Informationsblatt

Tipps und Hinweise an die Gemeinden zum Thema Informationssicherheit

—

ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

EC 915

Bearbeiten Personenbezogener/sensibler Daten

Zugang zum Informationssystem

- Der Zugang zum Informationssystem muss **persönlich** und **individuell** sein (Login + Passwort).
- Der Zugang muss auf **die Daten (Anwendungen und Dateien) beschränkt sein, die die Benutzer/innen (einschliesslich externe Gesellschaften) benötigen,** um ihre Aufgaben zu erfüllen (nach dem Prinzip «need to know, need to do»).
- Erstellen Sie eine **Zugriffsrechtematrix**, die angibt, welche Benutzer welche Zugriffe (Lesen, Übertragen, Löschen, etc.) auf welche Daten haben, mit den Namen der Personen, die berechtigt sind, diese Zugriffsrechte zu ändern. Diese Liste der Zugriffsrechte sollte regelmässig aktualisiert werden.
- Die Zugriffsrechte liegen in der Verantwortung eines oder mehrerer Datenverantwortlicher (zu definieren).
- Sorgen Sie für die Einrichtung einer **starken Authentifizierung** (Name + Passwort + Code) für den Zugriff auf sensible Anwendungen von ausserhalb Ihrer Organisation.
- Erlauben Sie keinen Fernzugriff durch externe Dienstleistende auf einen Computer Ihrer Organisation ohne zu überprüfen, was getan wird, und ohne zuerst sensible Anwendungen zu schliessen.

Datentransport

- Schützen Sie sensible Dokumente, wenn Sie sie aus den Räumlichkeiten Ihrer Organisation mitnehmen:
  - Um Diebstahl oder Verlust von Dokumenten in elektronischer Form zu verhindern, verwenden Sie **gesicherte Laptops mit verschlüsselten Festplatten;**
  - führen Sie ausgedruckte Dokumente in einer **mit Schloss gesicherten Mappe** mit sich.
- Lassen Sie Ausdrucke oder beruflich genutzte elektronische Hardware nie in einem geparkten Fahrzeug zurück und bewahren Sie sie an einem sicheren Ort auf, wenn es nicht möglich ist, sie ins Büro zurückzubringen.
- **Sie tragen die Verantwortung für die Informationen in den von Ihnen mitgenommenen Dokumenten.**

Datenaufbewahrung

- Sorgen Sie für ein **hohes Schutzniveau** für alle sensiblen Daten, unabhängig von der Form (Ausdrucke, elektronische Dateien usw.) sowie von Aufbewahrungsort und -dauer.
- Lassen Sie **sensible Dokumente** nicht beim **Drucker** liegen.
- Persönliche und vertrauliche Informationen müssen:
  - **unter Verschluss gehalten**, vor neugierigen Blicken und Diebstahl geschützt werden (Ausdrucke);
  - **in Ordner (Verzeichnisse) abgelegt werden,** die durch Zugriffsrechte geschützt sind, die nur für die zur Bearbeitung berechtigten Personen gelten.

Datenberichtigung

- Jede Informatikanwendung, die personenbezogene Daten verwaltet, sollte auf einem Datenkorrektursystem aufgebaut sein, um nachverfolgen zu können, wer was wann usw. geändert hat.
- Sensible Daten müssen regelmässig aktualisiert werden.

Datenspeicherung

- Vergewissern Sie sich, dass **das Datensicherungssystem** richtig funktioniert.
- **Digitalisieren** Sie möglichst viele Dokumente zur Gewährleistung der Integrität und Vollständigkeit der Daten.
- Stellen Sie sicher, dass die **Datenbanken**, die sensible Daten enthalten, **verschlüsselt** sind oder dass die Mittel zum Schutz dieser Daten angemessen sind.
- Bewahren Sie die Sicherungsbänder in sicheren Räumen und in abschliessbaren Schränken auf.

Datenvernichtung

- Nach Ablauf der gesetzlichen Aufbewahrungsfrist müssen sensible Daten auf konventionelle Weise (**Aktenvernichter** oder **Verbrennungsanlage**) vernichtet werden.
- Das Vorgehen bei der Entsorgung ausgedienter Hardware und Drucker sollte genau definiert sein (**Überschreiben von Festplatten, Zurücksetzen von Smartphones usw.**).

Datenbearbeitung

- Jede Datenbearbeitung muss rechtmässig sein und nach den **Grundsätzen von Treu und Glauben und Verhältnismässigkeit** erfolgen.
- Personendaten dürfen nur zu dem **Zweck** bearbeitet werden, der für ihre Beschaffung angegeben wird, der in einer gesetzlichen Bestimmung vorgesehen ist oder sich aus den Umständen ergibt.
- Die Erhebung personenbezogener Daten muss für die betroffene Person **erkennbar** sein.
- Die Art und Weise, wie die einzelnen Dateien verwaltet werden, muss **bei jedem Bearbeitungsschritt** definiert werden (Anlegen, Bearbeiten, Bekanntgabe, Archivierung, Löschen usw.).
- Ein **Anonymisierungsprozess** sollte so oft wie möglich durchgeführt werden, insbesondere beim Austausch sensibler Informationen.

E-Mail

–

› Verschicken Sie **keine unverschlüsselten** E-Mails mit amtlichen, personenbezogenen oder sensiblen Daten.
› Ausserhalb des Netzwerks des Staates Freiburg:
  • verwenden Sie ein Verschlüsselungssystem;
    oder
  • schützen Sie die Dokumente mit einem **starken Passwort** (Bekanntgabe über einen anderen Kanal wie SMS oder Telefon).
› Schicken Sie keine **beruflichen Informationen** an eine **Privatadresse**.
› Schicken Sie keine **sensiblen Informationen** an einen **generischen elektronischen Briefkasten.**
› Klären Sie im E-Mail-Verkehr immer ab, worum es genau geht und mit wem Sie es zu tun haben.

Internet

–

› **Verwenden Sie NIE Ihr Windows-Passwort oder das Passwort für eine Business-Software im Internet.**
› Falls Sie eine Software zur Übertragung von Dateien über einen Webbrowser (https://www.grosfichiers.com/de/ zum Beispiel) verwenden, benützen Sie ein starkes Passwort, um die Dateien vor der Übermittlung zu verschlüsseln.
› **Achtung:** Dateiübertragungssoftware speichert in der Regel keine Dateien in der Schweiz.

Telefon

–

› **Seien Sie sich sicher, mit wem Sie es zu tun haben,** bevor Sie Informationen herausgeben.
› Geben Sie Informationen telefonisch **nur Personen oder amtliche Stellen bekannt**, denen Auskunft erteilt werden darf:
  • rufen Sie die Kontaktperson auf ihre Büronummer zurück, um sicherzugehen, dass sie die Person ist, für die sie sich ausgibt;
    oder
  • stellen Sie Fragen, mit denen sich feststellen lässt, ob eine falsche Identität vorgetäuscht wird.

Post

–

› Stellen Sie sicher, dass die Posteingangs- und Ausgangskästen für unberechtigte Personen nicht zugänglich sind.
› Bestimmen Sie die Regeln für die Weiterleitung von Einschreiben.

Mobilgeräte und Wechselmedien

Mobilgeräte

- Bewusstsein für die Speicherung und Sicherung sensibler Daten auf mobilen Geräten schärfen.
- Verwenden Sie eine MDM-Anwendung (Mobile Device Management) zur Fernverwaltung geschäftlicher Daten, insbesondere bei Verlust oder Diebstahl.
- Schützen Sie jedes mobile Gerät (Smartphone, Tablet), das für geschäftliche Zwecke verwendet wird, mit einem komplexen Passwort.
- Regeln Sie die Verwendung privater Mobilgeräte am Arbeitsplatz.
- Verschlüsseln Sie so weit wie möglich mobile Geräte (Smartphone, Tablet, Laptop, etc.).

Wechselmedien

- Führen Sie ein Inventar aller Wechseldatenträger und bestimmen Sie die Regeln für deren Verwendung.
- Stellen Sie bei Bedarf verschlüsselte USB-Sticks für den internen Gebrauch bereit.
- Setzen Sie sich für die systematische Nutzung des VPN für den Zugriff auf das Informationssystem von ausserhalb Ihrer Organisation ein und schärfen Sie das Bewusstsein für die Gefahren des WLAN.

Mitarbeitende

Stellenantritt neuer Mitarbeitender

- Lassen Sie allen neuen Mitarbeitenden die Sicherheitsrichtlinien zukommen.
- Infomieren Sie externe Dienstleistende über die Sensibilität der bearbeiteten Informationen.

Austritt von Mitarbeitenden

- Löschen Sie die Konten von Mitarbeitenden, die die Organisation verlassen.
- **Deaktivieren Sie den Zugriff auf das Informationssystem und die Anwendungen.**
- Sperren Sie den physischen Zugang zu Gebäuden.
- **Ändern Sie allfällige Gruppenpasswörter,** insbesondere wenn sie für den Zugriff auf Webanwendungen erstellt wurden.

Bei der Arbeit

- **Immer wieder Bewusstsein schaffen für die Informationssicherheit** bei allen, die auf das Informationssystem zugreifen (Mitarbeitende, Auszubildende, externe Dienstleistende falls erforderlich, usw.). Thematisiert werden können beispielsweise:
  - Passwortverwaltung
  - Internetnutzung
  - Nutzung sozialer Netzwerke
  - Umgang mit «Social Engineering»
  - Verhalten bei Identitätsdiebstahl
  - E-Mail-Nutzung
  - Gefahren der Mobilität usw.
- **Hinweis:** Der richtige Umgang mit Business- und Office-Software hat Auswirkungen sowohl auf die Arbeitseffizienz als auch auf die Sicherheit.

Zugang zu den Räumen

- Statten Sie die Räume mit einem **Brandmeldesystem und/oder einer Einbruchsicherung aus,** wenn sensible Daten in ausgedruckter Form aufbewahrt werden (Archiv oder anderes).
- Schliessen Sie die Büros ab.
- Verlangen Sie von Ihren Mitarbeitenden, dass sie ihren Schreibtisch am Ende des Tages oder bei Kundenbesuchen aufräumen.
- Alle Personen (intern oder extern) müssen eine Berechtigung für den (physischen) Zugang haben.
- **Lassen Sie Personen von ausserhalb nicht alleine Räume betreten, in denen sensible Daten aufbewahrt werden.**

Vertraulichkeitserklärung

- Sorgen Sie dafür, dass mit **allen externen Dienstleistenden eine Vertraulichkeits-vereinbarung abgeschlossen wird** (im IT-Bereich oder in einem anderen Bereich).

Arbeitsplatz

- **An erster Stelle für den Schutz vor unbefugtem Zugriff steht das Sperren der Arbeitsstation (Desktop und mobile Geräte).**
- Lassen Sie den Zugriff auf das Informationssystem, wichtige Anwendungen und mobile Geräte nach maximal drei bis fünf Verbindungsfehlern sperren.
- **Speichern Sie Dateien auf den Netzwerkservern** und nicht auf Desktops oder mobilen Geräten.
- Installieren Sie ein **Passwort-Registrierungstool** für eine bessere Passwortverwaltung durch die Benutzerinnen und Benutzer.
- Richten Sie ein Verbindungssystem mit einem einheitlichen Passwort für den Zugriff auf alle Business-Anwendungen ein.
- Richten Sie ein P**asswortkontrollsystem** für (komplexe) Passwörter zur Einhaltung der guten Sicherheitspraktiken ein.
- Lassen Sie die Benutzerinnen und Benutzer die Konfiguration ihres Computers nicht selber ändern oder Software installieren.

Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB
Chorherrengasse 2, CH-1700 Freiburg
T +41 26 322 50 08
-
www.fr.ch/de/oedsb
-
April 2019
-
Quelle
Der Inhalt dieses Dokuments ist eine Zusammenfassung der Tipps und Hinweise, die an Gemeinden oder andere Verwaltungen zum Thema Informationssicherheit abgegeben worden sind.