



Dienstanweisungen für den Bereich der EDV in der Gemeinde Leopoldshöhe

Dienstanweisung für die Informationstechnologie – IT

Inhaltsverzeichnis

1.	Rechtsgrundlagen	S. 3
2.	Allgemeines	S. 3
2.1.	Geltungsbereich	S. 3
2.2.	Sicherheitsziele	S. 3
2.3.	Allgemeine Zuständigkeiten	S. 3
2.4.	Zentrale Zuständigkeiten	S. 3
3.	Automatisierte Datenverarbeitung	S. 4
3.1.	Begriffsbestimmungen	S. 4
3.2.	Technische und organisatorische Maßnahmen gemäß § 10 DSGVO NRW	S. 4
3.2.1.	Zugangsberechtigung	S. 4
3.2.2.	Zugriffsberechtigung	S. 5
3.2.3.	Benutzerkennwort	S. 5
3.2.4.	Protokollierung	S. 6
3.2.5.	Maßnahmen an den Arbeitsstationen	S. 6
3.2.6.	Private Datenträger	S. 6
3.2.7.	Benutzung von privater Hard- und Software	S. 6
3.2.8.	Datenimport / Datenexport	S. 6
3.2.9.	Einsatz von DV-Verfahren und Programmen	S. 7
3.2.10.	Aufbewahrung von Datenträgern	S. 7
3.2.11.	Transport von Datenträgern	S. 7
3.2.12.	Löschung, Vernichtung und Entsorgung von Datenträgern	S. 7
3.2.13.	Wartung / Fernwartung	S. 7
3.2.14.	Internet, Extranet, Intranet und Nutzung der Kommunikationssoftware (Exchange-Server, E-Mail)	S. 8
4.	Nicht automatisierte Datenverarbeitung	S. 8
4.1.	Allgemeines	S. 8
4.2.	Sicherungsmaßnahmen	S. 8
4.2.1.	Aufbewahrung der Akten in zentralen Registraturen	S. 8
4.2.2.	Aufbewahrung der Akten in den Diensträumen	S. 8
4.3.	Maßnahmen bei der Bearbeitung personenbezogener Daten	S. 9
4.3.1.	Übermittlung / Aktenübersendung	S. 9
4.3.2.	Transport, Sicherheitsmaßnahmen bei zentraler Textverarbeitung	S. 9
4.3.3.	Auskünfte	S. 9
4.3.4.	Vernichtung von Akten und Vorgängen	S. 9
5.	Inkrafttreten	S. 10

1. Rechtsgrundlagen

In Ergänzung des Gesetzes zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) vom 9.5.2000 in der zur Zeit gültigen Fassung (GV NW S.452) wird folgende Dienstanweisung für die „ Informationstechnologie -IT“ –DA –IT- erlassen:

2. Allgemeines

2.1. Geltungsbereich

Diese Dienstanweisung gilt für alle DV-Systeme und –Verfahren der Gemeinde Leopoldshöhe.

2.2. Sicherheitsziele

Der Sicherheitspolitik der Gemeinde Leopoldshöhe liegen folgende Leitsätze und Handlungsempfehlungen zugrunde:

- Schutz der persönlichen Daten der Bürger(innen) und sonstiger vertraulicher Daten
- Informationssicherheit als integraler Bestandteil des Verwaltungshandelns
- Beachtung der datenschutzrechtlichen Vorschriften durch die Mitarbeiter/innen
- Hohe Verlässlichkeit des Verwaltungshandelns in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit durch Informationsverarbeitung (Schutz von Daten und Objekten)
- Verantwortung der Führungskräfte für angemessene(n) Datenschutz und Datensicherheit
- Sicherstellung der Kontinuität der Arbeitsabläufe

2.3. Allgemeine Zuständigkeiten

Die Mitarbeiter/innen der Gemeinde Leopoldshöhe sind im Rahmen der Aufgabenerledigung für die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Aufgabenbereich verantwortlich. Sie sind verpflichtet, bei der Einführung neuer Verfahren oder Änderung bestehender Verfahren sowie bei der Erarbeitung behördeninterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten die/den Datenschutzbeauftragte/n frühzeitig zu beteiligen.

Im übrigen können sie sich jederzeit in Angelegenheiten des Datenschutzes unmittelbar an die/den Datenschutzbeauftragte/n wenden.

Die Vorgesetzten haben im Rahmen ihrer Führungsaufgaben die Einhaltung der datenschutzrechtlichen Vorschriften und Weisungen zu überwachen.

2.4. Zentrale Zuständigkeiten

Zentrale Datenschutzangelegenheiten obliegen

- der/m IT-Sicherheitsbeauftragten der Verwaltung,
- der/m Datenschutzbeauftragten und deren/ dessen Stellvertreter/in sowie
- der Systemadministration.

Die/der IT-Sicherheitsbeauftragte ist verantwortlich für die Durchführung organisatorischer Datenschutzmaßnahmen, wie

- allgemeinverbindliche DA und Rundschreiben,

- die Angaben für das vom der/dem Datenschutzbeauftragten zu führende Verzeichnis, sowie
- die Bearbeitung aller Datenschutzangelegenheiten, die nicht in die Zuständigkeit der/des Datenschutzbeauftragten bzw. Systemadministration fallen, insbesondere die Erstellung und Pflege des Sicherungskonzeptes gemäß § 10 DSGVO NRW.

Ist kein/e IT-Sicherheitsbeauftragte/r bestellt worden, sind die vorstehenden Aufgaben einer geeigneten Fachkraft zu übertragen. Sicherheitsbeauftragte/r oder Fachkraft sind Ansprechpartner/in der/des Datenschutzbeauftragten und unterstützen diese/n bei der Wahrnehmung ihrer/seiner Aufgaben.

Der/die Datenschutzbeauftragte ist in dieser Funktion der Verwaltungsleitung unmittelbar unterstellt. Ihre/seine Aufgabe ist es, ungeachtet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten, die Verwaltung bei der Sicherstellung des Datenschutzes zu unterstützen. Im einzelnen ergeben sich die Aufgaben aus § 32a DSGVO NRW.

Zentrale Aufgabe der Systemadministration ist die Sicherstellung eines ordnungsgemäßen Betriebsablaufs. Die Aufgaben und Abläufe sind schriftlich festzulegen. Soweit erforderlich, sind zusätzliche schriftliche Weisungen der Vorgesetzten zu erteilen. Die in der Systemadministration tätigen Mitarbeiter/innen dürfen, soweit sie nicht ausdrücklich zugriffsberechtigt sind, auf Anwendungen oder Dateien der Benutzerinnen und Benutzer nur in besonders begründeten Fällen zugreifen. Jeder Zugriff ist unter Angabe der Gründe zu dokumentieren. Soweit auf Dateien der Benutzerinnen und Benutzer zugegriffen wurde, sind die betroffenen Beschäftigten davon zu unterrichten.

Die für den Datenschutz und die Datensicherheit erforderlichen Maßnahmen sind, soweit im folgenden keine andere Regelung getroffen ist, von den Stellen, für deren Aufgabenerfüllung die DV-Geräte eingesetzt sind, durchzuführen oder zu veranlassen.

3. Automatisierte Datenverarbeitung

3.1. Begriffsbestimmungen

In die automatisierte Datenverarbeitung (einschließlich Textverarbeitung) sind einbezogen

- installierte mehrplatzfähige Systeme, wie z.B. vernetzte PC
- grafisch interaktive Arbeitsplätze
- PC als Einzelplatzlösung
- Laptops, Notebooks u.ä.
- Zeiterfassungsanlage
- Telefonanlage
- Mobiltelefone
- Telefaxgeräte

3.2. Technische und organisatorische Maßnahmen gemäß § 10 DSGVO NRW

Werden personenbezogene Daten automatisiert verarbeitet, sind die folgenden Maßnahmen zu beachten, die den Schutz dieser Daten gewährleisten. Die Maßnahmen sind zugleich Bestandteil des Sicherungskonzeptes gemäß § 10 DSGVO NRW.

3.2.1. Zugangsberechtigung

Räume mit DV-Ausstattung sind beim - nicht nur kurzfristigen - Verlassen grundsätzlich zu verschließen. Räume mit mehr als einem Arbeitsplatz sind von der letzten Person, die den Raum verläßt, zu verschließen. DV-Endgeräte sind bei Dienstschluß nach vorschriftsmäßiger Programmbeendigung abzuschalten. Bei kurzfristiger Abwesenheit ist der Bildschirmarbeitsplatz softwaremäßig zu sperren.

Benutzerinnen und Benutzer haben dafür Sorge zu tragen, daß bei Darstellung personenbezogener Daten auf Bildschirmen und Druckern Unbefugten die Einsicht verwehrt wird.

Das Betreten von Räumen, in denen sich DV-Geräte befinden, ist nur Mitarbeiter/innen gestattet. Dritte dürfen die Räume unter Beachtung von Absatz 2 nur bei Anwesenheit der Mitarbeiter/innen betreten.

Die für die Systeme notwendigen Komponenten (Server, Hubs, Switch u.ä.) sind im System/Technikraum untergebracht. Zugangsberechtigt ist nur die Systemadministration. Anderen Personen ist der Zugang nur in Anwesenheit der Systemadministration gestattet.

3.2.2. Zugriffsberechtigung

DV-Geräte dürfen nur von den Mitarbeiter/innen genutzt werden, die von der Leitung bzw. den zuständigen Fachbereichen hierzu ermächtigt worden sind.

Wird ein DV-Gerät von mehreren Mitarbeiter/innen genutzt, ist von der Leitung bzw. vom zuständigen Fachbereich ein/e verantwortliche/r Benutzerin/Benutzer zu bestellen.

Die Mitarbeiter/innen dürfen nur Zugriff zu den Daten und Programmen erhalten, die sie im Rahmen der ihnen übertragenen Aufgaben benötigen. Die Festlegung der Zugriffsberechtigung – unterteilt nach Benutzerin/Benutzer oder Benutzergruppen sowie der Art der Zugriffsberechtigung (Lesen, Schreiben, Löschen, Ausführen) – erfolgt durch die Leitung bzw. durch den zuständigen Fachbereich.

Die Einrichtung von berechtigten Benutzerinnen/Benutzern einschließlich der Übernahme der zugewiesenen Zugriffsrechte erfolgt durch die Systemadministration, die eine aktuelle Übersicht über die vergebenen Berechtigungen schriftlich zu führen hat.

3.2.3. Benutzerkennwort

Es sind die Voraussetzungen dafür zu schaffen, daß die von den DV-Systemen gebotenen technischen Möglichkeiten des Kennwortschutzes genutzt werden.

Benutzerkennworte dürfen nicht aus einer zu einfachen Ziffern- und/oder Buchstabenkombination, aus einfach abzuleitenden Begriffen oder leicht zu erratenden Namen (Vornamen, Namen von Angehörigen, Monatsnamen) bestehen. Es sollte möglichst eine Kombination aus Buchstaben und Ziffern ohne erkennbare Gesetzmäßigkeit gewählt werden.

Benutzerkennworte müssen mindestens 6-stellig sein. Bei systembedingten Abweichungen von dieser Forderung ist eine Ausnutzung der maximal möglichen Stellenzahl erforderlich.

Benutzerinnen und Benutzer haben darüber hinaus folgendes zu beachten:

- Benutzerkennworte dürfen nur dann eingegeben werden, wenn die Eingabe nicht von Unbefugten beobachtet werden kann.
- Die Kennworte sind geheim zu halten. Es ist unzulässig, das Benutzerkennwort anderen Personen mitzuteilen oder zur Kenntnis gelangen zu lassen. Die Geheimhaltungspflicht gilt auch gegenüber Vorgesetzten.
- Benutzerkennworte sollten nach Möglichkeit nicht aufgeschrieben werden. Falls dies dennoch geschieht, ist dafür zu sorgen, daß keine andere Person die Möglichkeit erhält, diese Aufzeichnung einzusehen.
- Um die Vertraulichkeit der Benutzerkennworte zu gewährleisten, sind sie spätestens nach Ablauf der von der Systemadministration festzulegenden Gültigkeitsintervalle (systemabhängig) zu ändern. Die Gültigkeitsintervalle sollen drei Monate nicht

überschreiten. Die Änderung des Kennwortes soll möglichst in unregelmäßigen Abständen erfolgen.

Sollte Unsicherheit darüber bestehen, ob ein benutztes Kennwort Dritten zur Kenntnis gelangt ist, muß dieses unverzüglich geändert werden.

Soweit technisch möglich, sind alle Versuche, sich mittels falscher Benutzerkennworte Zugang zum DV-System zu verschaffen, vom System zu protokollieren.

Nach dreimaligem fehlerhaften Zugangsversuch ist die Arbeitsstation zu sperren. Die Sperre kann nur durch die Systemadministration aufgehoben werden.

3.2.4. Protokollierung

Die Protokollierung von Systemereignissen einschließlich der jeweiligen Benutzeridentifizierung dient der Datensicherheit und gehört zu den Maßnahmen der Verarbeitungs-, Benutzungs-, Zugriffs- und Organisationskontrolle.

Zur nachträglichen Kontrolle, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat, ist bei sämtlichen Dateien, in denen personenbezogene Daten verarbeitet werden, der Zugriff auf jeden Datensatz in geeigneter Weise festzuhalten. Die Protokolle sind mindestens bis zur Durchführung einer Kontrolle aufzubewahren.

3.2.5. Maßnahmen an den Arbeitsstationen

Die installierten Laufwerke der vernetzten Arbeitsplatz PC's werden aus Datensicherheitsgründen gesperrt. Eine Aufhebung der Sperre ist nur unter besonderen Umständen und in Abstimmung mit der Systemadministration zulässig.

Bei vernetzten Systemen sind Daten grundsätzlich auf zentralen Laufwerken zu speichern. Datenbestände auf der lokalen Festplatte (Laufwerk C:) werden nicht gesichert.

Änderungen an den installierten DV-Geräten oder der Verkabelung sind nur in Abstimmung mit der Systemadministration zulässig. Dies gilt auch für den Austausch von Hardwareteilen sowie für den Standortwechsel.

3.2.6. Private Datenträger

Der Einsatz privater Datenträger ist grundsätzlich unzulässig. Dieses Verbot gilt auch für die Verarbeitung nicht personenbezogener Daten. In Ausnahmefällen und nur zur unbedingt erforderlichen Aufgabenerfüllung dürfen Fremddatenträger verarbeitet werden. Es ist grundsätzlich eine Viren-Überprüfung mit den entsprechenden Virenschutzprogrammen vorzunehmen.

3.2.7. Benutzung von privater Hard- und Software

Die Benutzung von privater Hardware und Software (Programme bzw. Anwendungen jeglicher Art, Shareware und Publicdomain-Produkte) ist grundsätzlich untersagt. Es darf nur lizenzierte oder zu Testzwecken zur Verfügung gestellte Software benutzt werden.

3.2.8. Datenimport / Datenexport

Ein Datenimport (beispielsweise über Datenträger) in das System darf nur durch zentrale, besonders autorisierte Stellen vorgenommen werden. Hierbei sind die zu übernehmenden Daten auf mögliche Gefährdungen des Systems zu überprüfen, insbesondere durch den Einsatz von aktuellen Virenscannern.

Ein Export personenbezogener Daten darf nur erfolgen, soweit er rechtlich zulässig ist. Die Verantwortung hierfür trägt das jeweilige Amt.

3.2.9. Einsatz von DV-Verfahren und Programmen

Für jede Entwicklung, Änderung und jeden Einsatz von Anwendungsprogrammen im Produktionsbetrieb sind besondere Richtlinien über die Programmentwicklung, die Programmdokumentation, die Programmprüfung und die Programmfreigabe zu erlassen.

Es dürfen nur Programme eingesetzt werden, die nach den vorstehenden Richtlinien freigegeben worden sind.

Für jedes DV-System ist ein Verzeichnis über die auf dem System eingesetzten Programme zu führen. Das Verzeichnis hat mindestens die Bezeichnung der Programme, die Programmversion und das Datum der Erstinstallation zu enthalten.

3.2.10. Aufbewahrung von Datenträgern

Datenträger, die der System- und Datensicherung dienen, sind verschlossen im Datentresor aufzubewahren. Die zuständigen Stellen haben jeweils ein aktuelles Verzeichnis über den zur System- und Datensicherung erforderlichen Datenträgerbestand zu führen.

Kopien wichtiger System- und Anwendungsdateien sind an geeigneter Stelle auszulagern.

3.2.11. Transport von Datenträgern

Datenträger, die personenbezogene Daten enthalten, sind vor Versendung und Transport durch geeignete Verschlüsselungsverfahren vor dem Zugriff Dritter zu schützen. Sollte dies nicht möglich sein, ist der Transport durch gleichwertige Maßnahmen (beispielsweise Transport durch Boten) sicherzustellen.

Der Transport von Datenträgern sowie von Unterlagen mit personenbezogenen Daten außerhalb des Dienstgebäudes durch Kuriere hat in verschlossenen Behältnissen zu erfolgen. Die Behältnisse dürfen nur empfangsberechtigten Personen gegen eine Empfangsbescheinigung ausgehändigt werden.

3.2.12. Löschung, Vernichtung und Entsorgung von Datenträgern

Auf maschinell einsetzbaren Datenträgern (beispielsweise Disketten, Festplatten), die an Herstellerfirmen zurückgehen, verkauft werden sollen oder nicht mehr verwendbar sind, sind noch vorhandene personenbezogene oder vertrauliche Daten physikalisch zu löschen. Falls dies nicht mehr möglich sein sollte, sind die Datenträger in geeigneter Weise unbrauchbar zu machen.

Ist die Löschung der Daten technisch nur durch die Herstellerfirma möglich, ist eine Weitergabe der Datenträger an diese zulässig, wenn der sichere Transport gewährleistet, eine mißbräuchliche Nutzung der Daten ausgeschlossen und ihre unverzügliche vollständige Löschung garantiert wird. Dies ist durch eine schriftliche Vereinbarung mit der Herstellerfirma zu gewährleisten.

Aussondernde Datenträger sind an die ausgebende Stelle zurückzugeben. Diese sorgt für eine sachgerechte Vernichtung.

3.2.13. Wartung / Fernwartung

Wartung sind alle Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der DV-Systeme.

Bei Wartungsarbeiten darf grundsätzlich nicht auf personenbezogene Daten zugegriffen werden. Sofern dies nicht gewährleistet ist, ist sicherzustellen, daß nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.

Eine Wartung durch externe Stellen darf nur aufgrund schriftlicher Vereinbarungen (Wartungsvertrag) erfolgen. Darin sind die im Rahmen der Wartung notwendigen

technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit festzulegen. Die mit den Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

Bei Wartung durch Externe ist sicherzustellen, daß nur dafür autorisiertes Personal die Wartung vornimmt, alle Wartungsvorgänge während der Durchführung kontrolliert und nach der Durchführung nachvollzogen werden können.

Eine Fernwartung ist in jedem Einzelfall frei zu schalten. Während der Fernwartung hat die zuständige Stelle besonders darauf zu achten, daß nur erlaubte Funktionen ausgeführt werden. Erforderlichenfalls ist die Fernwartung abzubrechen. Soweit möglich, sind technische Ablaufprotokolle zu erstellen und für Kontrollzwecke zu sichern.

Wartungstechniker und sonstige Dritte dürfen grundsätzlich nicht mit den von ihnen eingebrachten Datenträgern arbeiten. Statt dessen stellt die zuständige Stelle erforderlichenfalls Datenträger zur Verfügung, auf die der Inhalt des eingebrachten Datenträgers übertragen werden kann. Kann nur mit den eingebrachten Datenträgern gearbeitet werden, ist vor deren Einsatz eine Virenprüfung vorzunehmen.

Änderungen der Betriebssysteme bzw. systemnaher Software während der Wartung sind erst nach Freigabe zu übernehmen. Die Änderungen sind schriftlich zu dokumentieren.

3.2.14. Internet, Extranet, Intranet und Nutzung der Kommunikationssoftware (Exchange-Server, E-Mail)

Die Nutzung der genannten Medien bzw. der Kommunikation per PC-Fax und E-Mail wird in einer gesonderten Dienstanweisung geregelt.

4. Nicht automatisierte Datenverarbeitung

4.1. Allgemeines

Die nachfolgenden Regelungen gelten für jedwede Art der nicht automatisierten Verarbeitung von personenbezogenen Daten in oder aus Akten bzw. Karteien.

4.2. Sicherungsmaßnahmen

4.2.1. Aufbewahrung der Akten in zentralen Registraturen

Soweit Ämter zur Aktenverwaltung eine zentrale Registratur führen, sind Akten, die nicht unmittelbar für die Aufgabenerfüllung benötigt werden, in den Räumen der Registratur, möglichst getrennt nach den Fachbereichen unter Verschluss aufzubewahren.

Die Registraturräume bzw. die Registraturschränke der Zentralregistratur sind bei –auch kurzfristiger- Abwesenheit durch die für die Registratur verantwortlichen Mitarbeiter/innen möglichst ständig verschlossen zu halten.

Akten stehen Mitarbeiter/innen nur für ihren jeweiligen Aufgabenbereich zur Verfügung.

4.2.2. Aufbewahrung der Akten in Diensträumen

Die Mitarbeiter/innen sind in ihrem Aufgabenbereich für die Ordnung, Führung und sichere Aufbewahrung der Akten und Unterlagen mit personenbezogenen Daten verantwortlich.

Akten, Karteien und Unterlagen mit personenbezogenen Daten sind in den Diensträumen in verschlossenen Schränken aufzubewahren.

Bei kurzfristiger Abwesenheit der Mitarbeiter/innen während der Dienstzeit reicht es aus, die Türen der Diensträume, soweit möglich, zu verschließen.

Am Arbeitsplatz dürfen sich nur solche Akten und Unterlagen befinden, die unmittelbar bearbeitet werden.

Ausgehändigte Schlüssel sind an sicheren, für Unbefugte nicht erreichbaren Orten, aufzubewahren.

4.3. Maßnahmen bei der Bearbeitung personenbezogener Daten

4.3.1. Übermittlung / Aktenübersendung

Die Übermittlung personenbezogener Daten (Akten) ist nur unter den Voraussetzungen der §§ 14 bis 17 DSGVO zulässig.

Innerhalb der Verwaltung dürfen Akten unter Beachtung der vgl. Bestimmungen grundsätzlich nur zu dienstlichen Zwecken übersandt werden.

Werden Akten an Dritte weitergegeben, ist durch das Amt ein Nachweis zu führen, aus dem ersichtlich sind:

- Empfänger der Akte
- Abgabezweck
- Abgabedatum / Rückgabedatum
- Handzeichen des Aktenverwalters

4.3.2. Transport, Sicherheitsmaßnahmen bei zentraler Textverarbeitung

Beim Versand von Akten und Schriftstücken durch Boten oder Transportunternehmen (z. B. Post AG) außerhalb der Verwaltung ist den besonderen Anforderungen des Datenschutzes Rechnung zu tragen. Zum Transport verwendete Umschläge oder Verpackungsmaterialien müssen so beschaffen sein, daß Dritte keine Kenntnis oder Hinweise auf die Angelegenheit erlangen können.

Akten und Unterlagen mit personenbezogenen Daten, die dem Schreibdienst zur Textverarbeitung übergeben werden, sind bei Abwesenheit der Mitarbeiter/innen unter Verschluss zu halten.

Am Arbeitsplatz der Schreibkräfte dürfen sich nur solche Akten und Unterlagen befinden, die unmittelbar bearbeitet werden.

Außerhalb der Dienstzeit sind alle Akten und Unterlagen, die sich im Schreibdienst befinden, sicher verschlossen aufzubewahren.

4.3.3. Auskünfte

Telefonische Auskünfte über personenbezogene Daten dürfen nur unter den Voraussetzungen der §§ 14 bis 17 DSGVO erteilt werden.

Sie sind nur dann zulässig, wenn die Identität und Berechtigung des Anfragenden eindeutig feststeht.

Bestehen Zweifel an der Identität oder Berechtigung des Anfragenden, ist auf eine schriftliche Anfrage zu verweisen.

4.3.4. Vernichtung von Akten und Vorgängen

Akten und Vorgänge, die zur Aufgabenerfüllung nicht mehr benötigt werden, sind unter Beachtung der geltenden Aufbewahrungsfristen zu vernichten.

Die erforderliche Vernichtung von Akten und Unterlagen mit personenbezogenen Daten ist dem Haupt- und Personalamt anzuzeigen.

5. Inkrafttreten

Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft. Gleichzeitig tritt die Dienstanweisung für die Technikunterstützte Informationsverarbeitung – DA-TUIV – außer Kraft.

Leopoldshöhe, den 22. Januar 2002

Schemmel
(Bürgermeister)

Dienstanweisung Internet und PC-Kommunikation

Inhaltsverzeichnis

1.	Rechtsgrundlagen	S. 12
2.	Allgemeines	S. 12
2.1.	Gegenstand dieser Dienstanweisung	S. 12
2.2.	Ziele	S. 12
2.3.	Geltungsbereich	S. 12
2.4.	Allgemeine Betriebssicherheit	S. 12
2.5.	Personenbezogene Daten der Beschäftigten	S. 12
2.6.	Nutzung des Internet	S. 13
2.7.	Protokollierung und Kontrolle der Nutzung	S. 13
2.8.	Kommunikation per PC-Software	S. 13
2.9.	Verstöße gegen diese Dienstanweisung	S. 13
2.10.	Schlußbestimmung	S. 14
Anlage 1	S. 15
Anlage 2	S. 15

1. Rechtsgrundlagen

In Ergänzung des Gesetzes zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) vom 9.5.2000 in der zur Zeit gültigen Fassung (GV NW S.452) und der Dienstanweisung für die Informationstechnologie – IT wird folgende Dienstanweisung für die Gemeinde Leopoldshöhe erlassen:

2. Allgemeines

2.1. Gegenstand dieser Dienstanweisung

Gegenstand dieser Dienstanweisung ist die ausschließlich dienstliche Nutzung der Online-Dienste (Internet, Surfzugänge, Extranet bzw. Intranet) und die Kommunikation per PC-Software (Exchange u. FerrariFax) durch die Beschäftigten der Gemeinde Leopoldshöhe.

2.2. Ziele

Ziel dieser Dienstanweisung ist es, mit der Ausstattung der Arbeitsplätze durch die vg. Medien

- die Arbeitsbedingungen der Beschäftigten, insbesondere vor dem Hintergrund der technischen Entwicklung im Bereich des elektronischen Informationsaustausches, zu verbessern,

gleichzeitig aber

- den Beschäftigten Sicherheitsrisiken bei der Nutzung vor Augen zu führen und die Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen Daten zu gewährleisten.

Die einzelnen Internet-Dienste werden in Anlage 1 zu dieser Dienstanweisung näher ausgeführt.

2.3. Geltungsbereich

Diese Dienstanweisung gilt primär für die Nutzung der zu Ziffer 2.1. genannten Dienste und Kommunikationssoftware und ergänzt die bestehenden Regelungen der Dienstanweisung für die Informationstechnologie - IT.

2.4. Allgemeine Betriebssicherheit

Die zuständigen Stellen der Verwaltung sichern im Rahmen ihrer Aufgaben den allgemeinen Betrieb zur Nutzung der Internet-Dienste. Sicherheitsrelevante Ereignisse im Zusammenhang mit der Nutzung von Internet-Diensten sind den zuständigen Stellen der Verwaltung unverzüglich mitzuteilen.

Die Übertragung von schutzwürdigen bzw. personenbezogenen Daten über das Internet ist nicht zulässig, es sei denn, sie können zur Wahrung der Vertraulichkeit und Integrität verschlüsselt werden.

Die Internet-Nutzer der Verwaltung sind in ihrem Zuständigkeitsbereich verantwortlich für die Einhaltung der datenschutzrechtlichen Bestimmungen.

2.5. Personenbezogene Daten der Beschäftigten

Im Rahmen des Informations- und Kommunikationsangebotes der Verwaltung im Internet sollen autorisierte Beschäftigte von Dritten global erreichbar sein.

Die zu diesem Zweck maximal erforderlichen Beschäftigtendaten sind als Anlage 2 aufgeführt. Ansonsten sind keine personenbezogenen Daten im Internet zu veröffentlichen bzw. preiszugeben.

2.6. Nutzung des Internet

Eine Datenübermittlung, aus der die Struktur des lokalen Netzwerkes, (z.B. Verzeichnispfade), seine Authentifizierungshilfsmittel (Paßworte o.ä.) oder seine zugelassenen Benutzer (andere Benutzerkennungen) hervorgehen, ist unzulässig.

Die Nutzung von Internet-Diensten unter einer Benutzerkennung, die im lokalen Netzwerk über administrative Rechte verfügt, ist unzulässig.

Beim Ausführen bereits installierter Software ist darauf zu achten, daß Zugriffe aus dem Internet auf die Hardware des PC nicht möglich ist.

Software und sonstige Daten, die aus dem Internet in das lokale Netz eingebracht werden, sind auf ein notwendiges Minimum zu reduzieren und zuvor mittels der zur Verfügung gestellten Virenschutz-Software auf eventuelle Sicherheitsbedenken (Virenübertragung) zu untersuchen.

2.7. Protokollierung und Kontrolle der Nutzung

Jeder Datenverkehr zwischen dem lokalen Netz und dem Internet wird einer automatischen Protokollierung unterzogen. Dabei werden folgende Daten erfaßt.

- die Benutzerkennung (USERID) des/der Beschäftigten
- Datum und Uhrzeit jeder Datenübermittlung zwischen dem lokalen Netz und dem Internet
- Art und Umfang der übermittelten Daten sowie
- die jeweilige Internet-Adresse

Mit vorheriger Zustimmung des Personalrates wird die Protokollierung als Hilfsmittel zur stichprobenartigen Verhaltenskontrolle eingesetzt.

2.8. Kommunikation per PC-Software

Die dienstliche Kommunikation mit der in der Verwaltung eingesetzten Software (E-Mail, Faxe versenden und empfangen) ist grundsätzlich zulässig und in der Verwaltung bzw. im Verbandsgebiet des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe(KRZ) vorrangig zu nutzen.

Um ein einheitliches Erscheinungsbild von elektronischen Nachrichten zu gewährleisten, ist folgende Autosignatur am Ende der Nachrichten zu benutzen:

*Mit freundlichen Grüßen
Vorname Nachname*

*Gemeinde Leopoldshöhe
Tel.:
Fax:
E-Mail: x.nachname@leopoldshoehe.de
<http://www.leopoldshoehe.de>*

Eingehende E-Mail sind wie Posteingänge zu behandeln. Ggf. sind Vorgesetzte und andere Mitarbeiter/innen zu unterrichten bzw. zu beteiligen. Es dürfen keine Bestellungen per E-Mail getätigt werden. Die Versendung und der Empfang von privaten E-Mail mit Anlagen (Attachement) ist untersagt.

2.9. Verstöße gegen diese Dienstanweisung

Verstöße gegen diese Dienstanweisung haben dienst- bzw. arbeitsrechtliche Konsequenzen.

2.10. Schlußbestimmung

Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft.

Leopoldshöhe, den 22. Januar 2002

Schemmel
(Bürgermeister)

Anlage 1 -Internet-Dienste- der Gemeinde Leopoldshöhe

Folgende Internet-Dienste stehen zur Verfügung:

WWW / HTTP

World Wide WEB / Hypertext Transfer Protocol

Ein Standard zur Übermittlung von Multimedia-Dokumenten (Surfzugänge)

FTP

File Transfer Protocol

Standard zur Übertragung von Dateien von einem Computer auf einen anderen

E-Mail / SMTP

Simple Mail Transfer Protocol

Standard für den Versand und Empfang von E-Mails über das Internet

Anlage 2 -Zulässige Beschäftigtendaten im Internet-

Als max. personenbezogene Daten für autorisierte Beschäftigte der Gemeinde Leopoldshöhe gelten:

- . Name
- . Vorname
- . Dienstliche Anschrift
- . Telefon
- . Fax-Nummer
- . E-Mail-Adresse