliziert gelagert und werden zusätzlich in einer Google Drive-Cloud im virtuellen Raum unabhängig von den Gefahren einer physischen Lagerung gelagert bzw. gesichert. Die Datensicherheit dort ist von Google garantiert.

14. Anforderung: TRENNBARKEIT:

Anforderung:
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Unsere Umsetzung (Punkt 14):
Alle Daten werden bei uns nur zu fl. Zwecken verarbeitet:

1. **Adresserfassung in MS-Access**
2. **Angebotserstellung in MS-Word bzw. als pdf-Datei**
3. **Auftragsbestätigung in MS-Word bzw. als pdf-Datei**
4. **Zahlungs- und Fälligkeitsübersichten in MS-Excel bzw. als pdf-Datei**

Folgende technische Schutzmaßnahmen werden vorgehalten:

Unsere Computer- und Smartphone-Geräte haben einen aktuellen Anti-Viren-Schutz und eine aktuelle Firewall.
Die Geräte sind passwortgesichert.
Das Passwort enthält Zahlen sowie eine Kombination aus Groß- und Kleinbuchstaben. Es ist auch nicht zu kurz.
Es gibt keine Familienangehörige oder Dritte, die ebenfalls das Gerät benutzen, alle Ordner mit personenbezogenen Daten sind passwortgesichert und in einem virtuellen Safe aufbewahrt, so dass sie für Dritte nicht zugänglich sind.
Jegliche Weitergabe von Daten erfolgt verschlüsselt.
Verschlüsselungssoftware ist installiert und wird benutzt (Steganos bzw. PDF24).
Sofern möglich, werden Daten nur in anonymisierter oder pseudoanymisierter Form weitergegeben.
Von den Dateien werden regelmäßig mehrfach Sicherheitskopien auf unterschiedlichen Datenträgernormen erstellt. Dabei werden Löschpflichten beachtet. Die Datenträger werden regelmäßig adäquat überschrieben.

Physische Akten mit personenbezogenen Daten werden nicht geführt.
Bei der Benutzung von Mailverteilern gilt: E-Mailadressen der anderen Empfänger sind nicht sichtbar (BCC-Einstellungen); nur verschlüsselte W-LAN-Netze werden genutzt.

Physische und analoge Unterlagen werden grundsätzlich vor Ort eingescannt und dann sofort und vor bei Ablauf der Löschfristen ordnungsgemäß durch den Einsatz von entsprechenden örtlich vorhandenen Aktenvernichtern mit der höchsten Sicherheitsstufe vernichtet.
Auch Datenträger und Computer sind, wenn sie aussortiert werden, ordnungsgemäß gelöscht, beispielsweise durch Einsatz von professioneller Überschreibungssoftware.

Dieses Verzeichnis wurde erstellt auf Basis eines Vorschlags des Kölner Haus- und Grundbesitzervereins von 1888, Newsletter vom 25.04.2018, "Ihre Immobilie liegt uns am Herzen".