Datenschutzkonzept (TOM)

der

PriSend

Druck . Service . Logistik

gemäß

ISO / IEC 27001 und DS-GVO

Inhaltsverzeichnis

I. Grundlagen und Aufbau: Zielrichtung:

Bei der Pri/Send wird bei der Datenverarbeitung nach folgendem Datenschutzkonzept verfahren:

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.
Die Sicherheitsmaßnahmen werden in dem Datenschutzkonzept in die Bereiche

- Allgemeine Datenverarbeitung
- Automatisierte Datenverarbeitung
- Versand von Daten (auch nichtelektronischer)
- Nutzung der Internetdienste
- Nutzung der Telekommunikationsdienste

und Zusatzmaßnahmen für sensible personenbezogene Daten gegliedert und geben mithin ein hohes Sicherheitsniveau vor.

Die festgelegten Sicherheitsmaßnahmen gelten als Mindestanforderungen.

Grundlagen für die Festlegung der Sicherheitsmaßnahmen bilden die durchgeführte Bestandsaufnahme zur Ermittlung der Datensicherheitssituation.

Zuständig- und Verantwortlichkeiten:

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung trägt die Geschäftsführung. Die zentralen Datenschutzfunktionen obliegen dem Datenschutzbeauftragten.

Der Datenschutzbeauftragte ist dabei insbesondere für den Erlass von Dienstanweisungen und Regelungen zum Datenschutz und zur Datensicherheit zuständig, die die gesamte Firma betreffen. Dies gilt sowohl für den allgemeinen, konventionellen Datenschutz als auch für den technischen Datenschutz.

Überwachung:

Die Überwachung und Prüfung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen obliegt dem Datenschutzbeauftragten.

II. Sicherheitskonzept für die allgemeine Datenverarbeitung: Schulung der Mitarbeiter/-innen:

Die Mitarbeiterinnen und Mitarbeiter sind über die bei ihrer Tätigkeit anzuwendenden datenschutzrechtlichen Vorschriften zu unterrichten und zu schulen. Während der Einarbeitungszeit hat eine umfassende Unterrichtung über die einschlägigen Datenschutzbestimmungen zu erfolgen. Die Unterrichtung ist aktenkundig zu machen und zur Personalakte zu nehmen.

Datenschutzrechtliche Vorschriften müssen fester Bestandteil der Fortbildungsplanung der jeweiligen Organisationseinheiten sein. Dies schließt auch die Fortbildung im Umgang mit technikunterstützter Informationsverarbeitung und den daraus resultierenden Datensicherheitsmaßnahmen ein.
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.

Datenführung und Datenaufbewahrung:

Die Daten der Kunden und deren Postsendungen sind sicher und vor fremden Zugriff geschützt aufzubewahren und zu transportierten.

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. Bei Akten, die einem besonders schutzwürdigen Interesse unterliegen, entscheidet die jeweilige Organisationseinheit über die darüber hinaus erforderliche Form der Aufbewahrung. Für die Vernichtung von Papierabfällen sind Schredder vorzusehen.

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 Einsichtsnahme durch unbefugte Dritte besonders zu sichern.

Akten und die damit verarbeiteten personenbezogenen Daten sind grundsätzlich zu löschen, wenn sie für die Aufgabenerledigung nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen. Die Akten sind einer physikalischen Vernichtung zuzuführen, bei der gewährleistet ist, dass unbefugte Dritte keine Einsicht nehmen können.

Den Ablauf der Frist überwacht die für die Aktenführung zuständige Organisationseinheit.

Reinigungs- und weiteres Servicepersonal:

Das Personal das von Dritten in unserem Auftrag tätig ist, ist rechtswirksam zur Einhaltung unserer Datenschutzbestimmungen zur verpflichten. Hierzu gibt es eine Übersichtliste über das Vorliegen einer solchen Vereinbarung.
Dieses Servicepersonal darf nur den Büro- und Arbeitsraum sich aufhalten, denen die Arbeti erbracht werden muss.

Auskünfte, Datenübermittlung:

Bei einer Auskunftserteilung bzw. Datenübermittlung ist die Identität der bzw. des Ersuchenden zu prüfen.

Die Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten hat grundsätzlich nur aufgrund einer schriftlichen Anfrage auf schriftlichem Wege zu erfolgen.

Die jeweiligen Organisationseinheiten entscheiden selbständig über die Erforderlichkeit und die Festlegung von einheitlichen Verfahrensregelungen für die Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten an Dritte.

III. Sicherheitskonzept für die automatisierte Datenverarbeitung:

Systemadministrator(en):
Die Systemadministrator(en) stellen den Einsatz und den Betrieb der IT-Systeme sicher. Die durchzuführenden Aufgaben und Zuständigkeiten der Systemadministrator(en) sind in einer Dienstanweisung festzuschreiben.
Die Systemadministrator(en) haben grundsätzlich Zugriffsrechte auf alle PCs und Server.
Ein Zugriff auf verschlüsselte Datenbestände darf nur unter Beteiligung autorisierter Mitarbeiterinnen und Mitarbeiter des jeweiligen Bereichs erfolgen.

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.

Kennwörter:
Für alle PC-Benutzerinnen und PC-Benutzer sind Zugangskennungen für das Netzwerk und für die Verfahren zu vergeben.

Dabei sind neben Benutzernamen auch mindestens 8-stellige Kennworte zu verwenden.

Die Hinweise des Landesbeauftragten für Datenschutz / Bundesdatenschutzbeauftragten sind zu beachten. Die Kennworte müssen alle 90 Tage gewechselt werden. Die Anzahl der Anmeldeversuche ist zu begrenzen. Nicht erfolgreiche Anmeldeversuche sind aufzuzeichnen. An jedem PC ist ein passwortgeschützter Bildschirmschoner einzurichten. Die Aktivierungszeit darf 3 Minuten nicht überschreiten.

Externe Dienstleister/-innen:
Der Leistungsumfang externer Dienstleisterinnen und Dienstleister ist durch schriftlichen Vertrag zu regeln. Im Vertrag sind die durchzuführenden Aufgaben abschließend zu beschreiben. Die Dienstleisterinnen und Dienstleister sind zu verpflichten, Daten, die ihnen durch ihre Tätigkeit bekannt werden, vertraulich zu behandeln.

Die von der Dienstleisterin oder dem Dienstleister durchgeführten Aktivitäten sind zu protokollieren.

Fernadministration hat auf gesicherten Leitungen unter Verwendung von einmaligen Passworten zu erfolgen. Die Leitungen sind nach Ende der Tätigkeit wieder zu sperren. Die Administration ist von den [internen] Systemadministratoren zu überwachen.

Hardware und Software:
Sämtliche Hard- und Software ist unter Beachtung der Datenschutzanforderung zu beschaffen.

Bei Lieferung sind sämtliche Geräte, die Datenschutzrelevant sind, zu prüfen und durch den Datenschutzbeauftragten freizugeben.

Die Konfigurationsdaten der eingesetzten Hard- und Software (IP-Adressen etc.) sind vor unbefugtem Zugriff zu schützen.

Bei Entfernung der Geräte (Reparatur, Verschrottung etc) ist der Verbleib dahingehend sicher zu stellen, dass keine Datenschutzprobleme entstehen – physikalische Löschungen sind vorzunehmen.

Bei Weitergabe an Dritte (z. B. Schulen, Verkauf an Mitarbeiter/innen) ist sicherzustellen, dass die auf den Festplatten gespeicherten Daten physikalisch gelöscht und keine Rekonstruktion möglich ist.

Es ist grundsätzlich Standardsoftware einzusetzen. Open Source Lösungen ist bei sonstiger Gleichheit der Vorzug vor proprietären Lösungen zu geben. Die Originalsoftware ist durch die Geschäftsleitung gesichert aufzubewahren.

Private Hard- und Software darf am Arbeitsplatz nicht eingesetzt werden. Die private Nutzung von dienstlicher Hard- und Software ist nicht zulässig oder muss durch die Geschäftsleitung erlaubt werden.

Arbeitsplatz-PC:

Beim Auf- oder Umstellen der Geräte ist auf geeignete Standorte (Lichtverhältnisse, Ergonomie, Ausschluss der Bildschirmeinsicht durch Fremde) zu achten.

Die PC-Benutzerinnen und PC-Benutzer sind durch die Systemadministratoren in die Bedienung der Geräte einzuweisen.

Vorhandene Disk/CD-Laufwerke bzw. USB-Schnittstellen o.ä. sind, soweit möglich, mittels eines passwortgeschützen BIOS zu deaktivieren. Sollte für die Aufgabenerfüllung ein geöffnetes Laufwerk erforderlich sein, sind die PC-Benutzerinnen und PC-Benutzer schriftlich zu verpflichten, das Laufwerk lediglich für diesen Zweck zu nutzen. Es ist dann zusätzlich durch mechanische Maßnahmen zu sichern.

Der Systemadministrator stellt die Installation, Konfiguration und den Netzzugang der PCs sicher.

Es sind ausschließlich die für die dienstliche Aufgabe notwendigen Funktionen und Anwendungen zu installieren.

Zentrale Rechner (Server):

Die Server sind soweit möglich in zentralen Serverräumen oder in einem abschließbaren Behältnis aufzustellen. Die Festplatten der Server sind als Raid-Systeme zu konfigurieren. Sämtliche an Servern vorgenommene Arbeiten (Einstellungen oder Reparaturen) sind in einer Datei zu dokumentieren.

Mobile PCs (Notebooks):

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

Zentrale Drucker:

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

Datenverwaltung:

Alle Datenbestände sind zentral zu speichern. Die Daten sind durch Zugriffsrechte auf dem jeweiligen Server voneinander abzugrenzen.

Sensible Dateien sind mit Kennwortschutz abzulegen. Die Vergabe der Kennwörter ist einheitlich durch das entsprechende Team festzulegen.

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

Datensicherung:

Die Daten sind täglich zu sichern. Die Datensicherungsmedien sind diebstahl- und datensicher aufzubewahren.

Datenträger:

Externe Datenträger sind vor ihrem Einsatz durch bevollmächtige Mitarbeiter/innen auf vorhandenen schädigenden Code (z. B. Viren) zu prüfen.

Das gleiche gilt, wenn dienstliche Daten auf externen Datenträgern gespeichert und weitergegeben werden sollen.

Die Datenträger sind eindeutig zu kennzeichnen.

Nicht mehr benötigte Datenträger werden durch einen zertifizierten Dienstleister (Reisswolf) entsorgt.

Jedes Verfahren ist vor dem Einsatz mit einem Testdatenbestand zu testen und von der Geschäftsführung freizugeben. Test und Freigabe müssen für jede Programmaktualisierung erneut durchgeführt werden.

Die Rechte für den Zugriff auf die Verfahren sind von der Geschäftsführung zu regeln. Sie sind innerhalb der Verfahren auf das notwendige Maß zu beschränken und zu dokumentieren.

Die Rechteverwaltung ist durch die Systemadministratoren wahrzunehmen.

IV. Sicherheitskonzept für die Internetdienste: Allgemein

Der Leistungsumfang des Providers ist in einem Vertrag festzulegen. Es ist insbesondere darzustellen, auf welche Daten der Provider zugreifen kann.
Daten über den Ablauf der Internetkommunikation, die nicht für Abrechnungs- oder angeordnete Überwachungszwecke gespeichert werden, müssen unmittelbar nach Beendigung gelöscht werden.

Die eingesetzten Internet-Komponenten sind über ihren Funktionsumfang und über ihren Einsatz ausreichend zu dokumentieren. Die Nutzung der Internetdienste ist in einer gesonderten Dienstanweisung zu regeln.

Die Systemadministratoren sind für die Betreuung der Internet-Komponenten (Hard- und Software) ausreichend zu schulen.

Die Befugnisse bzw. Zugriffsberechtigungen der Systemadministratoren sind festzulegen. Die Administration der Internet-Komponenten ist zu protokollieren.
Veränderungen der Sicherheitseinstellungen sind nur mit Zustimmung der Leitungsebene durchzuführen.
Die festgelegten Sicherheitsmaßnahmen sind auf ihre Wirksamkeit hin in regelmäßigen Abständen zu testen. Der Testumfang ist schriftlich vorzugeben. Die Testergebnisse sind zu dokumentieren.
Die Überwachung der Internet-Kommunikation erfolgt durch die Systemadministratoren.
Physikalische Ebene
Die Übergänge vom internen Netz zum externen Netz sind durch Firewall-Systeme (z. B. Router, Gateways etc.) zu schützen.
Die Verbindung zum „E-Mail-Provider" ist nur nach Bedarf ausgehend aufzubauen.
Die Verfügungsgewalt (Überwachung und Administration) über die eingesetzten Firewall Komponenten (Router, Gateways etc.) im Bereich der Netzübergänge (intern/extern) liegt bei dem Teamleiter Verwaltung.

Es muss sichergestellt werden, dass Angriffe auf der physikalischen Ebene erkannt und abgewehrt werden.

Es ist nach dem Grundsatz - Es ist alles verboten, was nicht erlaubt wurde - zu verfahren. Eine Fernadministration der Firewall-Komponenten ist nicht gestattet.

Funktionalitäten (Dienste, Ports etc.) der Firewall-Komponenten, die nicht für die Internet- Kommunikation benötigt werden, sind zu deaktivieren.
Die Einstellungen der einzelnen Komponenten des Firewall-Systems sind zu dokumentieren.
Datenschutzkonzept

E-Mail:

E-Mail-Eingänge sind wie allgemeine Posteingänge zu behandeln.
Für alle PC-Benutzerinnen und PC-Benutzer sind eindeutige E-Mail-Adressen vorzuhalten. E-Mails sind grundsätzlich verschlüsselt zu versenden. Dafür werden geeignete Programme vom Systemadministrator zur Verfügung gestellt.

Die Schlüsselverwaltung wird von der Geschäftsführung durchgeführt und beaufsichtigt.

E-Mails und die an ihnen angehängten Attachments (Dateien) sind einer Virenüberprüfung zu unterziehen. Die dazu eingesetzte Virenschutzsoftware ist täglich zu aktualisieren.

Attachments mit ausführbaren Programmen und Dateien (Dateiendungen: z. B. EXE, COM, BAT und VBS) sind auf den Arbeitsplätzen (Benutzerebene) nicht zugelassen. E-Mails dieser Kategorie sind in ein separates zentrales Fach der administrativen Ebene umzuleiten. Sofern diese E-Mails dienstlich nicht angefordert wurden, werden sie ohne weitere Überprüfung gelöscht.

WWW:

Der Zugriff auf das WWW ist nur für dienstliche Aufgaben einzurichten.

Die Eingrenzung bzw. Deaktivierung von WWW-Seiten ist mittels Sicherheitssoftware zu realisieren, wenn dies notwendig erscheint.

Die Web-Seiten sind in Bezug auf Computerviren (schädliche Java-Applets und ActiveX-Controls) in regelmäßigen Abständen zu überprüfen.

Das Herunterladen ausführbarer Programme und Dateien (Dateiendung: z. B. EXE, COM, BAT und VBS) ist auf den Arbeitsplätzen (Benutzerebene) nicht zugelassen oder muss durch die Geschäftsleitung genehmigt werden.