REMARKETING COMPANY

BETRIEBLICHER DATENSCHUTZ

(für IT-Daten inkl. Smartphones)

A) Gesetzliche Vorschriften

§ Bundesdatenschutzgesetz
§ Der betriebliche Datenschutzbeauftragte
§ Inhalt des betrieblichen Datenschutzes
§ Technisch–organisatorische Maßnahmen

1. BUNDESDATENSCHUTZGESETZ

1.1 §1 BDSG

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

2. PFLICHTEN DES UNTERNEHMENS

Nach § 4 f des Bundesdatenschutzgesetzes, haben Unternehmen einen Datenschutzbeauftragten zu stellen, wenn:

- personenbezogene Daten automatisiert erhoben, erarbeitet oder genutzt werden und damit i.d.R. mindestens 10 Arbeitnehmer ständig beschäftigt sind;
- personenbezogene Daten auf andere Weise verarbeitet werden und damit i.d.R. mindestens 20 Arbeitnehmer beschäftigt sind.

3. PRINZIP DES DATENSCHUTZES

- Einhaltung der Prinzipien der Datenvermeidung und Datensparsamkeit
- Sorgfaltspflicht mit Daten
- Technisch-organisatorische Maßnahmen zum betrieblichen Datenschutz

4. GRUNDLAGEN DES DATENSCHUTZES

4.1 Beachtliche Bußgelder

Wer entgegen den gesetzliche Vorschriften keinen Datenschutzbeauftragten bestellt, muss mit einem Bußgeld von bis zu 50.000 Euro rechnen (§ 43 Abs. 1 Nr.2 i.V.m. Abs. 3 S. 1 BDSG).

4.2 Weitere Folgen durch Datenschutzvergehen persönliche Haftbarmachung der Geschäftsführung

- erheblicher Imageschaden wirtschaftliche Einbußen
- mögliche Bußgelder aufgrund unlauteren Wettbewerbs

ACHTUNG: Für Folgen von Verstößen gegen das Datenschutzgesetz, aus welchen Gründen auch immer, ist in jedem Fall die Geschäftsführung persönlich verantwortlich!

5. RECHTE DER BETROFFENEN

5.1 Betroffene im Sinne des Bundesdatenschutzgesetzes

Kunden, Geschäftspartner, Lieferanten, Mitarbeiter

5.2 Benachrichtigung

- Kenntnis über die Speicherung und Übermittlung von personenbezogenen Daten
- Hinweis auf die möglichen Empfänger
- Hinweis auf Widerspruchsrecht gegen Werbung

5.3 Auskunftspflicht

- Einsicht in das öffentliche Verfahrensverzeichnis
- Einsicht in gespeicherte Daten durch Betroffene
- Einsicht auch in strukturierten Akten (Personal-, Kundenakten)

5.4 Anspruch auf Löschung/Sperrung

- Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) Anrufung der Datenschutzbehörde
- Schadensersatz (Datenschutz, Strafrecht, Zivilrecht)

6. AUFGABEN DES DATENSCHUTZBEAUFTRAGTEN

- Auf die Ausführung des BDSG und anderen Datenschutzvorschriften hinwirken
- Beratung/Überwachung der ordnungsgemäßen Ausführung der Datenschutzvorschriften
- Durchführen von Schulung zum Datenschutz

- Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 5 BDSG
- Beratung zur Erstellung und Führung des Verfahrensverzeichnisses
- Beratung bei den organisatorischen Aufgaben zur IT-Sicherheitsrichtlinie
- Audits der Lieferanten/Auftragsnehmer im Sinne § 11 BDSG durch den Datenschutzbeauftragten
- Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme § 4g /2 BDSG
- Auskunft an und Benachrichtigung der Betroffenen
- Vorabkontrolle
- Auskunft an jedermann
- Unterstützung bei organisatorische Aufgaben wie die Sicherheitsrichtlinie IT
- Ständige Anlaufstelle für Geschäftsleitung/Mitarbeiter bei Sicherheitsvorfällen
- Regelmäßige Überprüfung des Sicherheitskonzeptes auf Aktualität

7. § 5 BDSG DATENGEHEIMNIS

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, [...], bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

8. WAS IST EINE AUTOMATISIERTE VERARBEITUNG?

- Erheben ist das Beschaffen von personenbezogenen Daten
- Verarbeiten ist das
  - Speichern, Verändern, Übermitteln, Sperren, Löschen

  von personenbezogenen Daten
- Nutzen ist jede sonstige Verwendung von personenbezogenen Daten

8.1 Sonderfall Private Internet und Mailnutzung

Privatnutzung der Internetdienste (WWW/MAIL/Dateisystem) in einem Firmennetz führt zu einer Gleichstellung des Arbeitsgebers mit einem Internet Service Provider. Folge: Jede Änderung des Inhalts einer Nachricht. (Virus)

Vorenthalten (Spam) oder administrativer Einblick (Umleitung durch Administrator etc.) kann ggf. zu einer Strafbarkeit nach 206 STGB führen. Daher ist die Internet- und Mailnutzung in der Praxis nicht erlaubt.

9. STAATLICHE KONTROLLE

9.1 Kontrolle durch Datenschutzbehörden

Bußgeldvorschriften nach § 43 BDSG 50.000 – 300.000 EURO

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig:

- Den Betroffenen bei der Werbeansprache nicht ausreichend unterrichtet
- Daten unzulässig übermittelt oder nutzt
- Trotz Widerspruch den Betroffenen in Verzeichnisse aufnimmt
- Den Betroffenen unvollständig benachrichtigt Daten ohne Gegendarstellung übermittelt
- Zweckgebundene Daten an Dritte weitergibt
- Abmahnungen durch Wettbewerber nach § 1 UWG möglich

10. KLÄRUNG ÜBER BEREITS BESTEHENDEN REGELUNGEN (TECHNISCH-ORGANISATORISCHEN MASSNAHMEN)

Beispiele:

- Verpflichtungen im Arbeitsvertrag
- Bildschirmschoner
- Passwortrichtlinien
- Domänenrichtlinien
- Standardsoftware/Standardhardware
- Standardlieferanten
- Zugangsrichtlinien
- Zutrittsrichtlinien
- Zugriffsrichtlinien/Freigabeverfahren
- Organisationshandbücher/ISO 9001/14001/ ...

11. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Wie müssen Daten nach BDSG geschützt werden?

11.1 Die 8 Gebote des Datenschutzes §9 BDSG

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

11.2 Zutrittskontrolle

Maßnahmen die sicherstellen, dass Unbefugte keinen Zutritt (räumlich) zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

Gebäudesicherung:

- Zäune
- Pforte
- Videoüberwachung

Sicherung der Räume wie z.B.:

- Sicherheitsschlösser
- Chipkartenleser
- Codeschlösser
- Sicherheitsverglasung
- Alarmanlagen

11.3 Zugangskontrolle

Maßnahmen die sicherstellen, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können. Gemeint ist hiermit im Gegensatz zur Zutrittskontrolle das Eindringen in das IT-System seitens unbefugter Personen.

- Zugang zu Rechnern/Systemen (Authentifizierung)
- Benutzerkennung mit Passwort (Passwortrichtlinien)
- Benutzeridentifikation
- Firewall
- Zugangsberechtigungskonzept

11.4 Zugriffskontrolle

Sicherstellung, dass berechtigte User IT-Anlagen ausschließlich auf Inhalte zugreifen können für welche sie berechtigt sind und das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können. z.B.:

- Berechtigungskonzept (Dokumentation)
- Benutzerkennung mit Passwort
- Datenträgerverwaltung

11.5 Trennungsgebot

Dabei ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testsystemen
- getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)
- separierbare Kundendaten
- getrennte Datenbanken

11.6 Eingabekontrolle

- Tracking von Eingaben/Veränderungen

11.7 Weitergabekontrolle

- Zugriffsberechtigungen und Tracking der Weitergabe von Daten
- Eskalationsprozesse mit Kommunikation zum Betroffenen

11.8 Verfügbarkeitskontrolle

- dokumentierte und regelmäßig überwachte Brandschutzbestimmungen
- Brandschutztüren an Hallenübergängen
- Datensicherungskonzept (12 Generationen)
- geregelte USV-Absicherung aller Server

11.9 Auftragskontrolle

- Schriftlicher Auftrag zur Datenverarbeitung und Dokumentation des Prozesses für den Vertragspartner

B) Spezielle Vorschriften zur betrieblichen Datenlöschung

1. DEUTSCHLAND

Zentrale Norm ist § 35 Abs. 2 Nr. 3 BDSG (Bundesdatenschutzgesetz):

„Die für eigene Zwecke verarbeiteten personenbezogenen Daten, die für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich sind, sind zu löschen."

2. DEUTSCHLAND, EUROPA, USA

Standards wie ISO 27001, ISO 15408, PCI DSS (Payment Card Industry Data Security Standard HIPAA (Schutz der Gesundheitsdaten), SOX (Sarbanes-Oxley-Act USA und ausländische Firmen) aber auch Direktiven der Europäischen Union und FISMA (Federal Information Security Management, USA)

Geplante Sanktionen bei Missachtung dieser neuen EU Anforderungen reichen von 250.000 EUR bis zu 100 Million oder von 0,5% bis zu 5% des Umsatzes für größere Verstöße.

So geht das Bundesamt für Sicherheit in der Informationstechnik vor:

Werden Unterlagen durch externe Dritte als "Datenverarbeitung im Auftrag" vernichtet, ist die gesamte Handhabung und Sicherung der Unterlagen zwischen der Übergabe und dem Abschluss der Vernichtung vertraglich festzulegen. Es müssen der Transport, eine eventuell erforderliche Zwischenlagerung, der Vernichtungsort und der höchstzulässige Zeitraum zwischen der Übergabe der Unterlagen sowie dem Abschluss der Vernichtung geregelt sein. Weiter ist schriftlich festzulegen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet gelten zu können. Durch den Auftragnehmer ist zu gewährleisten, das Unbefugte keine Kenntnis der in den Unterlagen gespeicherten Daten erhalten können. Die Übergabe von Unterlagen

an das Auftragsunternehmen sollte quittiert werden und die Durchführung jeder Vernichtungsaktion sollte schriftlich bestätigt werden. Generell gilt, dass die Erteilung von Unterauftragsverhältnissen möglichst ausgeschlossen werden sollte.

C) Praktische Umsetzung

1. SICHERSTELLUNG DER DATENLÖSCHUNG FÜR AUSGEDIENTE HARDWARE UND SMARTPHONES

Gemäß den gesetzlichen Vorschriften müssen die Daten gelöscht werden. Gleich, ob Sie die Hardware intern verschenken oder zur Wiederaufbereitung (Remarketing) weiterverkaufen. Die Verantwortung dazu liegt in Ihrem Hause. Sie kann an ein Remarketing-Unternehmen weitergegeben werden. Revisionssichere Löschberichte geben Ihrem Unternehmen Sicherheit.

Zum Einsatz kommen die folgenden technische Methoden zur Datenlöschung:

1.1 Löschung per Software

Derzeit verlässliche Methoden sind 3-fache oder 7-fache Datenlöschung. Es können durch uns sowohl Festplatten als auch Ihre HANDYS zertifiziert gelöscht werden!

Die eingesetzte Löschsoftware sollte folgende Anforderungen erfüllen

- löscht alle Daten einer Festplatte sicher und unwiederbringlich (je nach Sicherheits-Standard)
- Entfernt Fragmente alter Installationen
- Löscht Boot- und Partitionssektor-Viren
- Erfüllt internationale Sicherheits-Standards (wie z.B. DoD, BSI)

Die eingesetzte Software sollte folgende Sicherheitsstandards erfüllen

- BSI Standard (Bundesamt für Sicherheit in der Informationstechnik, Deutschland)
- BSI VS (BSI, Deutschland)
- DoD 5220.22M (Department of Defense, USA)
- DoD 5220.22M erweitert (Department of Defense, USA)
- AR380-19 (US-Army)
- AFSSI 5020 (US-Air-Force)
- Peter Gutmanns Methoden

Verwendbare Löschverfahren und Löschstandards (z.B. Blancco 5)

Alle internationalen Löschstandards sind implementiert

- HMG Infosec Standard 5, Baseline Standard
- HMG Infosec Standard 5, Enhanced StandardNAVSCO P-5239 (TOP SECRET) for FEPROM
- NAVSCO P-5239 (SECRET or CONFIDENTIAL) for FEPROM
- Peter Gutmann's Algortihm
- NIST, Enhanced NIST standard
- US Department of Defense Sanitizing.
- DOD 5220.22-M & ECE
- Bruce Scheier's Algorithm
- Navy Staff Office Publication NAVSOP-5239-26 for RLL
- The National Computer Security Center NCSC-TG-025
- Air Force System Security 5020
- US Army AR380-19
- German Standard VSITR / BSI GS/GSE
- NSA (Overwrite standard by National Security Agency)
- BSI-GS / BSI GSE

1.2 Schreddern der Hardware

Eine zuverlässige Methode zur endgültigen Datenlöschung ist die physikalische Zerstörung von Datenträgern. Eine gängige Methode ist das sogenannte Schreddern.

Ein Schredder (englisch: shredder) ist ein mechanisches Gerät zum Zerkleinern von unterschiedlichsten Materialien. Das bedeutet, der Datenträger wird zerstört, indem

er in kleine Teile zerlegt wird. Diese Dienstleistung kann auch bei Ihnen vor Ort in Ihrem Unternehmen durchgeführt werden.

2. GEWINNMAXIMIERUNG DURCH VERKAUF DER GEBRAUCHTEN HARDWARE

Nach Einhaltung der Sicherheitsstandards können Sie Ihre Hardware bedenkenlos verkaufen. Dies ist die Aufgabe der Remarketing-Unternehmen. Sie erhalten ein Ankaufangebot und überlassen die gesamte Umsetzung des Projektes einer renommierten Remarketing-Firma.

Hierfür stehen wir Ihnen gerne zur Verfügung!
Finden Sie mehr zum konkreten Ablauf heraus.

www.remarketing.company

Fragen/Anregungen? Wir freuen uns auf Ihr Feedback!

Nils Beckmann
Geschäftsführender Gesellschafter

RC GmbH
Carl-Zeiss-Ring 4
85737 Ismaning

M +49 171-6844-756
nb@remarketing.company