Datenschutzkonzept

Auktion & Markt AG

I. Grundlagen und Aufbau

Die Verarbeitung personenbezogener Daten soll unter Berücksichtigung:

- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

gewährleistet werden.

II. Sicherheitskonzept für die allgemeine Datenverarbeitung

1. Schulung der Mitarbeiter/-innen

- Die Mitarbeiterinnen und Mitarbeiter sind über die bei ihrer Tätigkeit anzuwendenden datenschutzrechtlichen Vorschriften zu unterrichten und zu schulen.
- Die Unterrichtung ist aktenkundig zu machen und zur Personalakte zu nehmen.

2. Tür- und Fenstersicherung

- Nicht besetzte Büro- und Arbeitsräume sowie die Archive sind abzuschließen.
- Die Schlüssel sind abzuziehen und sicher zu verwahren.
- Bei längerer Abwesenheit und Dienstende sind die Fenster zu schließen.

3. Aktenführung und Aktenaufbewahrung

- Akten, in denen personenbezogene Daten verarbeitet werden, sind so aufzubewahren, dass eine Einsichtnahme durch unbefugte Dritte nicht möglich ist. Sie sind grundsätzlich in verschlossenen Schränken aufzubewahren.
- Dies gilt auch für Vorgänge, die in der laufenden Bearbeitung sind (Clear-Desk-Anweisung).
- Bei Akten, die einem besonders schutzwürdigen Interesse unterliegen, entscheidet der jeweilige Verantwortliche über die darüber hinaus erforderliche Form der Aufbewahrung.

4. Archiv und Aufbewahrungsfristen

- Die Aufbewahrung von Akten im Archiv ist bereichsbezogen durchzuführen.
- Akten, die einem besonders schutzwürdigen Interesse unterliegen (z.B. Personalakten) sind vor der Einsichtnahme durch unbefugte Dritte besonders zu sichern.

5. Publikumsverkehr

- Es ist sicherzustellen, dass Kunden und Lieferanten bei ihrer Vorsprache in der jeweiligen Abteilung andere, als die ihre Angelegenheit betreffende personenbezogene Daten, nicht zur Kenntnis nehmen können. Dies gilt sowohl für Daten in Akten, als auch für automatisiert verarbeitete Daten.
- Bildschirme sind so aufzustellen, dass sie für Dritte nicht einsehbar sind.

6. Auskünfte, Datenübermittlung

- Bei einer Auskunftserteilung bzw. Datenübermittlung ist die Identität der bzw. des Ersuchenden zu prüfen und zu dokumentieren.
- Die Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten hat grundsätzlich nur aufgrund einer schriftlichen Anfrage auf schriftlichem Wege zu erfolgen und auch nur aufgrund eines rechtlichen Anspruchs.

III. Sicherheitskonzept für die automatisierte Datenverarbeitung

1. PC-Benutzer/-innen

- Die PC-Benutzerinnen und PC-Benutzer sind vor Aufnahme der Arbeit an PCs umfassend zu schulen.
- Die PC-Benutzerinnen und PC-Benutzer sind selbst für die ordnungsgemäße Nutzung der ihnen zur Verfügung gestellten Hard- und Software zuständig.
- Sie sind über die grundsätzlichen Datensicherungsmaßnahmen aufzuklären.

2. Kennwörter

- An jedem PC ist ein passwortgeschützter Bildschirmschoner einzurichten. Die Aktivierungszeit darf 10 Minuten nicht überschreiten.

3. Hardware und Software

- Ein Umstellen der Geräte innerhalb der Abteilung ist der IT-Administration zwecks Berichtigung des Geräteverzeichnisses zu melden.
- Private Hard- und Software darf am Arbeitsplatz nicht eingesetzt werden.
- Die private Nutzung von dienstlicher Hard- und Software ist nicht zulässig.

4. Arbeitsplatz-PC

- Die IT-Administration stellt die Installation, Konfiguration und den Netzzugang der PCs sicher.
- Es sind ausschließlich die für die dienstliche Aufgabe notwendigen Funktionen und Anwendungen zu installieren. Die Entscheidung hierüber trifft die IT.

5. Mobile PCs (Notebooks)

- Die Verarbeitung personenbezogener Daten außerhalb darf nur auf dienstlichen Notebooks zu dienstlichen Zwecken erfolgen.

6. Zentrale Drucker

- Werden Drucker für zentrale Druckaufträge aufgestellt, ist darauf zu achten, dass Ausdrucke mit personenbezogenen Daten nicht unbeaufsichtigt erfolgen.

7. Datenverwaltung

- Sensible Dateien sind mit Kennwortschutz abzulegen.
- Die dauerhafte Speicherung von Dateien als Muster oder Textbausteine ist nur zulässig, wenn sie anonymisiert werden.
- Dienstliche Daten dürfen nicht auf privaten Rechnern und private Daten nicht auf dienstlichen Rechnern gespeichert werden.

IV. Sicherheitskonzept für die Internetdienste

1. Allgemein

- Die Überwachung der Internet-Kommunikation erfolgt durch die IT-Administratoren.

2. E-Mail

- E-Mail-Eingänge sind wie allgemeine Posteingänge zu behandeln.
- Vorgangsbezogene E-Mails und Faxe sind zu archivieren.
- Attachments mit ausführbaren Programmen und Dateien (Dateiendungen: z. B. EXE, COM, BAT und VBS) sind auf den Arbeitsplätzen (Benutzerebene) nicht zugelassen.

3. World Wide Web

- Der Zugriff auf das WWW ist nur für dienstliche Aufgaben freigegeben.
- Zugriffe auf Seiten ohne dienstlichen Bezug sind zu unterlassen.
- Der Zugriff auf Web-Seiten enthaltene Verknüpfungen (Links) auf andere nicht zugelassene Web-Seiten sind zu unterlassen.
- Das Herunterladen ausführbarer Programme und Dateien (Dateiendung: z. B. EXE, COM, BAT und VBS) ist auf den Arbeitsplätzen (Benutzerebene) nicht zugelassen.

4. Mobiltelefone (Handys/Smartphones/Tablets)

- Die Sim-Karte ist mit einer Geheimnummer (PIN) zu versehen.
- Die PIN ist nur berechtigten Personen zu nennen und verschlossen, getrennt von der SIM-Karte, aufzubewahren.
- Der Verlust des Gerätes der SIM-Karte oder PIN ist unverzüglich der IT zu melden.
- Das Smartphone oder Tablet ist mit einen Code vor unbefugter Benutzung zu sichern.
- Das Gerät ist ausschließlich für den dienstlichen Gebrauch.
- Tablets sind nach der Benutzung wieder abzugeben.
- Die Smartphones oder Tablets werden zentral verwaltet und können bei Verlust gelöscht und deaktiviert werden.