

**Dienstanweisung
für den Datenschutz und die Datensicherheit
bei der Stadtverwaltung Trier
(DA DAT)**

Gliederung

Vorbemerkungen

Teil A – Allgemeines

Teil B – Personenbezogene und vertrauliche Datenverarbeitung in automatisierten
Verfahren

Teil C – Entwicklung und Steuerung von automatisierten Verfahren

Teil D – Handling von Medien mit vertraulichen und personenbezogenen Daten (Schriftstücke,
Pläne, Dokumente, Akten) und deren Vernichtung

Teil E – Aufgaben des Datenschutzbeauftragten

Teil F - Schlussbestimmungen, Inkrafttreten

Anlagen:

1. Verpflichtung zur Einhaltung des Datenschutzes
2. Nachweis eingehender Datenträger
3. Begleitschein für den Transport von Datenträgern
4. Anmeldung zum Datenschutzregister
5. Hinweise für die Gestaltung und den Einsatz von Passwörtern
6. Sicherheitsstufen nach DIN 32 757 zum Vernichten vertraulicher und personenbezogener Medien.

Vorbemerkungen

Gemäß § 9 Abs. 1 Landesdatenschutzgesetz (LDSG) ist die Stadtverwaltung Trier verpflichtet technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen des Landesdatenschutzgesetzes zu gewährleisten und gemäß § 9 Abs. 5 LDSG die Sicherungsmaßnahmen in einer Dienstanweisung festzulegen.

Diese Verpflichtung umfasst neben den automatisierten Verfahren auch die herkömmliche Aktenführung oder die Verarbeitung personenbezogener Daten in nichtautomatisierten Dateien (z.B. Karteien). Danach sind alle Festlegungen, die unabhängig vom Verfahren und der Art der Verarbeitung sind, und damit generell zu beachten sind, in einer Dienstanweisung festzuhalten.

Die Regelungen der Dienstanweisung sind von allen Mitarbeitern, die personenbezogene Daten im Sinne des § 3 Abs. 1 LDSG verarbeiten, zu beachten.

Um auf Wiederholungen von gesetzlichen Bestimmungen und des Inhalts von Verwaltungsvorschriften verzichten zu können, wird auf die im verwaltungsinternen Netzwerk hinterlegten Ausführungen zum Datenschutz verwiesen.

Teil A

Allgemeines

1. Diese Dienstanweisung enthält nähere Bestimmungen über den Umgang mit personenbezogenen sowie sonstigen vertraulichen Daten und den technisch-organisatorischen Datenschutz
 - a) bei der Verarbeitung von Daten in automatisierten Verfahren durch die Anwender (Teil B),
 - b) bei der Entwicklung und Steuerung von automatisierten Verfahren (Teil C),
 - c) beim Handling und Vernichtung von Medien mit personenbezogenen oder sonstigen vertraulichen Daten (Schriftstücke, Pläne, Dokumente, Akten, elektronische Datenträger) (Teil D)
 - d) sowie über die Bestellung und die Aufgaben des behördlichen Datenschutzbeauftragten (Teil E).

Sie ist von allen MitarbeiterInnen, die personenbezogene Daten im Sinne des § 3 Abs. 1 LDSG und vertrauliche Informationen der Stadtverwaltung verarbeiten, zu beachten.

2. MitarbeiterInnen, die Umgang mit Daten i.S. von Teil A 1. a), b) und c) haben, sind nach § 8 LDSG unter Verwendung des als Anlage 1 angefügten Vordrucks auf die Einhaltung des Datengeheimnisses zu verpflichten. Die Verpflichtung erfolgt durch ZL 10/11.
3. Anträge auf Auskunft von betroffenen Personen sind von der zuständigen Organisationseinheit im Sinne § 18 LDSG zu gewähren. Für den Fall der Auskunftsuntersagung ist der Antrag dem Datenschutzbeauftragten zuzuleiten, der über die weitere Behandlung entscheidet.
4. Der Datenschutzbeauftragte ist in allen Angelegenheiten, die den Datenschutz und insbesondere den technischen und organisatorischen Datenschutz betreffen, beratend hinzuzuziehen.

Teil B

Personenbezogene und sonstige vertrauliche Datenverarbeitung in automatisierten Verfahren

1. Die Räume, in denen sich zentrale Einrichtungen der Datenverarbeitung oder Datenträger befinden, sind von außen verschlossen zu halten und es dürfen nur die von ZD 16 bestimmten MitarbeiterInnen Zutritt haben. Reinigungs-, Wartungs- und ähnliche Arbeiten dürfen nur in Anwesenheit dieser MitarbeiterInnen durchgeführt werden.
2. Datenträger sind mit einem Aufkleber zu versehen, der mindestens folgende Angaben enthalten soll:
 - Behördenbezeichnung
 - Kennzeichnung des Datenträgers
 - Hinweis ob Original oder Kopie
 - Datum der Erstellung bzw. letzten Änderung
 - Inhalt des Datenträgers
 - Namenszeichen des Verantwortlichen.
3. Nicht benötigte Datenträger mit personenbezogenen und sonstigen vertraulichen Daten sind unter Verschluss zu halten.

4. Ein- und ausgehende Datenträger sind in eine Liste (Anlage 2) einzutragen. Die Liste wird von der/dem jeweiligen, vom Fachamt bestimmten MitarbeiterIn geführt. Vor der weiteren Verarbeitung von eingehenden Datenträgern ist z.B. durch eine Virenprüfung sicherzustellen, dass von ihnen keine Gefährdung für automatisierte Verfahren ausgeht.
5. Datenträger mit personenbezogenen und sonstigen vertraulichen Daten dürfen innerhalb der Stadtverwaltung nur persönlich oder durch Mitarbeiter der Botenmeisterei weitergegeben werden. Bei der Überstellung von Datenträgern sind Begleitscheine mitzuführen (Anlage 3). Die Versendung auf dem Postweg erfolgt in der Form eines Wertbriefs.
6. Bei Unterbrechung, Beendigung der Bildschirmarbeit mit personenbezogenen und sonstigen vertraulichen Daten und/oder Verlassen der Diensträume muss sichergestellt sein, dass der Bildschirm in der Zwischenzeit nicht von Dritten genutzt werden kann (sperrern oder abmelden).
7. Bildschirmgeräte sind nach Möglichkeit so aufzustellen, dass sie von Unbefugten nicht eingesehen werden können.
8. Passwörter sind in regelmäßigen Zeitabständen, längstens bis zu 90 Tagen, durch den Nutzer zu ändern (Passwortgestaltung siehe Anlage 5). ZD 16 installiert für Arbeitsplätze an denen personenbezogene und sonstige vertraulichen Daten verarbeitet werden eine automatische Abfrage zur Passwortänderung.
9. Datenbestände sind in regelmäßigen Zeitabständen zu sichern.
10. Protokolle, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen erstellt werden, dürfen nur von den jeweils zuständigen Amtsleitern gemeinsam mit dem Datenschutzbeauftragten und dem Personalrat eingesehen werden.
11. Die Protokolldaten dürfen gemäß § 13 Abs. 5 LDSG nur zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage genutzt werden. Ausdrücklich untersagt ist nach § 31 Abs. 5 LDSG deren Verwendung für Leistungs- und Verhaltenskontrollen. Soweit keine andere Vorschrift existiert, sollte eine Aufbewahrungsdauer von einem Jahr nicht überschritten werden. Soweit personenbezogene Protokolldaten zum Zwecke gezielter Kontrollen angefertigt werden, ist eine kürzere Speicherungsfrist vorzusehen; in der Regel

reicht dabei eine Aufbewahrung bis zur tatsächlichen Kontrolle aus.

12. Für die Weitergabe von personenbezogenen Daten via Internet gilt die Rahmenvorgabe Internet.

Teil C

Entwicklung und Steuerung von automatisierten Verfahren für die Verarbeitung von personenbezogenen und sonstigen vertraulichen Daten

1. Für jedes Verfahren in dem personenbezogene Daten automatisiert verarbeitet werden (§ 27 Abs. 1 LDSG) ist durch das jeweilige Fachamt eine Verfahrensbeschreibung zu erstellen und fortzuschreiben. Hierfür ist der Vordruck (siehe Anlage 4) zu verwenden. Sie dient als Grundlage für das vom Datenschutzbeauftragten geführte Verzeichnis (§ 10 Abs. 2 LDSG) und für die Anmeldung zum Datenschutzregister.

Alle eingesetzten Geräte werden von ZD 16 / ZD 10 in einem Geräteverzeichnis erfasst.

2. Die Anmeldung beim Landesbeauftragten für den Datenschutz (LfD) nach § 27 Abs. 1 LDSG erfolgt durch die jeweilige Organisationseinheit unter Verwendung des vorgesehenen Vordrucks (siehe Anlage 4). Die Übersendung erfolgt über den Datenschutzbeauftragten. Bei der Einrichtung eines automatisierten Übermittlungsverfahrens gemäß § 7 LDSG ist auf die rechtzeitige Beteiligung des Datenschutzbeauftragten und des LfD zu achten.
3. Für autorisierte MitarbeiterInnen ist eine Benutzerkennung einzurichten und ein Anfangspasswort zuzuweisen. Dieses ist bei der ersten Anmeldung durch den Anwender sofort zu ändern. Sofern möglich, ist diese Änderung automatisiert vorzugeben.
4. Auch für das Wartungspersonal ist eine Benutzerkennung mit Passwort zu vergeben. Es ist sicherzustellen, dass diese Kennung nur für Wartungsfälle benutzt werden kann. Die Inanspruchnahme ist zu dokumentieren (z.B. Eintragung in Logbuch, automatische Protokollierung).
5. Benutzername, Zeitpunkt der An- und Abmeldung sowie fehlerhafte Zugriffsversuche sind zu protokollieren. Weitergehende Protokollierungen werden in Absprache mit den zuständigen Amts-, Organisationsleitern und ZD 16 festgelegt. Der Datenschutzbeauftragte und der Personalrat sind zu beteiligen.

6. ZD 16 hat die Aufgabe die automatisierte Datenverarbeitung gegen unbefugten Zugriff und gegen Zerstörung des Datenbestandes (Virenschutz) mittels geeigneter Produkte zu schützen.
7. Für die Einrichtung eines Verfahrens zur Fernwartung trifft ZD 16 nähere Bestimmungen. Der Datenschutzbeauftragte ist zu beteiligen.
8. Die Verarbeitung von Daten im Auftrag (auch nicht personenbezogene) durch andere Personen oder Stellen ist nur mit Zustimmung von ZD 16 zulässig. Der Datenschutzbeauftragte ist vorher zu hören. Der Vertragsgestaltung sind die Empfehlungen des LfD zur „Datenverarbeitung im Auftrag“ (§ 4 LDSG) zu Grunde zu legen. Weiterhin ist zu prüfen, inwieweit hierfür spezialgesetzliche Regelungen bestehen (z.B. § 80 SGB X).

Teil D

Handling von Medien mit vertraulichen und personenbezogenen Daten (Schriftstücke, Pläne, Dokumente, Akten, elektr. Datenträger) und deren Vernichtung

1. Medien mit vertraulichen und personenbezogenen Daten (Schriftstücke, Pläne, Dokumente, Akten, elekt. Datenträger) sind unter Verschluss aufzubewahren.
2. Es sind technische und organisatorische Maßnahmen (§ 9 Abs. 4 LDSG) zu treffen, die verhindern, dass diese von Unbefugten eingesehen, benutzt, kopiert, verändert oder entwendet werden können.
3. Behördenintern archivierte Medien i. S. von Teil D 1. sind entsprechend den Regelungen der Aktenordnung in der jeweils gültigen Fassung zu behandeln.
4. Sind Medien i. S. von Teil D 1. unter Beachtung der Aktenverordnung zur Vernichtung bestimmt so ist jedes Fachamt in seinem Bereich vom Sammeln bis zur ordnungsgemäßen Vernichtung verantwortlich. Die Fachämter haben dafür Sorge zu tragen, dass Unbefugte keine Kenntnis über den Inhalt der zu vernichtenden Medien erhalten.

5. Das Vernichten der Medien erfolgt durch Zerkleinern mittels Schneidwerken. Die DIN 32 757 regelt in Abhängigkeit der Schutzwürdigkeit des Dateninhaltes die Größe der Abfallstreifen bzw. der -partikel und teilt diesen Zusammenhang in 5 Sicherheitsstufen ein. Siehe Anlage 6 Es kann unter Berücksichtigung von DIN 32 757 wie folgt vernichtet/entsorgt werden:
 - 5.1. Geringe Mengen der Schutzstufe 1 und 2 nach DIN 32 757 (z.B. Einzelblätter) können in den Ämtern von den MitarbeiterInnen vor Ort mit kleinen Aktenvernichtungsgeräten selbst zerkleinert werden.
 - 5.2. Große Mengen von Medien i.S. von Teil D 1. und insbesondere auch die Medien, die in die Sicherheitsstufe 3 und höher einzustufen sind, werden zentral durch ZD 10 zerkleinert.
 - 5.3. Der Transport zur zentralen Datenträgervernichtung kann selbst durchgeführt und/oder in Absprache mit ZD 10 organisiert werden (Terminvereinbarung).
 - 5.4. Beim Transport, Lagern und der Vernichtung sind Maßnahmen zu treffen, die verhindern, dass Unbefugte auf diese Daten zugreifen können. (§ 9 Abs. 4 LDSG). In jedem Fachamt ist eine individuelle Organisation durch eine Ergänzung dieser Dienstanweisung im Einzelnen festzulegen (§ 9 Abs. 5 LDSG)
 - 5.5. Für zerkleinerte Medien bedarf es im Sinne des Datenschutzes keiner besonderen Aufbewahrung und Entsorgung.

Teil E

Datenschutzbeauftragter

Stellung, Rechte und Aufgaben

1. Die Bestellung und Abberufung des Datenschutzbeauftragten unterliegt der Mitbestimmung des Personalrates (§ 80 Abs. 2 Nr. 8 LPersVG).
 - 1.1. Der Datenschutzbeauftragte ist in der Wahrnehmung dieses Amtes organisatorisch keiner Organisationseinheit zugeordnet, sondern unmittelbar dem Oberbürgermeister unterstellt. Gegenüber dem Oberbürgermeister hat er ein direktes Vortragsrecht. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.
2. Er ist über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.
 - 2.1. Er ist bei der Erfüllung seiner in § 11 LDSG genannten Aufgaben durch die Verwaltung zu unterstützen.

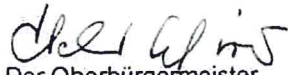
- 2.2. Er hat das Recht, jederzeit das Verfahrens- und Geräteverzeichnis einzusehen. Auf Verlangen ist ihm eine Abschrift oder Kopie zur Verfügung zu stellen.
- 2.3. Ihm ist Kenntnis vom Schriftverkehr mit dem LfD zu geben.
3. Der Datenschutzbeauftragte hat gem. § 11 Abs. 3 LDSG folgende Aufgaben:
 - 3.1. Er hat die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften des LDSG, den hierzu ergangenen Verordnungen und Vorschriften sowie mit dieser Dienstanweisung vertraut zu machen und ihnen Hinweise zur Einhaltung dieser Bestimmungen zu geben.
 - 3.2. Bei der Einführung und Anwendung von Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, wirkt er auf die Einhaltung dieser Bestimmungen hin.
 - 3.3. Er unterstützt die Dienststelle bei der Durchführung der Maßnahmen des technischen und organisatorischen Datenschutzes, bei der Erstellung von Geräte- und Verfahrensverzeichnissen, Verfahrensbeschreibungen und Anmeldungen zum Datenschutzregister.
 - 3.4. Er hat darauf hinzuwirken, dass die bei der Verarbeitung personenbezogener Daten tätigen Personen gemäß den datenschutzrechtlichen Bestimmungen auf das Datengeheimnis verpflichtet werden.
 - 3.5. Er koordiniert die Maßnahmen für die Sicherstellung des technischen und organisatorischen Datenschutzes. Er überwacht die Einhaltung der Bestimmungen dieser Dienstanweisung.
 - 3.6. Er wirkt darauf hin, dass nach Teil B Nr. 10 und 11 die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen erstellten Protokolle in regelmäßigen Abständen auf eventuell vorhandene Unregelmäßigkeiten überprüft werden. Die Prüfung der Protokolle ist von dem Datenschutzbeauftragten zu dokumentieren. Die Ergebnisse sind im Tätigkeitsbericht (s. Nr. 10) zu veröffentlichen.
 - 3.7. Er hat bei der Benachrichtigung und der Auskunftserteilung gemäß den datenschutzrechtlichen Bestimmungen mitzuwirken. Er ist bei Zweifelsfragen, die die Anwendung des LDSG, anderer Vorschriften zum Datenschutz und diese Dienstanweisung betreffen, zu beteiligen.
 - 3.8. Er ist verpflichtet alle zwei Jahre einen Bericht über seine Tätigkeit zu erstellen.

Teil F**Schlussbestimmungen, Inkrafttreten**

Der Personalrat hat dieser Dienstanweisung zugestimmt.

Diese Dienstanweisung tritt am **01. April 2003** in Kraft. Gleichzeitig tritt die Dienstanweisung über den Datenschutz und die Datensicherheit bei der Stadtverwaltung vom 20.10.1988 außer Kraft.

Trier, den 25/3 2003


Der Oberbürgermeister

Kopie

des/der Bediensteten Familienname Vorname/n

- Mir ist bekannt, dass es untersagt ist, vertrauliche und personenbezogene Daten unbefugt zu einem anderen als zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren. Die Verpflichtung besteht auch noch nach Beendigung meiner Tätigkeit fort.

Mir ist bekannt, dass Verstöße gegen die Verpflichtung zur Wahrung des Datengeheimnisses nach § 37 LDSG mit Geld oder Freiheitsstrafe geahndet werden können; davon unberührt bleibt die Strafbarkeit nach anderen Vorschriften, z.B. §§ 203, 353 b StGB.

- ☐ - ist jederzeit in der Systemablage, zur Zeit unter *Ablage\$ auf 'Rh-fs-19' (O:)\Datenschutz\Formulare* abrufbar.
- ☐ - steht zur Einsicht in der Bibliothek/beim behördlichen Datenschutz-beauftragten bereit.
- ☐ - ist mir ausgehändigt worden.

Trier den, Datum Unterschrift

Nachweis eingehender Datenträger
(für Ausgänge sinngemäß)

lfd. Nr.	Datum	Absender	Empfänger	Art des Datenträgers	Kenn- zeichnung	Bemerkungen
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						

Begleitschein für Datenträgertransport

Absender:	Empfänger:
Bearbeiter(in):	
Tel.-Nr.:	Tel.-Nr.:

Art und Inhalt des Datenträgers:

.....

.....

ggf. Anzahl und Größe der Dateien:**Tag und Uhrzeit der Absendung:**

Transportiert durch

☐ Boten

Herrn/Frau

☐ Abholer

Herrn/Frau

☐ Post**Datum und Unterschrift des Absenders**

Empfangsbestätigung (ggf. auch telefonisch)

Tag/Uhrzeit des Empfangs:

Anmeldung zum Datenschutzregister

Das Anmeldeformular liegt beim Datenschutzbeauftragten vor und ist jederzeit in der Systemablage (öffentlicher Ordner), zur Zeit unter

ablage\$ auf 'Rh-fs-19' (O:)\Datenschutz\Verfahrens anmeldung\DS-Antrag.doc
abrufbar.

Hinweise für die Gestaltung und den Einsatz von Passwörtern**Für den Benutzer:**

- Ihr Passwort sollte für Sie leicht zu merken, für andere jedoch schwer zu erraten sein. Sie sollten daher keine Trivialpasswörter wie Namen, Geburtstage, Telefonnummern, Urlaubsziele verwenden. Auch gängige Zeichenfolgen (123456, abcdef, 08/15, 4711, sesam) bieten keinen wirksamen Schutz. Vermeiden Sie Systematiken (sesam1, sesam2, sesam3...).
- Nutzen Sie Gestaltungsmöglichkeiten wie Zeichenmischung und Verfremdung (z.B. zerberus wird zu z\$rb\$ŕ§s oder z1rb2r3s) oder die Memotechnik (Einmal ist keinmal! wird zu 1x=k1x!).
- Notieren oder speichern Sie keine Passwörter! Ausnahme: Systemverwalter- oder selten benutzte Passwörter. Hinterlegen Sie diese im versiegelten Umschlag an einem sicheren Ort.
- Geben Sie Passwörter grundsätzlich nicht an andere weiter! Soweit dies im Einzelfall unvermeidlich ist, ändern Sie anschließend Ihr Passwort.
- Ändern Sie Ihr Passwort in angemessenen Zeitabständen, wenn Ihr System Ihnen das nicht automatisch vorgibt. Ändern Sie es nicht zu oft, aber ändern Sie es!
- Wenn Sie mit mehreren Passwörtern arbeiten (müssen) versuchen Sie, diese zu synchronisieren. Ein Passwort im Kopf ist günstiger als drei auf Papier.

Für den Systemverwalter:

- Versehen Sie jede Benutzerkennung mit einem Passwort!
- Begrenzen Sie die Gültigkeitsdauer von Passwörtern; der Zeitraum sollte Abwesenheiten (Urlaub, Krankheit) abdecken, 90 Tage jedoch nicht überschreiten.
- Passwörter sollten verschlüsselt abgelegt werden, und der Zugriff soweit wie möglich beschränkt sein.
- Nutzen Sie systemseitige Möglichkeiten, die Gestaltung von Passwörtern zu beeinflussen (Nr. 1, 2). Soweit möglich, setzen Sie Stoplisten ein, um Trivialpasswörter zu verhindern.
- Begrenzen Sie die Zahl erfolgloser Anmeldeversuche und sperren Sie die Benutzerkennung nach Erreichen der zulässigen Anzahl.
- Richten Sie das System so ein, dass die Benutzer ihr Passwort selbständig ändern können. Von Ihnen sollte lediglich ein Anfangspasswort vergeben werden, das nur für die erstmalige Anmeldung gilt, und anschließend geändert werden muss.

Sicherheitsstufen nach DIN 32 757 zum Vernichten vertraulicher und personenbezogener Medien (Schriftstücke, Pläne, Dokumente, Akten)

<p>Sicherheitsstufe 1: Allgemeines Schriftgut, z.B. Altbestände. Streifenbreite max. 12 mm.</p> <p>Sicherheitsstufe 2: Interne Unterlagen wie EDV-Listen und Fehlkopien. Streifenbreite max. 6 mm.</p>	<p>Sicherheitsstufe 3: Vertrauliche oder personenbezogene Dokumente. Streifenbreite max. 2 mm (DIN A 4 lang) oder Partikelgröße max. 4 x 80 mm.</p> <p>Sicherheitsstufe 4: Existentiell wichtige Unternehmensinformationen. Partikelgröße max. 2 x 15 mm.</p> <p>Sicherheitsstufe 5: Geheim-klassifizierte Dokumente. Partikelgröße max. 0,8 x 13 mm.</p>
--	--

Die Schutzstufen werden wie folgt unterschieden:

Stufe 1: frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, zum Beispiel Adressbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken,

Stufe 2: personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, zum Beispiel beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen,

Stufe 3: personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Ansehen), zum Beispiel Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.

Stufe 4: personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann (Existenz), zum Beispiel Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Konkurse,

Stufe 5: Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, zum Beispiel Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

Falls die Sensibilität nicht bekannt ist, ist von der höchsten Sensibilitätsstufe auszugehen. Denkbar ist auch, dass der Schutz empfindlicher Firmendaten ohne Personenbezug die Einstufung bestimmt.

**Dienstanweisung
über den automatisierten Abruf von Meldedaten
innerhalb der Stadtverwaltung Trier**

Aufgrund des § 31 Abs. 6 des Meldegesetzes (MG) in Verbindung mit § 7 des Landesdatenschutzgesetzes (LDSG) wird bestimmt:

1. Allgemeines

- 1.1. Die fachlich zuständigen Stellen innerhalb der Stadtverwaltung sind befugt, Meldedaten im Rahmen eines automatisierten Abrufverfahrens nach Maßgabe dieser Dienstanweisung aus dem Melderegister abzurufen. Darüber hinausgehende Regelungen durch Bundes- oder Landesrecht bleiben unberührt.
- 1.2. Nach § 7 Abs. 1 Satz 1 i.V.m. Absatz 5 Satz 2 LDSG ist die Einrichtung eines automatisierten Verfahrens, das den Abruf personenbezogener Daten für einen anderen Zweck ermöglicht als den, für den sie gespeichert worden sind, zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Belange der Betroffenen, des Schutzes besonderer Berufs- oder Amtsgeheimnisse und der Aufgaben der beteiligten Stellen angemessen ist. Nach § 7 Abs. 5 Satz 2 LDSG bedarf die Einrichtung eines automatisierten Abrufverfahrens innerhalb einer öffentlichen Stelle der Zulassung durch die Leitung der öffentlichen Stelle.
- 1.3. Um die Zulässigkeit eines automatisierten Abrufverfahrens kontrollieren zu können, sind nach § 7 Abs. 2 Satz 2 LDSG der Anlass und der Zweck des Abrufverfahrens sowie die empfangenden Stellen, die Art der zu übermittelnden Daten und die nach § 9 LDSG erforderlichen technischen und organisatorischen Maßnahmen festzulegen.
- 1.4. Die Verantwortung für die Zulässigkeit des Abrufs von Daten aus dem Melderegister trägt diejenige Stelle, die den Abruf veranlasst. Um die Rechtmäßigkeit des Zugriffs auf Meldedaten zumindest stichprobenweise überprüfen zu können, sind nach § 7 Abs. 4 Satz 3 LDSG entsprechende Vorkehrungen zu treffen.
- 1.5. Vor der Einrichtung eines automatisierten Abrufverfahrens sowie im Falle einer Änderung ist der behördliche Datenschutzbeauftragte zu beteiligen und gemäß § 7 Abs. 3 Satz 1 LDSG der Landesbeauftragte für den Datenschutz zu hören.

2. Sicherungsmaßnahmen

- 2.1. Werden Daten zum Zwecke des automatisierten Abrufs für einzelne fachlich zuständige Stellen innerhalb der Stadtverwaltung bereitgehalten, darf ein Abruf nur vorgenommen werden, wenn die Kenntnis der Daten im Einzelfall für die Erfüllung der in der Zuständigkeit der abrufenden Stelle liegenden Aufgaben erforderlich ist.
- 2.2. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass Daten aus dem Melderegister nur durch hierzu berechnigte Bedienstete abgerufen werden können und der Zugriff auf die in den nachfolgenden Vorschriften für den Abruf zugelassenen Daten beschränkt ist. Der Abruf kann auch im Wege einer automatisierten Abfrage aus einem Fachverfahren heraus erfolgen, wenn hierbei die Einhaltung der Nummer 2 gewährleistet ist.
- 2.3. Für Abfragen aus dem Melderegister nach einzelnen natürlichen Personen dürfen nur Vor- und Familiennamen, frühere Namen, Geschlecht, Tag und Ort der Geburt sowie gegenwärtige und frühere Anschrift der betroffenen Person verwendet werden. Zur näheren Bezeichnung einer Person dürfen bei der Abfrage bis zu drei Buchstaben des Vor- und Familiennamens sowie früherer Namen durch Platzhalter ersetzt werden. Werden aufgrund einer Abfrage die Datensätze von mehreren Personen angezeigt, so darf die abrufberechnigte Stelle diese Daten nur in dem Umfang verarbeiten, wie dies zur Erfüllung der ihr durch Rechtsvorschrift übertragenen Aufgaben erforderlich ist.
- 2.4. In den Fällen des § 34 Abs. 8 und 9 des Meldegesetzes (MG) ist der abrufberechtigten Stelle nur die Tatsache des Vorliegens einer Auskunftssperre mitzuteilen. Unberührt hiervon bleibt die Übersendung von Listen und vergleichbaren Übersichten über Personengruppen (bspw. Steuerpflichtige,

Gebührenpflichtige bei der Abfallentsorgung) an die fachlich zuständige Stelle, in denen diejenigen Personen, für die eine Auskunftssperre nach § 34 Abs. 8 und 9 MG eingetragen ist, enthalten sind. Soweit Daten aus dem Melderegister, für die eine Auskunftssperre eingetragen ist, von den fachlich zuständigen Stellen an Dritte weitergegeben werden sollen, hat eine Abstimmung mit der Meldebehörde zu erfolgen, inwieweit hierdurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden können.

- 2.5. Die Abfrage von Daten über eine Vielzahl namentlich nicht näher bezeichneter Personen (Gruppenabfrage) ist nur in den in dieser Dienstanweisung zugelassenen Fällen zulässig. Für die Zusammensetzung der Gruppe dürfen nur die in § 31 Abs. 1 Satz 1 MG genannten Daten zugrunde gelegt werden.
- 2.6. Jeder Abruf ist zu protokollieren. Bei Abfragen nach einzelnen natürlichen Personen sind die abrufberechtigte Stelle, die Art der Abfrage, der Zeitpunkt der Abfrage sowie der Name der abgefragten Person zu protokollieren. Bei Gruppenabfragen sind die abrufberechtigte Stelle, die Kennung der abfragenden Person oder Personengruppe, der Anlass der Abfrage, die Abfragekriterien, die Art der Abfrage, der Zeitpunkt der Abfrage und die Anzahl der Treffer zu protokollieren. Ist das Ergebnis einer Gruppenabfrage Grundlage für die Abfrage von einzelnen natürlichen Personen, gilt Satz 2 entsprechend.
- 2.7. Die Protokolldaten dürfen grundsätzlich nur für Zwecke der Datenschutzkontrolle ausgewertet werden. Eine darüber hinaus gehende Nutzung ist ausnahmsweise zulässig, wenn dies im Einzelfall zur Sicherstellung des Betriebs des Verfahrens erforderlich ist.
- 2.8. Für Zwecke einer Verhaltens- und Leistungskontrolle von Bediensteten der abfrageberechtigten Stellen dürfen die Protokolldaten nicht ausgewertet werden. Die Befugnis, Protokolldaten nach vorheriger Unterrichtung des behördlichen Datenschutzbeauftragten und des Landesbeauftragten für den Datenschutz zur Überprüfung des Verdachts eines Datenschutzverstoßes oder zur Verfolgung einer Straftat auszuwerten, bleibt unberührt.
- 2.9. Die Protokolldaten sind mindestens zwölf Monate aufzubewahren und spätestens bis zum Ende des auf die erstmalige Speicherung folgenden Kalenderjahres zu löschen.

3. Abruf von Meldedaten zur Veranlagung von Abfallentsorgungsgebühren

Die Abfallentsorgung wird im Gebiet der Stadt Trier durch den Zweckverband Abfallbeseitigung im Raum Trier ausgeführt. Ein Abruf von Meldedaten über das stadtinterne Verfahren entfällt.

4. Abruf von Meldedaten zur Erfüllung von Aufgaben aufgrund des Gesetzes über Ordnungswidrigkeiten sowie des Gesetzes über das Fahrlehrerwesen und des Straßenverkehrsgesetzes einschließlich der auf deren Grundlage erlassenen Rechtsverordnungen

Zur Erfüllung der Aufgaben aufgrund des Gesetzes über Ordnungswidrigkeiten sowie des Gesetzes über das Fahrlehrerwesen und des Straßenverkehrsgesetzes einschließlich der auf deren Grundlage erlassenen Rechtsverordnungen dürfen für die zuständigen Stellen folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Staatsangehörigkeiten.

5. Abruf von Meldedaten zur Wahrnehmung von Aufgaben des Sozialamtes

Für das Sozialamt dürfen zur Erfüllung der ihm durch Rechtsvorschriften übertragenen Aufgaben folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Familienstand,
11. Ehegattin oder Ehegatte,
12. minderjährige Kinder,
13. Staatsangehörigkeiten.

6. Abruf von Meldedaten zur Wahrnehmung von Aufgaben der Kinder- und Jugendhilfe

Zur Erfüllung von durch Rechtsvorschriften übertragenen Aufgaben der Kinder und Jugendhilfe dürfen für die zuständigen Stellen folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Familienstand,
11. Ehegattin oder Ehegatte,
12. minderjährige Kinder,
13. Staatsangehörigkeiten.

7. Abruf von Meldedaten durch die Stadtkasse

Zur Feststellung einer Person und deren Anschrift dürfen für die zuständige Stadtkasse folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Staatsangehörigkeiten,
11. Hinweis auf weitere Informationen zum Verbleib bei der Meldebehörde.

8. Abruf von Meldedaten für Zwecke der Energie- und Wasserversorgung

Aufgaben der Energie- und Wasserversorgung im Gebiet der Stadt Trier nimmt die Anstalt des öffentlichen Rechts SWT-AÖR wahr. Ein Abruf von Meldedaten über das stadtinterne Verfahren entfällt.

9. Abruf von Meldedaten zur Durchführung von Besteuerungs-, Gebühren- und Beitragsverfahren sowie zur Geltendmachung von sonstigen Geldforderungen

Zur Feststellung einer Person und deren Anschrift im Rahmen eines Besteuerungs- sowie eines Gebühren- und Beitragserhebungsverfahrens dürfen für die zuständige Stelle folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Staatsangehörigkeiten.

10. Abruf von Meldedaten durch die Ausländerbehörde

Zur Erfüllung der Aufgaben der Ausländerbehörde dürfen die in der Aufenthaltsverordnung vom 25. November 2004 (BGBl. I S. 2945) genannten Daten sowie der Hinweis auf weitere Informationen zum Verbleib der betroffenen Person bei der Meldebehörde auch für Gruppenabfragen zum Abruf bereitgehalten werden.

11. Abruf von Meldedaten zur Wahrnehmung der Aufgaben des gemeindlichen Liegenschafts- und Vermessungswesens

Zur Führung des gemeindlichen Liegenschaftskatasters und zur Wahrnehmung der weiteren Aufgaben des gemeindlichen Liegenschafts- und Vermessungswesens dürfen folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht).

12. Abruf von Meldedaten für Zwecke des Staatsangehörigkeits- und Personenstandswesens

Zur Erfüllung der durch Rechtsvorschriften übertragenen Aufgaben der für Staatsangehörigkeits- und Personenstandsangelegenheiten zuständigen Stellen dürfen folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,

5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt sowie Hinweise zum Geburtseintrag und Aktenzeichen,
8. Sterbetag und -ort sowie Hinweise zum Sterbeeintrag und Aktenzeichen,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Familienstand sowie Hinweise zum Datum der Eheschließung und der Ehebeendigung, der Begründung und der Beendigung einer Lebenspartnerschaft sowie zum Aktenzeichen,
11. Ehegattin oder Ehegatte,
12. minderjährige Kinder,
13. Staatsangehörigkeiten,
14. Daten nach § 3 Abs. 2 Nr. 4 MG,
15. Daten nach § 3 Abs. 2 Nr. 10 MG.

13. Abruf von Meldedaten zur Wahrnehmung der Aufgaben der Ordnungsbehörde und zur Durchführung des Waffengesetzes

Zur Erfüllung der durch Rechtsvorschriften übertragenen Aufgaben dürfen für die Ordnungsbehörde folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Familienstand,
11. Ehegattin oder Ehegatte,
12. minderjährige Kinder,
13. Staatsangehörigkeiten,
14. Daten nach § 3 Abs. 2 Nr. 6 MG,

14. Abruf von Meldedaten zur Wahrnehmung von Rechtsangelegenheiten

Zur Erfüllung von Aufgaben im Zusammenhang mit der Geltendmachung von Rechtsansprüchen, der Erstattung von Strafanzeigen sowie der Erledigung von sonstigen Rechtsangelegenheiten dürfen für die zuständige Stelle folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Familienstand,
11. Staatsangehörigkeiten,

15. Abruf von Meldedaten zur Erledigung von Angelegenheiten der Schulverwaltung

Zur Erfüllung von durch Rechtsvorschriften übertragenen Aufgaben der Schulverwaltung dürfen für die insoweit zuständigen Stellen folgende Daten auch für Gruppenabfragen zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht),
10. Familienstand,
11. Ehegattin oder Ehegatte,
12. minderjährige Kinder,
13. Staatsangehörigkeiten,

16. Abruf von Meldedaten für Zwecke der Ausgleichsverwaltung

Für die durch Rechtsvorschriften übertragenen Aufgaben der Ausgleichsverwaltung dürfen folgende Daten zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Geschlecht,
4. Doktorgrad,
5. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung,
6. Tag des Ein- und Auszugs,
7. Tag und Ort der Geburt,
8. Sterbetag und -ort,
9. gesetzliche Vertreterin und gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht).

17. Abruf von Meldedaten zur Erfüllung allgemeiner Verwaltungsangelegenheiten

Zur Erfüllung von allgemeinen Verwaltungsangelegenheiten dürfen für die zuständige Stelle folgende Daten zum Abruf bereitgehalten werden:

1. Vor- und Familiennamen,
2. frühere Namen,
3. Doktorgrad,
4. gegenwärtige und frühere Anschriften,
5. Tag der Geburt,
6. Sterbetag.

18. In-Kraft-treten

Diese Dienstanweisung tritt am 15.04.2013 in Kraft.

Trier, den 08.04.2013

Klaus Jensen
Oberbürgermeister