Dienstanweisung
über den
Datenschutz und die Datensicherheit
bei der
Stadtverwaltung Fritzlar
(DA-Datenschutz)

Inhaltsverzeichnis

1. Allgemeine Regelungen und Hinweise

1.1 Grundlagen

Der Datenschutz beruht auf dem im Grundgesetz verankerten Persönlichkeitsrecht und dient dem Schutz personenbezogener Daten. Bei personenbezogenen Daten handelt es sich um Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Personenbezogene Daten sind außer dem Namen z. B. die Anschrift, das Geburtsdatum, der Familienstand, das Einkommen, die Bankverbindung, Angaben über den Gesundheitszustand.

Dem Datenschutz unterliegen personenbezogene Daten,

- die sich auf namentlich unmittelbar bekannte (bestimmte) Menschen beziehen oder
- die aufgrund von Identifikationsmerkmalen einer bestimmten Person zugeordnet werden können.

Anonymisierte und aggregierte Daten, die keinen Rückschluss auf bestimmte natürliche Personen zulassen, unterliegen nicht dem Datenschutz.

Werden personenbezogene Daten im Rahmen eines automatisierten Verfahrens verarbeitet, ist von der zuständigen Organisationseinheit zu prüfen, ob die folgenden datenschutzrechtlichen Voraussetzungen bestehen:

a) <u>Zulässigkeit der Verarbeitung</u>

Behörden dürfen personenbezogene Daten nur verwenden, wenn eine gesetzliche Ermächtigung besteht oder der/die Betroffene eingewilligt hat.

Der Datenschutz wird vorrangig durch Spezialgesetze (z. B. Abgabenordnung, Meldegesetz, Gewerbeordnung, Personalvertretungsgesetz) und nachrangig durch Datenschutzgesetze (Bundesdatenschutzgesetz und Hessisches Datenschutzgesetz HDSG) geregelt. Während das Bundesdatenschutzgesetz für Bundesbehörden und u. a. für kommunale Eigenbetriebe gilt, gilt das Hessische Datenschutzgesetz auch für die Gemeinden.

Grundsätzlich gehen auch hier die Regelungen der Spezialgesetze den Regelungen der Datenschutzgesetze vor.

Die Zulässigkeit der Datenverarbeitung (Gesetz oder Zustimmung) muss für jede Art der Verwendung personenbezogener Daten bestehen, also für deren Erhebung, Speicherung, Übermittlung, Sperrung und Löschung. (s. z. B. § 14 HDSG)
Besonders wird darauf hingewiesen, dass auch der Informationsaustausch innerhalb der Verwaltung aufgrund gesetzlicher Bestimmungen (z. B. § 11 HDSG) zulässig sein muss.

Die Vorschriften über die Zulässigkeit gelten grundsätzlich auch für die nichtautomatisierte Verarbeitung personenbezogener Daten.

b) <u>Erforderlichkeit der Verarbeitung</u>

Die Erforderlichkeit ist für jede Form der Datenverarbeitung zu prüfen. Erforderlich ist die Verarbeitung personenbezogener Daten nur dann, wenn

ohne sie eine Aufgabe der Daten verarbeitenden Stelle nicht oder nicht ordnungsgemäß erfüllt werden kann.

Nach dem Grundsatz der Erforderlichkeit sind solche Verfahren auszuwählen oder zu entwickeln, die geeignet sind, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Ziels erforderlich sind (Datensparsamkeit).

c) Zweckbindungsgebot

Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder gespeichert worden sind.
Ausnahmen vom Zweckbindungsgebot ergeben sich aus § 13 HDSG.

d) Vorabkontrolle

Vor dem Einsatz oder der wesentlichen Änderung von automatisierten Datenverarbeitungsverfahren hat die zuständige Organisationseinheit zu untersuchen, ob damit kurz-, mittel- oder langfristig Gefahren für die Persönlichkeitsrechte und den Datenschutz der vom Verfahren betroffenen Personen verbunden sind. Dies gilt besonders, wenn sensitive Daten verarbeitet werden.
Automatisierte Verfahren sind vor dem Echteinsatz auf ihre Vereinbarkeit mit den datenschutzrechtlichen Anforderungen zu überprüfen. Dabei sind die Wirkungsweisen der eingesetzten Technik und deren erkennbare Folgewirkungen auf die datenschutzbezogenen Rechte und Freiräume zu bewerten. Als Ergebnis der Vorabkontrolle ist für jedes Verfahren festzustellen, welche Risiken bestehen und wie ihnen entgegen gewirkt werden kann.

e) Beachtung der gesetzlichen Rechte der Betroffenen

Bei der Entwicklung oder der Auswahl von automatisierten Verfahren und deren Anwendung ist darauf zu achten, dass die gesetzlichen Rechte der Betroffenen gewahrt bzw. unterstützt werden.

§ 8 Absatz 1 HDSG kennt folgende (originäre) Rechte der Betroffenen

- Auskunft über automatisiert gespeicherte Daten sowie Akteneinsicht
- Benachrichtigung der Betroffenen über die erstmalige automatisierte Speicherung von personenbezogenen Daten
- Geltendmachung des persönlichen Widerspruchsrechts
- Einsichtnahme in das Verfahrensverzeichnis
- Anspruch auf Berichtigung, Sperrung oder Löschung von personenbezogenen Daten
- Geltendmachung von Schadenersatzansprüchen
- Anrufung des Hessischen Datenschutzbeauftragten

1.2 Zweck der Dienstanweisung

Zweck dieser Dienstanweisung ist es, die rechtmäßige Verarbeitung personenbezogener Daten einschließlich der Datensicherheit durch die zuständigen Stellen der Verwaltung im Sinne des informationellen Selbstbestimmungsrechts (das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen) zu gewährleisten bzw. ausschließlich hierin einzugreifen, sofern

eine Rechtsnorm dies erlaubt. Insofern tragen die städtischen Mitarbeiter/innen die datenschutzrechtliche Verantwortung bei Ausübung ihrer Tätigkeit.

Für alle Mitarbeiter/innen ergibt sich die Notwendigkeit, sich mit den jeweils geltenden datenschutzrechtlichen Bestimmungen ihres Aufgabenbereiches, auch über die Regelungen des HDSG hinaus, vertraut zu machen.

§ 9 Datengeheimnis

Den Mitarbeiter/innen, die Zugang zu personenbezogenen Daten haben, ist eine Verarbeitung dieser Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck während und nach Beendigung ihrer Tätigkeit untersagt. Diese Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

1.3 Geltungsbereich

Diese Dienstanweisung gilt für die Informations-/Daten-Eigenverarbeitung der Stadt Fritzlar als öffentliche Stelle in ihrer Gesamtheit, sofern sie mit personenbezogenen, sensiblen bzw. der natur der Sache nach schutzwürdigen Informationen/Daten umgeht.

Diese Dienstanweisung gilt auch für alle Arten einer von der Stadt Fritzlar ausgehenden Daten-Fremdverarbeitung sowie für jegliche externe Wartung und Systembetreuung; ihre Geltung ist entsprechend vertraglich zu übertragen

- soweit Phasen der o. g. Datenverarbeitung für städtische Organisationseinheiten durch verwaltungsinterne Dienstleister oder externe (Gebiets- und andere Rechenzentren oder gewerblich-private externe Outsourcingnehmer) Dienstleistungsunternehmen als Datenverarbeitung im Auftrage nach § 4 HDSG zu erfüllen sind,
- bei Wartung und Systembetreuung nach § 4 Absatz 4 HDSG,
- bei Funktionsübertragung, d. h. bei der inhaltlich-sachlichen Übertragung städtischer Aufgaben und Funktionen in die Erfüllungsverantwortung Dritter öffentlicher oder nicht öffentlicher Stellen, soweit hierzu u. a. in dieser Dienstanweisung angesprochene Informationen und Daten benötigt, d. h. für die Stadt Fritzlar beschafft oder aus Beständen der Stadt Fritzlar übermittelt werden,
- in Fällen, in denen gewerblich-technische Hilfsaufgaben (z. B. gewerbliches Schreddern von Datenträgern) mit o. g. Informationen / Daten zu besorgen sind, deren Inhalte dabei dem Auftragnehmer unvermeidbar zur Kenntnis gelangen können und daher unter Verwertungsverbot stehen bzw. zu stellen sind,

unabhängig davon, ob Dienstleistungen mittels übernommener Ressourcen der Stadt Fritzlar oder mittels der Ressourcen eines Dritten in städtischer oder der Betriebsstätte eines Dritten stattfinden.

1.4 Begriffsbestimmungen

1. **Personenbezogene Daten** sind Einzelangaben über persönliche und sachliche Verhältnis einer bestimmten oder bestimmbaren natürlichen Person (Betroffene/r).
2. **Sensible/sensitive Daten** sind Daten über die rassische und ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugung, eine Gewerkschaftszugehörigkeit sowie über die Gesundheit und das Sexualleben.
3. **Datenverarbeitung** ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten.

   Im Sinne der nachfolgenden Vorschriften ist

   3.1 **Erheben** das Beschaffen von Daten über den Betroffenen,

   3.2 **Speichern** das Erfassen, Aufnehmen oder Aufbewahrung von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,

   3.3 **Übermitteln** das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten der verarbeitenden Stelle an den Dritten weitergegeben werden oder dass der Dritte bereitgehaltene Daten abruft,

   3.4 **Sperren** das Verhindern weiterer Verarbeitung gespeicherter Daten,

   3.5 **Löschen** das Unkenntlichmachen gespeicherter Daten ungeachtet der dabei angewendeten Verfahren.

4. **Datenverarbeitende Stelle** ist jeder Fachbereich, der Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.
5. **Empfänger** ist jede Person oder Stelle, die Daten erhält.
6. **Dritter** ist jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie Daten im Auftrag verarbeiten.
7. **Automatisiert** ist eine Datenverarbeitung, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig abläuft.
8. Eine **Akte** ist jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist.

Soweit andere landesrechtliche Vorschriften den Dateibegriff verwenden, ist Datei

1. eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder
2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht-automatisierte Datei).

1.5 Zuständigkeiten und Verantwortungsbereiche hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften

1.5.1. Verantwortung

Die Fachbereiche sind im Rahmen der ihnen übertragenen Aufgaben gegenüber der Dienststellenleitung für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Sie sind im Sinne dieser Dienstanweisung Daten verarbeitende Stellen.

Der Fachbereich Zentralangelegenheiten richtet ein Sachgebiet „Datenverarbeitung“ ein. Hier werden alle Entscheidungen zu Einführung und Betrieb der Datenverarbeitung (Hard- und Software) koordiniert. Das Sachgebiet ist auch insbesondere zuständig für die Administration der gesamten DV-Anlage und die Sicherheit der Daten.

Die Fachbereiche haben innerhalb ihrer Zuständigkeiten durch organisatorische und technische Maßnahmen sicherzustellen, dass personenbezogene Daten für unbefugte Dritte nicht zugänglich sind. Die Fachbereichsleiter entscheiden im Benehmen mit dem Sachgebiet „Datenverarbeitung“ über die Einführung, Anwendung, Änderung oder Erweiterung der in ihrem Fachbereich eingesetzten automatisierten Datenverarbeitung. Diese Zuständigkeiten obliegen dem Fachbereich Zentralangelegenheiten in allen fachbereichsübergreifenden Angelegenheiten (insbesondere Schließdienst, Alarmanlage, Einbruchschutz etc.)

1.5.2. Behördlicher Datenschutzbeauftragter

1.5.2.1 Bestellung

Der Magistrat bestellt schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter. Bestellt werden dürfen nur Beschäftigte, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt werden.

1.5.2.2 Aufgaben

Der behördliche Datenschutzbeauftragte nimmt die Aufgaben nach § 5 Absatz 2 HDSG wahr. Er hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere,

- auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Maßnahmen, die das in § 1 Satz 1 Nr. 1 HDSG geschützte Recht betreffen, hinzuwirken,
- die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
- die Daten verarbeitende Stelle bei der Umsetzung der nach den §§ 6, 10 und 29 HDSH erforderlichen Maßnahmen zu unterstützen,
- das nach § 6 Absatz 1 HDSG zu erstellende Verzeichnis zu führen und für die Einsicht nach § 6 Absatz 2 HDSG bereitzuhalten,

- das Ergebnis der Untersuchung nach § 7 Absatz 6 HDSG zu prüfen und im Zweifelsfall den Hessischen Datenschutzbeauftragten zu hören.

1.5.2.3 Befugnisse

Der behördliche Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben frei von Weisungen und dem Bürgermeister unmittelbar unterstellt.

Zur Wahrnehmung seiner Aufgaben ist ihm Zugang zu allen Räumen, Dateien und Akten zu gewähren. Die erforderlichen Auskünfte sind ihm zu erteilen.

Stellt der behördliche Datenschutzbeauftragte Verstöße gegen Vorgaben zu Datenschutz und Datensicherheit fest, kann er diese beanstanden und die betroffene Organisationseinheit zu einer Stellungnahme auffordern; mit der Beanstandung können Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbunden werden.

Im Rahmen der Aufgabenerfüllung ist er im Übrigen gegenüber allen Fachbereichen weisungsbefugt.

Jede Mitarbeiterin und jeder Mitarbeiter hat das Recht, sich direkt an den behördlichen Datenschutzbeauftragten zu wenden.

2. Generelle Regelung für den Umgang mit Datenträgern und Schriftgut

2.1 Aufbewahrung von Datenträgern und Schriftgut

Datenträger und Schriftgut mit personenbezogenen oder sonstigen vertraulichen Daten sind so aufzubewahren, dass Unbefugte keinen Zugriff erhalten. Sie sind nach Dienstschluss verschlossen aufzubewahren. Wenn der zur Aufbewahrung der Datenträger oder des Schriftgutes verwendete Raum verlassen wird, ist er abzuschließen.

Falls im Rahmen der Aufgabenwahrnehmung personenbezogene Daten in Akten außerhalb der Organisation bearbeitet werden müssen (z. B. im Außendienst oder bei Hausbesuchen), sind diese gegen unbefugte Zugriffe zu schützen. Das heißt, die Akte darf nicht unbeaufsichtigt aus der Hand gegeben werden. Sie ist z. B. im Pkw nicht sichtbar unter Verschluss zu halten. Sie ist nach Dienstschluss grundsätzlich wieder in die Dienststelle zurückzubringen. Wenn dies nicht möglich ist, ist sie zu Hause unter Verschluss zu nehmen.

2.2 Versenden von Akten mit besonders geschützten personenbezogenen Daten.

Akten mit personenbezogenen Daten, die einem besonderen Amtsgeheimnis unterliegen (z. B. Personaldaten oder andere sensible Daten), dürfen im internen Postgang oder an andere öffentliche Stellen (z. B. Gerichte) nur im verschlossenen Umschlag o. ä. versandt werden. Nach Möglichkeit sind die verschlossenen Versandbehältnisse von einem Boten zu überbringen.

2.3 Vernichten von Datenträgern und Schriftgut

2.3.1 Vernichtung von Datenträgern

Alle Datenträger sind so zu vernichten, dass Unbefugte keine Zugriff auf die gespeicherten Daten erhalten und diese Daten auch nicht durch spezielle Verfahren rekonstruiert werden können.

- Magnetische Datenträger mit Ausnahme von Festplatten (d. h. z. B. Disketten, Bänder) sind physikalisch zu löschen
- Optische Datenträger sind mechanisch so zu vernichten, (z. B. durch einen geeigneten Aktenvernichter), dass eine Rekonstruktion der darauf enthaltenen Daten nicht mehr möglich ist.
- Festplatten sind durch das Sachgebiet Datenverarbeitung durch wiederholtes Überschreiben der darauf enthaltenen Daten sicher zu löschen oder mechanisch zu vernichten.

2.3.2 Vernichtung von Schriftgut

Nicht archivwürdiges und sonstiges Schriftgut ist nach der gesetzlich vorgeschriebenen Aufbewahrungsfrist zu vernichten. Der zur Vernichtung von Schriftgut mit personenbezogenen Daten verwendete Aktenvernichter muss mindestens der Sicherheitsstufe 3 nach DIN 32 757 entsprechen.

3. Einsatz von Telefaxgeräten

3.1 Zweck

Telefaxgeräte sind Daten verarbeitende Geräte, mit denen auch personenbezogene Daten automatisiert übertragen werden können. Sie werden eingesetzt, um bei einfacher Handhabung schnell Informationen zu übermitteln. Nicht alle Nutzer von Telefaxgeräten sind sich darüber im Klaren, welche Risiken für die Vertraulichkeit der per Telefax übermittelten Informationen bestehen.

Die besonderen Gefahren sind:

- Die Informationen werden grundsätzlich „offen“ (unverschlüsselt) übertragen, und der Empfänger erhält sie – vergleichbar mit einer Postkarte – in unverschlossener Form.
- Der Telefaxverkehr ist wie ein Telefongespräch abhörbar.
- Die Adressierung erfolgt durch eine Zahlenfolge (Telefaxnummer) und nicht durch eine mehrgliedrige Anschrift. Dadurch sind Adressierungsfehler wahrscheinlicher, und Übertragungen an den falschen Adressaten werden nicht oder erst nachträglich bemerkt.
- Bei Telefaxgeräten neueren Typs kann der Hersteller Fernwartungen durchführen, ohne dass der Besitzer diesen Zugriff wahrnimmt. Unter bestimmten Umständen kann er dabei auf die im Telefaxgerät gespeicherten Daten zugreifen (z. B. Lesen der Seitenspeicher sowie Lesen und Beschreiben der Rufnummern- und Parameterspeicher).

Diese Gefahren werden von Anbietern der Telekommunikationsnetze und –dienste nicht abgefangen. Deshalb ist insbesondere die absendende Stelle für die ordnungsgemäße Übertragung und die richtige Einstellung der technischen Parameter am Telefaxgerät verantwortlich.

Dieser Abschnitt der Dienstanweisung regelt den datenschutzrechtlichen Umgang mit Telefaxgeräten.

3.2 Konventionelle Telefaxgeräte

1. Aufgrund der gegebenen Gefährdungen darf die Übertragung sensibler personenbezogener Daten per Telefax nicht zum Regelfall werden, sondern darf nur im Ausnahmefall unter Einhaltung zusätzlicher Sicherheitsvorkehrungen erfolgen.
2. Was am Telefon aus Gründen der Geheimhaltung nicht gesagt wird, darf auch nicht ohne besondere Sicherheitsvorkehrungen (z. B. Verschlüsselungsgeräte) gefaxt werden. Das gilt insbesondere für sensible, personenbezogene Daten, beispielsweise solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial-, Steuer- und Personaldaten).
3. Bei der Übertragung sensibler personenbezogener Daten ist zusätzlich zu hier genannten Maßnahmen mit dem Empfänger ein Sendezeitpunkt abzustimmen, damit Unbefugte keinen Einblick nehmen können. So kann auch eine Fehlleitung durch z. B. veraltete Anschlussnummern oder beim Empfänger aktivierte Anrufumleitungen bzw. –weiterleitungen vermieden werden.
4. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.
5. Das Telefaxgerät ist so aufzustellen, dass Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.
6. Alle vom Gerät angebotenen Sicherheitsmaßnahmen (z. B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Passwort, Fernwartungsmöglichkeit sperren) sind zu nutzen.
7. Die vom Gerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.
8. Bei Telefaxgeräten, die an Nebenstellenanlagen angeschlossen sind, ist das Risiko einer Fehladressierung besonders groß, da vor der Nummer des Teilnehmers zusätzlich Zeichen zur Steuerung der Anlage eingegeben werden müssen. Beim Umgang mit derartigen Geräten ist deshalb besondere Sorgfalt geboten.
9. Die Dokumentationspflichten müssen eingehalten werden (z. B. Vorblatt oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren). Sende- und Empfangsprotokolle sind vertraulich abzulegen, da sie dem Fernmeldegeheimnis unterliegen.
10. Vor Verkauf, Weitergabe oder Aussortieren von Telefaxgeräten ist zu beachten, dass alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.
11. Die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.

12. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, ist sie grundsätzlich zu deaktivieren. Nur für notwendige Wartungsarbeiten ist diese Funktion freizugeben. Nach Abschluss der Wartungsarbeiten müssen die eingestellten Parameter und Speicherinhalte kontrolliert werden.

3.3 Telefax in Bürokommunikationslösungen

Bei der Installation und Nutzung integrierter Telefaxlösungen sind die folgenden Regelungen zusätzlich zu den Bestimmungen für konventionelle Telefaxgeräte zu beachten:

1. Das verwendete Rechnersystem ist sorgfältig zu konfigurieren und zu sichern. Die IT-Sicherheit des verwendeten Rechners bzw. Netzes ist Voraussetzung für einen datenschutzgerechten Betrieb der Faxlösung. Dazu gehört unter anderem, dass kein Unbefugter Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken hat.
2. Beim Absenden ist auf die korrekte Angabe der Empfänger zu achten. Dazu sind die durch die Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlusslisten, in denen Empfänger und Verteiler mit aussagekräftigen Bezeichnungen versehen werden können, zu nutzen.
3. Die vielfältigen Nutzungsmöglichkeiten integrierter Faxlösungen erfordern die regelmäßige und besonders sorgfältige Überprüfung der in der Faxsoftware gespeicherten technischen Parameter, Anschlusslisten und Protokolle.
4. Der Einsatz kryptographischer Verfahren ist bei integrierten Faxlösungen unkompliziert und kostengünstig möglich, sofern beide Seiten kompatible Produkte einsetzen. Deshalb sind in diesem Fall personenbezogene Daten immer verschlüsselt und digital signiert zu übertragen, um das Abhören zu verhindern und um den Absender sicher ermitteln und Manipulationen erkennen zu können.
5. Schon bei der Beschaffung integrierter Telefaxlösungen ist darauf zu achten, dass ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechtlichen Erfordernisse des Nutzers zu gewährleisten.

4. Digitale Kopierer

4.1 Zweck

Digitale Kopierer enthalten Festplatten, auf denen sämtliche Kopien zumindest vorübergehend oder auch dauerhaft aufgezeichnet werden. Dabei passen auf eine 20 GB-Festplatte etwa 70.000 Dokumente. Neben stand-alone-Kopierern gibt es zunehmend netzangebundene Kopierer. Bei den per Netz zugänglichen Kopierern fallen neben den Kopier- oftmals auch Druck- und Scanndateien an sowie Protokolldateien der jeweils beteiligten Rechner bzw. Nutzer. Dieser Datenbestand kann, sofern nicht anders konfiguriert, oftmals über das Netz unbefugt eingesehen werden. Weiterhin kommt hinzu, dass viele dieser Geräte über Leasingverträge aufgestellt werden, so dass nicht nur bei einer Reparatur oder

bei einem Plattentausch, sondern spätestens mit der Rückgabe des Gerätes sensible Daten auf den Festplatten in falsche Hände geraten können.

Dieser Abschnitt der Dienstanweisung regelt den datenschutzrechtlichen Umgang mit digitalen Fotokopierern.

4.2 Maßnahmen zum Datenschutz

1. Bei geleasten Geräten ist von Vertragsbeginn an sicherzustellen, dass die Festplatte vor Rückgabe des Gerätes Physikalisch gelöscht werden kann.
2. Es sind möglichst Kopierer anzuschaffen, die die Möglichkeit passwortgeschützter Mitarbeiterverzeichnisse bieten, damit sichergestellt ist, dass Mitarbeiter nur auf ihre eigenen Dateien Zugriff haben.
3. Die Geräte müssen so eingestellt werden, dass nach jedem Kopier-, Scann- oder Druckvorgang die zugehörige Datei auf der Festplatte nach Abschluss der Aktion gelöscht wird. Soll eine Datei länger gespeichert werden, so muss dies explizit durch den Benutzer veranlasst werden.
4. Bei Rückgabe des Gerätes ist die Festplatte durch die Datenschutzfachkraft des Fachbereichs Zentralangelegenheiten physikalisch zu löschen. Der Löschvorgang ist schriftlich zu dokumentieren. Die Dokumentation ist dem behördlichen Datenschutzbeauftragten zuzuleiten.

5. Einsatz der automatisierten Datenverarbeitung

5.1 Zuständigkeiten und Verantwortungsbereiche beim Einsatz automatisierter Datenverarbeitung

Um die Benutzer von technischen Problemen zu entlasten und um den Einsatz einheitlicher Programme (Software) zu gewährleisten, wird bei dem Fachbereich Zentralangelegenheiten ein Sachgebiet „Datenverarbeitung“ eingerichtet.

Für die Zusammenarbeit mit den Benutzern gilt folgendes:

5.1.1. Verantwortungsbereich der Fachbereiche als nutzende Stellen

Es obliegt den Fachbereichen

- die Aussage über Zweckmäßigkeit und Wirtschaftlichkeit des PC-Einsatzes bzw. des Einsatzes eines Verwaltungsverfahrens auf den Zentralrechnern im jeweiligen Fall,
- die Verantwortung für einen ordnungsgemäßen Arbeitsablauf und die Richtigkeit des Arbeitsergebnisses,
- die Sicherstellung der datenschutzrechtlichen Zulässigkeit der Speicherung und Verarbeitung von personenbezogenen Daten in von Benutzer erstellten Dateien,
- die Meldung von individuell erstellten Dateien mit personenbezogenen Daten an den behördlichen Datenschutzbeauftragten,

- die schriftliche Benennung eines Verfahrensverantwortlichen für Anwendungsprogramme, der zugleich Ansprechpartner für das Sachgebiet „Datenverarbeitung“ ist,
- die Meldung von automatisierten, personenbezogenen Dateien an den behördlichen Datenschutzbeauftragten vorzunehmen.

Die Benutzer bzw. Benutzerkreise haben zu gewährleisten, dass im Rahmen der Nutzungsbestimmungen Geräte und Systeme vor unbefugter, unsachgemäßer und missbräuchlicher Benutzung geschützt sind und auf Betriebsunterlagen und Programme nicht unberechtigt zugegriffen werden kann. Vom Benutzer erstellte Anwendungen und Verfahren sind so aufzubauen und zu dokumentieren, dass ein sachverständiger Berechtigter in angemessen kurzer Zeit die Nutzung und die Pflege des Programms vollverantwortlich übernehmen kann. Die Erstellung eigener Anwendungen bedarf der vorherigen Genehmigung des Sachgebietes „Datenverarbeitung“.

5.1.2. Zuständigkeiten des Sachgebietes „Datenverarbeitung“

Die für die Beratung und Betreuung der Benutzer zuständigen Mitarbeiter des Sachgebietes „Datenverarbeitung“ haben die Aufgabe,

- in Zusammenarbeit mit den Nutzern bei der Bedarfsfeststellung Gerätebedarf und Software zu planen und gegebenenfalls Beschaffungsmaßnahmen einzuleiten,
- Geräte und Software zu installieren sowie Benutzerprofile einzurichten,
- Geräte und Softwareprodukte vor deren Einsatz zu testen und zuzulassen,
- Störungen einzugrenzen, nach Möglichkeit zu beheben und bei Systemabstürzen den Wiederanlauf zu gewährleisten,
- Kontakt mit Hard- und Softwarelieferanten sowie Servicefirmen zu pflegen,
- Maßnahmen für eine regelmäßige Datensicherung auf externe Datenträger vorzusehen,
- die an den einzelnen Arbeitsplätzen installierte Gerätekonfiguration und die dazu gehörenden Softwareprodukte in einem zentralen Register zu führen,
- erforderliche Fortbildungsmaßnahmen im Office-Bereich für die Benutzer einzuleiten,
- die Entwicklung, Freigabe und Pflege von Anwendungen für die PC’s, soweit dies nicht durch die Benutzer selbst erfolgt, vorzunehmen,
- die datenschutzrechtliche Freigabe von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, zu beantragen,
- die allgemeinen Grundsätze im Rahmen der Nutzungsbestimmungen festzulegen,
- Regelungen für den Betrieb auf den Zentralservern, Verwaltung und Sicherung der Systemressourcen zu treffen.
- eine IT-Sicherheitsrichtlinie für die Stadtverwaltung Fritzlar zu erstellen und fortzuschreiben.

5.2 Ausstattung des Arbeitsplatzes

Für die computergerechte Ausstattung eines Arbeitsplatzes sorgt die Dienststelle.

Die Geräte sind so aufzustellen, dass eine unbefugte Kenntnisnahme von dargestellten oder ausgedruckten Informationen (z. B. durch Besucher oder sonstige Nichtbeteiligte) nach Möglichkeit ausgeschlossen ist.

5.3 Benutzungsbestimmungen

Für die Benutzung der PC's gelten folgende Bestimmungen:

5.3.1. Grundsätze

Für die Durchführung dienstlicher Aufgaben dürfen nur vom Sachgebiet „Datenverarbeitung" zugelassene bzw. installierte Hard- und Softwarekomponenten verwendet werden. Die Nutzung privater Geräte, Datenträger und selbst beschaffter Software ist nur mit vorheriger Genehmigung des Sachgebietes „Datenverarbeitung" gestattet.

Wird ein Laptop außerhalb der Diensträume verwendet und werden darauf personenbezogene Daten gespeichert, muss eine Software zur Festplattenverschlüsselung installiert sein.

Die Weitergabe von Programmen oder Daten ist nur im Rahmen der gesetzlichen Bestimmungen zulässig.

Jeder Computer-Arbeitsplatz ist einem Benutzer oder einem Benutzerkreis zugeordnet. Dieser ist verantwortlich für die Beachtung der Vorschriften und Anweisungen und hat den Arbeitsplatz vor unbefugtem Zugriff zu schützen.

5.3.2. Verhaltensmaßnahmen

Außenstehende Personen (z. B. Wartungspersonal) dürfen sich nur in Begleitung eines Mitarbeiters der Stadtverwaltung in Räumen mit PC-Ausstattung aufhalten. Unbesetzte Räume sind abzuschließen.

5.3.3. Informationspflichten

Alle sicherheitsrelevanten Ereignisse (unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung usw.) sind sofort an das Sachgebiet Datenverarbeitung zu melden. Es dürfen keine eigenen Aufklärungsversuche unternommen werden, da evtl. wertvolle Hinweise und Spuren verwischt werden oder verloren gehen könnten.

5.3.4. Arbeitsablauf

Der Bildschirmschoner ist auf jedem PC zu aktivieren.

Beim längeren Verlassen des Arbeitsplatzes (insbesondere bei Pausen und Dienstgängen) ist der PC durch den Benutzer zu sperren.

Drucker sind so aufzustellen, dass sie von berechtigten Nutzern kontrolliert werden können. Ist eine Kontrolle der Drucker nicht möglich, sind alle Ausdrucke unmittelbar nach dem Ausdruck aus dem Drucker zu entfernen. Der Zugriff Unbefugter auf die Geräte ist zu verhindern.

5.3.5. Umgang mit Passwörtern

Das persönliche Kennwort (Passwort) bestimmt der Benutzer selbst. Es darf keine Rückschlüsse auf seinen Besitzer zulassen. Die Passwortlänge muss mindestens acht Stellen betragen.

PC-Benutzer werden vom System aufgefordert, ihr Passwort alle 80 Tage zu ändern.

Vom Hersteller eines Softwareproduktes vorgegebene Benutzerkennungen und Passworte sind unmittelbar nach der Installation der Anwendung zu ändern.

Das Ausprobieren, das Ausforschen und die Benutzung fremder Zugriffsberechtigungen (Benutzerkennungen, Passworte) sind unzulässig.

Die Weitergabe und das Zurverfügungstellen von eigenen Benutzerkennungen, sofern vorhanden, für eine Benutzung durch Dritte ist unzulässig. Es wird ausdrücklich darauf hingewiesen, dass in einem derartigen Fall aus den Protokolldaten die Identität des Benutzers hervorgeht. Jegliche Aktivität – auch unzulässige – durch diesen Dritten wird also dem eigentlich berechtigten Mitarbeiter zugeschrieben.

5.3.6. Umgang mit Datenträgern

Datenträger (z. B. Disketten, CD’s, Streamerbänder, USB-Sticks) dürfen nur von Berechtigten aufbewahrt, befördert und benutzt werden.

Datenträger sind grundsätzlich auf dem Serversystem und nicht auf den PC’s zu speichern.

Daten auf den PC’s werden nicht durch das Sachgebiet „Datenverarbeitung“ gesichert. Für PC’s die nicht im Datennetz der Stadtverwaltung eingebunden sind, ist das Kopieren auf externe Datenträger nur für die regelmäßige Datensicherung gestattet. Ansonsten ist das Kopieren von Daten auf externe Datenträger nur zum berechtigten Datenaustausch gestattet.

Festplattenspeicher dürfen nur der EDV-Stelle überlassen werden. Werden sie ausnahmsweise an Servicefirmen weitergegeben, sind die Daten vorher physikalisch zu löschen. Sofern eine Löschung nicht angezeigt ist, ist eine vertragliche Regelung im Sinne von Nr. 1.3 Herbei zu führen.

5.3.7. Verwaltung von Datenträgern

Jeder PC-Benutzer hat einen Vermerk zu fertigen, sobald Datenträger mit sensiblen Daten außer haus gegeben werden. Eine Durchschrift des Vermerks erhält der Datenschutzbeauftragte.

6. Systemadministration

6.1 Grundsatz

Das Sachgebiet „Datenschutz“ ist für die Systemadministration und damit auch für die Datensicherheit und den Datenschutz innerhalb der Stadtverwaltung Fritzlar verantwortlich. Die Mitarbeiter dieses Sachgebietes haben im Rahmen der zur Verfügung stehenden Haushaltsmittel alle technischen Maßnahmen zu treffen, um den Missbrauch des Netzwerkes der Stadtverwaltung zu verhindern und Datenverlusten vorzubeugen.

Hierzu legen sie ein IT-Sicherheitskonzept fest, welches mit dem behördlichen Datenschutzbeauftragten abzustimmen ist.

Jeder Beschäftigte mit Befugnissen zur Systemadministration ist verpflichtet, über alle ihm zur Kenntnis gelangten personenbezogenen Daten Verschwiegenheit zu wahren.

6.2 Mitteilungspflichten

Die verantwortlichen Systemadministratoren sind mit dem verantwortlichen Administrationsbereich dem behördlichen Datenschutzbeauftragten zu benennen.

Ereignisse, welche die Datenintegrität oder die Datensicherheit beeinträchtigen können, sind dem behördlichen Datenschutzbeauftragten unverzüglich mitzuteilen.

6.3 Administratorkennwort

Der administrative Zugang ist ausschließlich für Zwecke der Systemverwaltung zu verwenden. Das jeweilige Kennwort muss aus mindestens acht Zeichen bestehen und darf keinen Begriff erhalten, der einem Wörterbuch zu entnehmen ist, oder auf die Person oder die Funktion hindeutet. Es muss Groß- und Kleinbuchstaben sowie Zahlen enthalten.

Die Kennwörter für den administrativen Zugang sind geheim zu halten. Hiervon unbeschadet ist jedes Kennwort für den administrativen Zugang in einem eigenen versiegelten und mit dem Benutzernamen versehenen Umschlag zu hinterlegen und im Tresor der Verwaltung zu verwahren.

6.4 Pflicht zur Protokollierung

Alle Systemarbeiten sind zu Protokollieren. Sofern keine automatische Protokollierung durch das System erfolgt, sind diese Arbeiten unter Angabe des Namens, Datums, Uhrzeit und Beschreibung der Tätigkeit schriftlich zu dokumentieren.

6.5 Fernwartung durch Systemadministration

Die Befugnis zur Systemadministration schließt die Befugnis zur Fernwartung der PC-Arbeitsplätze ein. Fernwartung ist auf das unabdingbare Maß zu beschränken. Die Systemadministratoren haben über personenbezogene Daten, von denen sie im Rahmen der Fernwartung Kenntnis erlangen, Verschwiegenheit zu wahren.

Die Verbindungsaufnahme zur Fernwartung muss vom Anwender ausdrücklich bestätigt werden. Sofern die Bestätigung nicht innerhalb von 5 Minuten erfolgt, wird der Verbindungsversuch zurückgewiesen.

Die Software zur Fernwartung wird durch ein Symbol in der Leiste neben der Bildschirmuhr signalisiert. Bei einem laufenden Fernwartungsprozess ändert dieses Symbol die Farbe.

Anwendungen, die schützenswerte personenbezogene Daten enthalten (Sozialdaten, Personaldaten, Meldedaten, Daten, die dem Steuergeheimnis unterliegen u. ä.) sind vor dem Fernwartungsprozess zu beenden. Eine Ausnahme hierfür gilt nur, wenn der Zugriff auf die Programme zum Zwecke der Wartung und Systempflege unabdingbar ist.

Der Anwender ist verpflichtet, den Fernwartungsprozess zu beobachten und beim Verdacht einer missbräuchlichen Verwendung die Verbindung zu unterbrechen. Der behördliche Datenschutzbeauftragte ist von dem Vorgang zu unterrichten.

Eine Verhaltenskontrolle der Beschäftigten durch Fernwartungsprozesse ist untersagt.

6.6 Fernwartung durch externe Stellen

6.6.1. Maßnahmen zur Zugangskontrolle

Bei der Fernwartung muss der Verbindungsaufbau stets durch den Kunden erfolgen, so dass Wartungsarbeiten nur mit Wissen und Willen des Kunden erfolgen können.

Der Kreis des autorisierten Wartungspersonals ist festzulegen; ohne genaue Identifizierung dürfen keine Wartungsarbeiten beginnen.

Um zu verhindern, dass ein unbefugter Teilnehmer Zugriff auf das DV-System erhält, ist die Verbindung vom DV-System aus aufzubauen.

Der Anwender muss die Fernwartungsarbeiten jederzeit abbrechen können.

6.6.2. Kontrolle der Datenübertragung

Wenn personenbezogene Daten an die Fernwartungszentrale übertragen werden müssen, ist vorher die Erlaubnis durch den behördlichen Datenschutzbeauftragten einzuholen.

Die Übertragung von Daten aus dem DV-System der Stadtverwaltung an die Fernwartungszentrale ist nur bei gleichzeitiger Protokollierung der übertragenen Daten zuzulassen.

Die Kontrolle der protokollierten Daten ist DV-technisch durch geeignete Kommandos und Dienstprogramme zu unterstützen.

Alle Wartungs- und Übertragungsaktivitäten müssen auf dem Bildschirm des Anwenders zum Mitlesen sichtbar gemacht werden.

6.6.3. Maßnahmen zur Speicherkontrolle

Es sind alle Programme durch Passwörter zu schützen, soweit diese bei der Wartung physisch im Zugriff bleiben.

Das Wartungspersonal muss sich einer Anmeldeprozedur unterwerfen. Diese muss aus einer Identifikation und einer Authentifikation bestehen (i. d. R. Benutzerkennung und Passwort).

Die Fernbetreuung von Anwenderprogrammen ist unter einer Kennung vorzunehmen, die keine Systemverwalterprivilegien einschließt.

Werden Test- und Serviceprogramme des Herstellers auf der DV-Anlage gespeichert, sind diese unter der Wartungskennung abzuspeichern. Ein Zugriff darf nur dem Wartungspersonal und der Systemverwaltung möglich sein.

Der Zugriffschutz muss hinreichend differenziert sein.

Im Rahmen der Fernwartung ist der Zugriff auf Daten, die im Netzwerk der Stadtverwaltung oder auf dem Anwender-PC gespeichert sind, grundsätzlich zu verhindern. Hierzu sind z. B. die Laufwerke, auf denen diese Daten gespeichert werden, vom DV-System physisch abzutrennen, soweit dies technisch möglich ist.

Ein Einspielen von Änderungen ins Betriebssystem, in systemnahe Software oder Anwendungsfremdsoftware im Rahmen der Fernwartung ist nicht zuzulassen. Die Änderungen sind ausschließlich vor Ort entweder von der Systemadministration selbst oder nach Freigabe durch den behördlichen Datenschutzbeauftragten vom Software-Hersteller in die entsprechende Software zu übernehmen. Dasselbe gilt für die Fehlerbehebung.

Wartungs- und Diagnosearbeiten im laufenden Betrieb, insbesondere wenn sie die Software betreffen, sind unter ständiger Kontrolle eines Systemadministrators oder einer von ihr beauftragten und eingewiesenen Person durchzuführen.

Es ist auszuschließen, dass andere Software oder gespeicherte Daten durch die Wartung verändert werden können.

Es ist auszuschließen, dass Anwendungsprogramme durch die Fernwartung aktiviert werden können, solange Dateien im direkten Zugriff stehen.

6.6.4. Maßnahmen zur Zugriffskontrolle

Für den Fall, dass in einem Wartungsvorgang ein Zugriff auf Dateien mit Daten der Verwaltung notwendig ist, sind nach Abschluss der Wartungsarbeiten die offenbarten Passwörter unverzüglich zu ändern.

Alle Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festgehalten werden, sind zu überprüfen und zur Beweissicherung mindestens ein Jahr aufzubewahren. die Verpflichtung des Verantwortlichen der Verwaltung, den Wartungsvorgang am Bildschirm zu verfolgen und gegebenenfalls zu unterbrechen, bleibt davon unberührt.

6.6.5. Maßnahmen zur Organisationskontrolle

Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenz und Pflichten zwischen dem Wartungspersonal und den Bediensteten der Stadtverwaltung zu treffen. Art und Umfang der Wartung (Hardware und Software) sind schriftlich festzulegen.

Das Wartungspersonal ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten.

Eine Weitergabe von – bei der Fernwartung übertragenen – Daten an Dritte ist vertraglich zu untersagen. Diese Daten sind ausschließlich für zwecke der Wartung zu verwenden und nach Abschluss der Wartungsarbeiten oder der Fehlersuche unverzüglich zu löschen.

Hinsichtlich der Fernwartung ist ein separater Vertrag abzuschließen, in dem Sicherungsmaßnahmen, auch die der Fernwartungszentrale, festgelegt werden und die Kontrolle der Einhaltung aller Maßnahmen geregelt wird.

Zur DV-Revision ist das Wartungs- bzw. Fernwartungskonzept schriftlich zu dokumentieren.

Die Systemadministratoren sind regelmäßig bezüglich der Möglichkeiten der Fernwartung zu schulen.

Die Einhaltung der getroffenen Sicherheitsmaßnahmen ist regelmäßig zu überprüfen.

7. Schlussvorschriften

7.1 Rechtscharakter

Die Dienstanweisung ist eine verwaltungsinterne Vorschrift.

7.2 Sanktionen

Grob fahrlässige oder vorsätzliche Verstöße gegen diese Dienstanweisung und die sonstigen Regelungen und Vorschriften bzgl. des Datenschutzes können dienst- und arbeitsrechtliche sowie straf- und haftungsrechtliche Konsequenzen haben.

7.3 Aufhebung von Vorschriften

Die Dienstanweisung zur Einhaltung des Datenschutzes und der Datensicherheit bei der Stadtverwaltung Fritzlar vom 01.11.1989 wird aufgehoben.

7.4 Weitere Regelungen

Regelungen zur E-Mail- sowie Internetnutzung werden durch den hier federführenden Fachbereich gesondert getroffen. Eine mögliche Beteiligung des Personalrates ist zu beachten

7.5 Inkrafttreten

Diese Dienstanweisung tritt am 01.03.2010 in Kraft.