Datenschutzkonzept der Krämer Marktforschung GmbH

Einleitung

Die Krämer Marktforschung GmbH ist Mitglied der Richtlinienverbände Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM), dem Berufsverband Deutscher Markt- und Sozialforscher e.V. (BVM) und der European Society for Opinion and Marketing Research (ESOMAR). Sie ist an die Richtlinien der o.g. Verbände sowie die Vorschriften des Bundesdatenschutzgesetzes (BDSG) gebunden.

Datenschutzbeauftragte im Unternehmen ist Silke Schulte-Uhr (s.schulte-uhr@kraemer-germany.com; 02501-802207).

Erfüllung der Aufgaben nach § 9 Bundesdatenschutzgesetz (BDSG)

1. Zutrittskontrolle
Verwehrung des Zutritts Unbefugter zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Das Gebäude ist durch eine Alarmanlage gesichert.

Der Empfang ist in der Zeit von 08:00 bis 17:30 werktags besetzt. Die zentrale Eingangstür ist zwischen 17.30 Uhr und 8.00 Uhr standardmäßig verschlossen.

Die Schließanlage wird durch individualisierte Schlüssel geschlossen und die Schließungen werden protokolliert. Es gibt ein Schlüsselverzeichnis; bei Firmenaustritt wir anhand eines Laufzettels kontrolliert, ob alle Schlüssel, Kennungen und Passworte gelöscht sind.

Unterschiedliche Gebäudeteile sind durch eine individuelle elektronische Sicherung vor unbefugtem Betreten nicht autorisierter Personen gesichert. Mitarbeiter sind nur für die für sie relevanten Gebäudebereiche freigeschaltet.

Der Server des gesamten Netzwerkes steht in einem verschlossenen Serverraum(Codeschloss);der Zutritt zu diesem Raum ist nur mit separatem Code möglich. Die Konsole für die Server steht im Serverraum und eine Administration ist nur nach Passwort geschütztem Login möglich.

Nur die Administratoren haben Zutritt zum Serverraum.

Für andere Räume ist eine Zeiterfassung vorhanden.

Das Reinigungspersonal hat keinen Zutritt zum Serverraum. Nichtautorisierte Mitarbeiter sowie betriebsfremde Personen (bspw. Techniker, Handwerker) haben nur unter Aufsicht eines autorisierten Mitarbeiters Zutritt zum Serverraum.

Wartungsarbeiten an den installierten Systemen durch externe Firmen werden nur in Gegenwart autorisierter KMF-Mitarbeiter durchgeführt. Es gibt keine Fernwartung der Systeme. Ein Serverzugriff durch die Projektmitarbeiter von zu Hause ist nicht möglich, lediglich die IT-Administration ist dazu autorisiert.

Die Büroräume können nur in Begleitung eines autorisierten Mitarbeiters betreten werden

2. Zugangskontrolle
Verhinderung der Nutzung von Datenverarbeitungssystemen mit personenbezogenen Daten durch Unbefugte.

Im Windows-System ist der Zugriff nur über Passwort bei der Anmeldung möglich; durch den Administrator werden projektbezogene Nutzergruppen eingerichtet und entsprechende Rechte vergeben.

Die Passworte an den internen Datenbanken müssen alle 4 Wochen geändert werden.

Der Zugang wird nach 3 fehlerhaften Anmeldeversuchen gesperrt.

Für jedes Projekt wird ein Ordner mit gesonderten Zugangsrechten erstellt auf den nur zugelassene Personen Zugriff haben (Administrator und Projektleiter).

Administratorenpassworte werden im Safe aufbewahrt.

Ein Zugriff auf die Systeme/Anwendungen von außerhalb des Unternehmens ist nur in Form von Zugriff auf Befragungsmasken (Telefonstudio) möglich.

Die Callcenter-Agenten-Rechner sind durch ein doppeltes Anmeldeverfahren gesichert. Alle Agenten haben nur begrenzte Rechte sowohl am Rechner als auch im Netzwerk.

Das Policy-Verfahren ist aus den o.g. Gründen vereinfacht. Kennwörter an den Rechnern werden nur von den Administratoren und Supervisoren in regelmäßigem Abstand (4 Wochen) geändert.

Um Zugriff auf die Befragungssoftware zu erhalten, werden die Agenten zusätzlich gesondert für jeden Einsatz/jede Schicht von den Supervisoren in einem hauseigenen Tool freigeschaltet.

Protokollierung von Zugriffen auf Anwendungen und Systeme durch Standleitung, Teilnehmerkennung, funktionelle Zuordnung einzelner Datenendgeräte, Protokollierung der Systemnutzung und Protokollauswertung (nur bei Verdachtsfällen). Zugriff auf Protokolle hat nur der Administrator.

Die Systeme/Anwendungen sind durch eine Firewall gegen unberechtigte Zugriffe abgesichert. Ein automatischer Virenscanner ist im Einsatz und wird laufend aktualisiert.

Alle Mitarbeiter, die mit personenbezogenen Daten arbeiten, haben eine Verschwiegenheitserklärung unterzeichnet.

Verschlüsselungen von Datenträgern werden je nach Maßgabe der Vorschriften der jeweiligen Auftraggeber vorgenommen.

3. Zugriffskontrolle

Verhinderung des Zugriffs auf personenbezogene Daten bzw. deren Veränderung durch Unbefugte.

Der Zugriff auf die verschiedenen Datenbereiche ist durch eine Rechte-Vergabe differenziert; nur die Administration hat Vollzugriff auf alle Systeme.

Es werden einzelne den Funktionen entsprechende Rollen und Rechte vergeben.

Es gibt differenzierte Berechtigungen für lesenden und schreibenden (Änderung/Löschung) Zugriff und anwendungsbezogen vergebende Userrechte

Die nicht aktuell im System befindlichen Speichermedien sind im Tresor hinterlegt. Die Daten werden generell in einer SQL-Datenbank abgelegt. Die Datenbank liegt auf einem redundant ausgelegten Server mit raid5-Festplatten gegen Datenverlust. Datensicherung erfolgt über Nacht. Es sind 2 Tresore vorhanden.

Befragungs- und Adressdaten werden nach Abschluss der Kontrollen einer jeden Studie spätestens aber 6 Wochen nach Befragungsende komplett gelöscht.

Nicht mehr benötigte Daten werden qualifiziert gelöscht bzw. vernichtet. Die Aktenvernichtung von personenbezogenen Daten erfolgt durch zertifizierte Firmen mit Bestätigung. Magnetische Datenträger werden durch Überschreiben oder physische Zerstörung gelöscht.

4. Weitergabekontrolle
Verhinderung unbefugten Lesens, Kopierens, Veränderns oder Entfernens personenbezogener Daten während der elektronischen Übertragung / des Transports / der Speicherung.

Datenübertragungen bzw. Ausgabe oder Versand von Datenträgern erfolgen grundsätzlich nur nach Maßgabe der Vorschriften des jeweiligen Auftraggebers. Eine Weitersendung der Adress-, Befragungsdaten an Dritte findet ebenso wenig statt wie die Nutzung der Daten außerhalb des vorgeschriebenen Projektes.

Versendung erfolgt durch LAN (nur für unsere Filialen oder lokal/Tunnelverbindung), Internet/Web, E-Mail, FTP, Post, Kurier, Telefax je nach Maßgabe der Vorschriften des jeweiligen Auftraggebers.

Verschlüsselungen von Daten, Transportprotokolle etc. werden auf Wunsch einzelner Kunden und dann nach Maßgabe der jeweiligen Vorschriften vorgenommen.

5. Eingabekontrolle
Nachträgliche Prüfmöglichkeit, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben / verändert / entfernt werden.

Nur Mitarbeiter im Projekt haben das Recht, Daten zu verändern. Die Zugriffsrechte und die Zuordnung zu den Benutzergruppen erfolgt durch die Projektleitung; sie werden vom Administrator eingerichtet und kontrolliert.

6. Auftragskontrolle
Gewährleistung, dass personenbezogene Auftragsdatenverarbeitung nur entsprechend den Weisungen des Auftraggebers erfolgt.

Jeder Auftrag wird strikt getrennt bearbeitet, protokolliert und verwaltet. Aufträge werden in getrennten Verzeichnissen ausgeführt.
Formalisierung der Auftragsvergabe und -abwicklung ist gegeben.
Kontrolle der Arbeitsschritte und Ergebnisse.

7. Verfügbarkeitskontrolle
Schutz personenbezogener Daten vor zufälliger/m Zerstörung / Verlust

Es existieren geeignete Backup- und Sicherungsverfahren für alle relevanten Systeme/Anwendungen (Backup-Verfahren, Plattenspiegelung (RAID), Brandschutzeinrichtungen, Klimatisierung).

Ein USV-Schutz (unterbrechungsfreie Stromversorgung) ist vorhanden.

Auf allen Arbeitsrechnern und Servern werden die sicherheitsrelevanten Patches regelmäßig eingespielt.

Es erfolgen je nach Bedarf tägliche, wöchentliche und monatliche Datensicherungen (bis 6 Monate)

Ein ständig aktualisierter Virenscanner ist im Einsatz.

Regelmäßig werden Tests zu Backup und Wiederanlauf durchgeführt.

Virenschutz ist gewährleistet.

Es befinden sich Feuerlöscher in Server- und Arbeitsräumen, ebenso Rauch- und Brandmelder; das Gebäude verfügt in einigen Bereichen über Brandschutztüren.

8. Trennungsgebot

Gewährleistung getrennter Verarbeitung zu unterschiedlichen Zwecken erhobener personenbezogener Daten.

Für jede Bearbeitung personenbezogener Daten ist festgelegt, zu welchem Zweck sie erfolgt.

Jeder Auftrag wird strikt getrennt bearbeitet, protokolliert und verwaltet. Aufträge werden in getrennten Verzeichnissen ausgeführt.

Eine Formalisierung der Auftragsvergabe und -abwicklung ist vorhanden.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Krämer Marktforschung GmbH setzt regelmäßig alternative adäquate Maßnahmen um, soweit sie dem technischen Fortschritt unterliegen und das Sicherheitsniveau der o.g. Maßnahmen nicht unterschritten wird.

.