Datenschutzkonzept

der Gemeinde Ilvesheim

Inhaltsverzeichnis

I. Grundlagen und Aufbau

1. Zielrichtung

Bei der Gemeinde Ilvesheim wird für die 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
- 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** für alle Bereiche der Gemeinde Ilvesheim (inkl. der Außenstellen) sowie für den Eigenbetrieb Wasser und die Gemeindestiftung.

In den Bereichen, in denen sensible Daten (z.B. Personal- oder Sozialdaten) vorhanden sind, werden über die Mindestanforderungen hinaus angemessene **Zusatzmaßnahmen** getroffen. Ihre Festlegung erfolgt gesondert durch die zuständige Amtsleitung (z.B. die speziellen Anforderungen an den Beschäftigtendatenschutz).

Grundlage für die Festlegung der Sicherheitsmaßnahmen bilden

- die bei der Gemeinde Ilvesheim durchzuführende Bestandsaufnahme zur Ermittlung der Datensicherheitssituation (Arbeitsplatzbegutachtung, Risikoanalyse, etc.)
- die IT-Konzepte im Rahmen der technisch organisatorischen Maßnahmen (TOMs) in der jeweils geltenden Fassung sowie
- Dokumentationsunterlagen über die Zusammensetzung der IT-Systeme.

2. Zuständig- und Verantwortlichkeiten

- Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Daten-Verarbeitung bei der Gemeinde Ilvesheim trägt der Bürgermeister als Vertreter der verantwortlichen Stelle.

- Regelungen zur Delegation sind im Organigramm der Gemeinde Ilvesheim der Anlage 1 zu entnehmen.

- Die verantwortliche Stelle ist dabei insbesondere für den Erlass von Dienstanweisungen und Regelungen zum Datenschutz und zur Datensicherheit zuständig. Dies gilt sowohl für den allgemeinen, konventionellen Datenschutz als auch für den technischen Datenschutz.

- Für die Einhaltung der jeweils anzuwendenden Vorschriften zum Datenschutz und zur Datensicherheit sind die Amtsleiterinnen und Amtsleiter sowie die Leiterinnen und Leiter der Einrichtungen zuständig und verantwortlich.

- Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu vermeiden und gegebenenfalls aufzulösen. Alle Regelungen sollten deshalb auch ein Erstellungsdatum oder eine Versionsnummer enthalten

3. Überwachung

Die Überwachung und Prüfung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen obliegt der verantwortlichen Stelle. Die Personalvertretung sowie die/der behördliche Datenschutzbeauftragte ist entsprechend zu beteiligen. Die Ergebnisse sind im Rahmen der Dokumentationspflicht schriftlich festzuhalten.

4. Fortschreibung

Das Datenschutzkonzept ist im Zusammenhang mit den technisch organisatorischen Maßnahmen (Art. 24 ff. EU-DSGVO) regelmäßig fortzuschreiben. Dabei ist zu prüfen, ob sich die Datensicherheitsmaßnahmen bewährt haben.

5. Inkrafttreten

Das Datenschutzkonzept tritt am 01.10.2019 in Kraft.

Ilvesheim, den

Andreas Metz
Bürgermeister

II. Sicherheitskonzept für die allgemeine Datenverarbeitung

1. Schulung der Mitarbeiter/-innen

- Die Mitarbeiterinnen und Mitarbeiter sind über die datenschutzrechtlichen Vorschriften zu unterrichten und zu schulen.

- Die Kenntnisse über die in der Tätigkeit des Mitarbeiters liegenden Datenschutz-bestimmungen hat sich der Mitarbeiter durch entsprechende Fortbildungen anzueignen (jeweils anzuwendende Fachgesetze).

- 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.

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

- Die mittels Standard- oder Fachsoftware verarbeiteten Daten sind nur auszudrucken und in die Akte zu nehmen, sofern dies gesetzlich vorgeschrieben ist oder für die Aufgabenerfüllung als erforderlich angesehen wird.

- Akten, in denen personenbezogene Daten verarbeitet werden, sind so aufzubewahren, dass eine Einsichtnahme durch unbefugte Dritte nicht möglich ist. Sie sind grundsätzlich in Schränken oder anderen zur Aktenaufbewahrungen geeigneten Möbeln aufzubewahren. Dies gilt auch für Vorgänge, die in der laufenden Bearbeitung sind (Clear-Desk- Anweisung).

- Bei Akten, die einem besonders schutzwürdigen Interesse unterliegen, entscheidet die jeweilige Organisationseinheit über die darüber hinaus erforderliche Form der Aufbewahrung.

- Papierabfälle, die personenbezogenen Daten enthalten, sind in den lokalen Aktenvernichtern, oder den dafür vorgesehenen Behältnissen (Im Keller) zu entsorgen.

4. Archiv und Aufbewahrungsfristen

- Die Aufbewahrung von Akten im Archiv ist bereichsbezogen durchzuführen.

- Akten, die einem besonders schutzwürdigen Interesse unterliegen (z.B. Personal- und Sozialakten) sind vor der Einsichtnahme 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. Dies betrifft sowohl elektronisch, als auch in Papier geführte Akten.

- Die Akten sind einer Vernichtung (z.B. Schreddern) zuzuführen, bei der gewährleistet ist, dass unbefugte Dritte keine Einsicht nehmen können.

- Soweit keine gesetzlichen Aufbewahrungsfristen bestehen, sind grundsätzlich die aktuellen Aufbewahrungsempfehlungen der KGSt, in der jeweils vorliegenden Fassung anzuwenden.

- Den Ablauf der Frist überwacht die für die Aktenführung zuständige Fachabteilung.

5. Reinigungspersonal

- Das Reinigungspersonal darf nur den Büro- und Arbeitsraum öffnen, in dem die Reinigung erfolgen soll.

- Die Kontrolle der Einhaltung dieser Vorschriften ist sicherzustellen.

- Verstöße sind der Fachabteilung für die Vergabe der Reinigungsstellen unverzüglich zu melden.

6. Publikumsverkehr

- Es ist sicherzustellen, dass Bürgerinnen und Bürger bei ihrer Vorsprache in der jeweiligen Fachabteilung 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.

- Bei Mehrfacharbeitsplätzen sollten die Bürgerinnen und Bürger nur einzeln bedient werden. Sollte eine Mitarbeiterin oder ein Mitarbeiter mehrere Arbeitsplätze gleichzeitig nutzen, muss von allen beteiligten Bürgern das Einverständnis zur Mehrplatzbearbeitung eingeholt werden. Zum Zeitpunkt der Erstellung des Datenschutzkonzepts ist dies in der Gemeinde Ilvesheim nicht der Fall.

- Computermonitore sind so aufzustellen, dass sie für Dritte nicht einsehbar sind.

7. Auskünfte, Datenübermittlung

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

- Die jeweiligen Fachabteilungen 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

1. EDV

- Die EDV-Abteilung des Hauptamtes stellen den Einsatz und den Betrieb der IT-Systeme sicher.

- Die durchzuführenden Aufgaben und Zuständigkeiten der EDV-Abteilung sind im Organisationsplan festgeschrieben.

- Ein Zugriff auf verschlüsselte Datenbestände darf nur unter Beteiligung autorisierter Mitarbeiterinnen und Mitarbeiter des jeweiligen Fachamtes erfolgen. Gleiches gilt für den im Bedarfsfall notwendigen Zugriff auf Userprofile.

- Ein Zugriff auf das Persönliche Email Postfach, ohne Anwesenheit des Besitzers, ist nur in Ausnahmefällen unter Aufsicht – nach dem sechs Augen Prinzip - mit dem Datenschutzbeauftragten, dem Personalrat und dem Verantwortlichen des Fachamtes möglich.

2. PC-Benutzer/-innen

- Die PC-Benutzerinnen und PC-Benutzer sind vor Aufnahme der Arbeit an PCs umfassend zu schulen.

- Ihnen sind entsprechende Anleitungen zur Verfügung zu stellen.

- 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 grundsätzliche Speicherinfrastruktur aufzuklären.

3. 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 Kennwörter** zu verwenden (genaue Passwortanforderungen werden systemseitig vorgegeben).

- Kennwörter sind alle 90 Tage zu wechseln. Tipps für Passwörter sind im Anhang 2 beigefügt.

- Die Anzahl der Anmeldeversuche ist zu begrenzen.

- Beim Verlassen des Arbeitsplatzes ist die passwortgeschützte Bildschirmsperre zu aktivieren. Dazu kann z.B. auf Windows Betriebssystemen die Tastaturkombination Windowstaste + L gedrückt werden. Die Bildschirmsperre wird nach 10 Minuten der Nichtnutzung des PC's automatisch aktiviert.

4. Externe Dienstleister/-innen

- Der Leistungsumfang externer Dienstleisterinnen und Dienstleister ist durch einen schriftlichen Vertrag zu regeln. Die Erfordernisse der EU-DSGVO - insbesondere bei der Verarbeitung Personenbezogener Daten - an die Auftragsdatenverarbeitung (ADV) sind zu beachten.

- Im Vertrag sind die durchzuführenden Aufgaben abschließend zu beschreiben.

- Die Dienstleisterinnen und Dienstleister sind zu verpflichten, Daten die ihnen durch ihre Tätigkeit für die Gemeinde Ilvesheim bekannt werden, vertraulich zu behandeln (Kontrollen sind 1x jährlich durch den behördlichen Datenschutzbeauftragten durchzuführen, es sei denn der Auftragnehmer kann eine aktuelle DIN-ISO 27001 Zertifizierung vorweisen).

- 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 Administration ist durch den jeweilig betroffenen Mitarbeiter zu überwachen.

- Die Leitungen sind nach Ende der Tätigkeit wieder zu schließen.

5. Hardware und Software

- Hard- und Software ist grundsätzlich von der EDV-Abteilung zu beschaffen.

- Anwendungsspezifische Software kann ggf. über die zentrale Beschaffungsstelle des Hauptamtes bestellt werden.

- Bei Lieferung sind sämtliche Geräte durch Inventarisierung in der Kämmerei zu erfassen.

- Aus dem Geräteverzeichnis müssen sich der Aufstellungsort, die Geräteart, der Gerätetyp, die Seriennummer und das Lieferdatum ergeben. Weitere Angaben können jederzeit ergänzt werden.

- Ein Umstellen der Geräte innerhalb eines Fachamtes ist im Geräteverzeichnis zu berichtigen.

- 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 zu notieren.

- Vor einer Weitergabe an Dritte (z. B. Schulen, Verkauf an Mitarbeiter/innen) ist von der EDV-Abteilung sicherzustellen, dass die auf den Datenträgern gespeicherten Daten unwiederbringlich gelöscht sind. Sollte dies nicht möglich sein, sind die Datenträger auszubauen.

- Es ist grundsätzlich Standardsoftware einzusetzen.

- Die Originalsoftware ist durch die EDV-Abteilung gesichert aufzubewahren.

- Private Hard- und Software darf am Arbeitsplatz nicht eingesetzt werden.

- Die private Nutzung von dienstlicher Hard- und Software außerhalb der vorhandenen Dienstanweisungen für den Bereich EDV ist nicht zulässig.

6. Arbeitsplatz-PC

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

- Die EDV 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 das Fachamt.

7. Zentrale Rechner (Server)

- Die Server sind soweit möglich in zentralen Serverräumen oder in einem abschließbaren, für den Serverbetrieb zugelassenen Schrank aufzustellen.

- Jeder Server ist mit einer unterbrechungsfreien Stromversorgung (USV) auszustatten, die Funktion ist in regelmäßigen Abständen zu überprüfen und zu protokollieren.

- Die Festplatten der Server sind mind. als Raid-5-Systeme zu konfigurieren.

8. Mobile Devices (Notebooks, Tablets, Smartphones)

- Die Verarbeitung personenbezogener Daten außerhalb der Diensträume der Gemeinde Ilvesheim, darf nur auf dienstlichen Geräten zu dienstlichen Zwecken erfolgen.

- Der Zugang ist durch Passwort zu schützen (siehe Punkt 3. Kennwörter).

- Die Nutzungsvereinbarung der Gemeinde Ilvesheim für Mobile Devices ist zu beachten.

- Datenträger in Laptops sind zu verschlüsseln.

- Die Vorgenommenen Einstellungen sind zu dokumentieren.

9. Netzstruktur/Verteiler

- Die in der Gemeinde Ilvesheim, oder in den Einrichtungen der Gemeinde vorhandene Netzstruktur ist in einer Übersicht zu dokumentieren (Nachweise über sämtliche IP-Ports, Benutzer, Telefon, PC, Drucker, Fax etc.).

- Die Verteiler (wie Router, Hub und Switch) sind in verschlossenen, für den Netzwerkbetrieb zugelassenen Schränken zu betreiben.

10. Zentrale Drucker u. Kopierer

- Werden Drucker für zentrale Druckaufträge genutzt, ist darauf zu achten, dass Ausdrucke mit personenbezogenen Daten nicht unbeaufsichtigt erfolgen, bzw. nach dem Ausdruck umgehend aus dem Gerät genommen werden.

11. Datenverwaltung

- Alle Datenbestände sind nur über die jeweilige Speicherinfrastruktur entsprechend der geltenden Dienstanweisung zu sichern.

- Die Daten sind durch Zugriffsrechte auf dem jeweiligen Server voneinander abzugrenzen.

- Der Zugriff erfolgt grundsätzlich auf Amtsebene (Speicherlaufwerk G: und jeweiliges Ämterverzeichnis, sowie Gruppenregelungen unter Windows Server). Die Ämter haben weitere Abgrenzungen zu regeln und zu dokumentieren.

- 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.

12. Datensicherung

- Um die Verfügbarkeit und die Wiederherstellbarkeit der Daten auf den Servern zu gewährleisten, sind regelmäßige, inkrementelle Backups durchzuführen.

- Im Rahmen einer Wochen- und Monatssicherung hat ein zusätzliches umfangreicheres Backup stattzufinden.

- Die Bänder sind diebstahl- und datensicher in besonderen Stahlschränken aufzubewahren.

- Die Backup Funktion und die Wiederherstellung der Daten ist in regelmäßigen Abständen zu überprüfen und zu protokollieren.

13. Datenträger

- Vorhandene USB Schnittstellen und CD-Laufwerke sind soweit möglich, mittels eines Passwort geschützen BIOS zu deaktivieren. Sollte für die Aufgabenerfüllung ein Zugriff erforderlich sein, sind die PC-Benutzerinnen und PC- Benutzer schriftlich zu verpflichten, den Datenträger lediglich für diesen Zweck zu nutzen. Es ist dann zusätzlich durch mechanische Maßnahmen zu sichern (Fingerabdruck oder Passwort).

- Externe Datenträger (z.B. USB-Anschlussmedien) sind vor ihrem Einsatz durch die EDV Abteilung auf vorhandenen schädigenden Code (z. B. Viren/Trojaner) zu prüfen.

- Sollen dienstliche Daten auf externen Datenträgern gespeichert und weitergegeben werden, so sind die Datenträger zu prüfen, zu verschlüsseln und deren Nutzung zu überwachen. Dies verhindert einen Missbrauch der Daten durch dritte bei z.B. Verlust oder Diebstahl.

- Die Datenträger sind eindeutig zu kennzeichnen.

- Nicht mehr benötigte Datenträger sind nach Rückgabe durch den Nutzer von der EDV-Abteilung unwiederbringlich zu löschen.

- Der Anschluss von privaten Geräten an die dienstliche Infrastruktur ist nicht gestattet.

14. Verfahren

- Die eingesetzten Verfahren sind in eine Bestandsliste aufzunehmen (Verzeichnis von Verarbeitungstätigkeiten, Art. 30 EU-DSGVO).

  Folgende Angaben müssen enthalten sein:

  1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

  2. die Zwecke der Verarbeitung;

  3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

  4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

  5. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Abs. 1 Unterabschnitt 2 DSGVO genannten Datenübermittlung die Dokumentierung geeigneter Garantien;

  6. wenn möglich die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

  7. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1

- Die Rechte für den Zugriff auf die Verfahren sind von der Amtsleitung des jeweiligen Fachamts zu regeln.

Sie sind innerhalb der Verfahren auf das notwendige Maß zu beschränken

15. Benutzer/-innen - und Rechteverwaltung

- Die Rechteverwaltung ist durch die EDV-Abteilung wahrzunehmen.

- Es ist eine bereichsbezogene Liste über PC-Benutzerinnen und PC-Benutzer und den ihnen zugewiesenen Rechten zu erstellen (Zugriffskonzept).

- Benutzerinnen und Benutzer sind ausschließlich auf den Zentralservern (Domänencontroller über Active Directory) einzurichten.

- Zur Vereinfachung der Rechtezuweisung sind Benutzergruppen zu bilden.

- Den Benutzerinnen und Benutzern sind nur mit schriftlicher Zustimmung der jeweiligen Verfahrensverantwortlichen entsprechende Zugriffsrechte zu erteilen. Entsprechende Formulare sind vorhanden, eine E-Mail an die EDV-Abteilung ist als Nachweis ausreichend.

- Die Berechtigungen sind soweit einzuschränken, dass ausschließlich verfahrensbezogene Speicher- oder Programmverzeichnisse genutzt werden können.

IV. Sicherheitskonzept für die Internetnutzung

1. Allgemein

- Der Leistungsumfang des Providers ist in einem ADV-Vertrag festzulegen. Es ist insbesondere darzustellen, auf welche Daten der Provider zugreifen kann.

- Daten über den Ablauf der Internetkommunikation (z.B. Verlauf Proxyserver), die nicht für Abrechnungs- oder angeordnete Überwachungszwecke gespeichert werden, müssen unmittelbar nach Beendigung gelöscht werden.

- Die Nutzung der Internetdienste ist in einer gesonderten Dienstanweisung zu regeln.

- Die Befugnisse bzw. Zugriffsberechtigungen der EDV-Abteilung sind festzulegen.

- Die Administration der Internet-Komponenten ist zu protokollieren.

- Veränderungen der Sicherheitseinstellungen sind nur mit Zustimmung der Leitungsebene, durch die EDV-Abteilung durchzuführen.

- Die Überwachung der Internet-Kommunikation erfolgt durch ITEOS.

- Sofern Dateien (z.B. Formulare u.a.) aus nicht vertrauenswürdigen Quellen oder unbekannten Internetseiten heruntergeladen werden, sind diese vor dem Öffnen einer Virenüberprüfung zu unterziehen. Das Herunterladen ausführbarer Programme und Dateien (Dateiendung: z. B. EXE, COM, BAT und VBS) ist auf den Arbeitsplätzen nur mit Zustimmung der EDV-Abteilung zugelassen, ggf. durch den Rechteentzug zu verhindern.

2. Physikalische Ebene

- Die Übergänge vom internen Netz zum externen Netz sind durch Firewallsysteme (z. B. Router, Gateways etc.) zu schützen.

- Die Verbindung für die Internetdienste darf nur über die Leitung der KabelBW

i.V.m. dem KIVBF / ITEOS Proxy-Server erfolgen. Ausnahme bilden hier Datenterminals wie EC Geräte, diese können auch direkt an den KabelBW Switch angeschlossen werden.

- Die Verfügungsgewalt (Überwachung und Administration) über die eingesetzten Firewall-Komponenten (Router, Gateways etc.) im Bereich der Netzübergänge (intern/extern) liegt beim Kommunalen Rechenzentrum.

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

- Die Eingrenzung bzw. Deaktivierung von Internetseiten ist mittels Sicherheitssoftware zu realisieren (Proxyserver).

3. E-Mail

- E-Mail-Eingänge sind wie allgemeine Posteingänge zu behandeln.

- Der E-Mail-Dienst ist auf einem Exchange Server einzurichten.

- Für alle PC-Benutzerinnen und PC-Benutzer sind eindeutige E-Mail-Adressen vorzuhalten und/oder zusätzliche Funktions-E-Mail-Adressen einzurichten (z.B. Mahnungen, Datenschutz usw.).

- E-Mails und die 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) werden ohne weitere Überprüfung gelöscht.

- Das Empfangen von Dateien mit der Endung .doc und .xls per E-Mail wird aus Sicherheitsgründen (Macros können Schadcode enthalten) bereits am Server blockiert. Der Absender erhält eine entsprechende Automatisch generierte Antwort.

- Die Nutzung des dienstlichen E-Mail Accounts für private Mails ist geduldet, wie in der Dienstanweisung beschrieben.

- Bei E-Mails die an mehrere Personen extern verschickt werden, sind die Empfänger im Feld BCC einzutragen. Das Feld AN oder BC darf für Verteiler an externe Empfänger nicht genutzt werden.

- Beim Einrichten des Abwesenheitsassistenten ist darauf zu achten, dass keine Gründe für die Abwesenheit genannt werden.

- In Einzelfällen muss bei länger andauerndem Ausfall wie z.B. Krankheit, der Zugriff auf den User E-Mail-Account möglich sein. Dies wird im Rahmen einer Einwilligung festgelegt, siehe Dienstanweisung zur E-Mailnutzung i.V.m. § 88 Abs. 3, §§ 91 ff Telekommunikationsgesetz.

- Beim Versenden von E-Mails ist auf die Minimierung der personenbezogenen Daten zu achten, d.h. so wenig personenbezogene Daten wie möglich zu verwenden. Bei der Nutzung der Antwortfunktion auf eine eingehende E-Mail ist die ursprüngliche Nachricht zu entfernen. Bei einer Weiterleitung sind nicht für den Fall relevante Personenbezogene Daten zu entfernen.

4. Homepage

- Die Inhalte der Homepage sind mit dem Bürgermeister abzustimmen.

- Für die Darstellung personenbezogener Daten ist von den Betroffenen eine Einwilligung gemäß Art. 6 ff. DSGVO einzuholen.

- Es muss sichergestellt werden, dass keine Manipulation der Daten durch Unbefugte möglich ist.

- Die Integrität der Homepage ist in regelmäßigen Abständen zu überprüfen.

- Die Homepage darf nur eine verschlüsselte Verbindung zulassen, um sicheren Kontakt z.B. über ein Formular zwischen Server und Benutzer zu gewährleisten. Diese Information ist in der Datenschutzerklärung zu erwähnen.

- Werden auf der Homepage weitere Kommunikations- und Informationsmedien wie ein Newsletter angeboten, ist eine Nutzung dieses Services nur durch aktive Bestätigung der Datenschutzerklärung möglich (z.B. E-Mail Bestätigung)

V. Sicherheitskonzept für die Telekommunikationsdienste

1. Allgemein

- Für die Nutzung der Telekommunikationseinrichtungen der Gemeinde Ilvesheim, ist die entsprechende Dienstvereinbarung maßgebend.

- Die Administration der TK-Anlagen ist in einer Dienstanweisung festzuschreiben.

- Für jede TK-Anlage ist eine Dokumentation in einer Systemakte anzulegen. Aufbau und Inhalt sind in die Dienstanweisung aufzunehmen.

2. Administration

- Die Zuständigkeiten, die Zugriffsberechtigungen und der Umfang der Administration der TK-Anlagen ist zu regeln. Dies betrifft insbesondere externe Dienstleister, die Datensicherung und Verfügbarkeit der Anlagen sicherstellen.

- Der Leistungsumfang der externen Dienstleister ist durch schriftlichen Vertrag zu regeln. Die durchzuführenden Aufgaben sind abschließend zu beschreiben.

- Die externen Dienstleister sind zu verpflichten, Daten, die ihnen durch ihre Tätigkeit für die Gemeinde Ilvesheim bekannt werden, vertraulich zu behandeln.

- Die von den externen Dienstleisterinnen und Dienstleistern durchgeführten Aktivitäten sind von ihnen zu protokollieren.

- Fernadministration hat auf gesicherten Leitungen unter Verwendung von einmaligen Passwörtern zu erfolgen. Die Leitungen sind nach Ende der Tätigkeit wieder zu sperren. Die Administration ist von der EDV-Abteilung zu überwachen.

- Veränderungen an der TK-Anlage sind mit der Fachleitung Hauptamt abzustimmen.

3. Leistungsmerkmale der TK-Anlage

- Die möglichen Leistungsmerkmale der einzelnen TK-Anlagen sind zu dokumentieren. Es sind jeweils nur die Leistungsmerkmale zu aktivieren, die für den dienstlichen Betrieb erforderlich sind. Diese sind in der Systemakte festzuhalten.

- Die Aktivierung oder Deaktivierung von Leistungsmerkmalen bedarf der Zustimmung der Fachleitung Hauptamt.

4. Gebührenabrechnung

- Die Zuständigkeiten und die Durchführung der Gebührenabrechnung sind festzulegen.

- Die Gebührendaten für dienstliche Gespräche sind so lange aufzubewahren, wie sie für dienstliche Erfordernisse benötigt werden.

- Eine Abrechnung für Privatgespräche findet nicht statt.

5. Voice-Mail-Server / Anrufbeantworter / Mailbox

- Die Verwaltung (z. B. Administration, Abhören, Löschen der Nachrichten) der auf dem Voice-Mail-Server liegenden Datenbestände ist zu regeln.

- Die vorhandenen Sicherheitseinstellungen sind zu nutzen (z. B. Passwort zum Abhören eingegangener Nachrichten).

6. Telefaxgeräte

- Jedem Mitarbeiter ist eine Faxnummer zuzuteilen, die ankommende Faxe direkt an das persönliche Email Postfach sendet.

- Alle geräteseitigen Sicherungsmaßnahmen (z. B. Anzeige der störungsfreien Übertragung oder der gesicherten Zwischenspeicherung) sind zu nutzen.

- Grundsätzlich sind Faxgeräte für den Direktsendebetrieb einzustellen. Sendeprotokolle sind dem Vorgang beizufügen.

- Telefaxgeräte sind so aufzustellen, dass Unbefugte keine Kenntnis von Inhalten eingehender und übertragener Telefaxe erhalten können.

7. Mobiltelefone (Handys)

- Die Übergabe eines Handys mit SIM Karte erfolgt erst nachdem die Empfangsperson das Überblickspapier durchgelesen und die Nutzungsvereinbarung unterschrieben hat.

- 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 von Telefon, SIM-Karte oder PIN ist sofort dem Hauptamt zu melden.