Der Bürgermeister

Hattingen, 26.08.2025

Dienstanweisung 5/2024

zum Datenschutz für die Stadt Hattingen

in der Fassung vom 26.08.2025

Inhalt

Anlage 2:	Informationspflichten
Anlage 3:	Prozess der Risikoanalyse im Zusammenhang mit Datenschutzverstößen
Anlage 4:	Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) – *gilt auch für Übernahme in der Online-Meldung an die Aufsichtsbehörde des Bundes* -
Anlage 5:	Checkliste für die Auftragsdatenverarbeitung
Anlage 6:	Verzeichnis von Verarbeitungstätigkeiten für „Verantwortliche“ (nach LDI)
Anlage 6a:	Verzeichnis von Verarbeitungstätigkeiten für „Auftragsverarbeitende“ (nach LDI)
Anlage 6b:	Hinweise zum Verzeichnis von Verarbeitungstätigkeiten der Datenschutzkonferenz (DSK) zu den Anlagen 6 und 6a
Anlage 7:	Erläuterungen zur Datenschutz-Folgeabschätzung (§ 18)
Anlage 8:	Checkliste zur Datenschutzfolgeabschätzung
Anlage 9:	Liste von Verarbeitungsvorgängen zur verbindlichen Datenschutzfolgeabschätzung (Positivliste) des LDI

I. Allgemeines

§ 1 Rechtliche Grundlagen

Grundlagen dieser DA sind:

- die Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46 EG (Datenschutzgrundverordnung-DSVGO),

- ergänzende allgemeine sowie bereichsspezifische Datenschutzvorschriften des Bundes und des Landes Nordrhein-Westfalen,

- das Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz Nordrhein-Westfalen – IFG NRW),

- das Umweltinformationsgesetz Nordrhein-Westfalen (UIG NRW) und das Umweltinformationsgesetz (des Bundes) und

- das Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (Verbraucherinformationsgesetz – VIG)

in den jeweils geltenden Fassungen.

§ 2 Zweck

(1) Die DA dient dem Zweck, die rechtmäßige Verarbeitung personenbezogener Daten einschließlich der Datensicherheit durch die Stadt Hattingen zu gewährleisten. Damit soll das Recht aller Personen gewahrt werden, im Rahmen des geltenden Rechts selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen (Informationelles Selbstbestimmungsrecht).

(2) Es werden auch Festlegungen für die Gewährung von Akteneinsicht, Amtshilfe und Auskunftserteilung getroffen, soweit personenbezogene Daten betroffen sind sowie notwendige Maßnahmen zum Schutz von Informanten. Ebenso wird die Gewährung des Zuganges zu amtlichen Informationen konkretisiert, soweit personenbezogene Daten, Betriebs-und Geschäftsgeheimnisse oder Urheberrechte betroffen sind.

§ 3 Geltungsbereich

Die DA gilt für alle städtischen Organisationseinheiten der Stadt Hattingen, die personenbezogene Daten selbst oder durch die Einschaltung Dritter verarbeiten.

§ 4 Begriffsbestimmungen

Für die in der DA verwendeten Begriffe gelten die Definitionen, die in der DSGVO und den sie ergänzenden deutschen Rechtsvorschriften verankert sind. Wesentliche Definitionen sind in der Anlage 1 aufgeführt.

II. Zuständigkeiten und Verantwortlichkeiten

§ 5 Grundsatz

(1) Alle Beschäftigen sind für die Einhaltung der jeweils anzuwendenden Vorschriften über den Datenschutz zuständig und verantwortlich, soweit sie personenbezogene Daten verarbeiten, insbesondere wenn sie

- personenbezogene Daten erheben,
- Akten bzw. Dateien, die personenbezogene Daten enthalten, anlegen, verwalten, führen, nutzen oder vernichten bzw. löschen,
- Akten und Vorgänge versenden,
- Auskünfte erteilen und Einsicht gewähren.

(2) Zur Erfüllung ihrer Aufgaben können die Beschäftigten jederzeit die Beratung und Unterstützung des für die technische Datenverarbeitung zuständigen Fachbereiches (FB 11 Personal, Organisation, Datenverarbeitung) und der*des Datenschutzbeauftragten in Anspruch nehmen.

§ 6 Verantwortliche und Verantwortlichkeiten

(1) Die Stadt Hattingen wird als Körperschaft des Öffentlichen Rechts nach außen hin durch den*die Bürgermeister*in (Behörde) vertreten.

(2) Für die Einhaltung und Umsetzung der rechtlichen, technischen und organisatorischen Vorschriften zum Datenschutz sind die Leitungen der Organisationseinheiten (§ 3) im Innenverhältnis zuständig und verantwortlich. In der Verantwortung der Organisationseinheiten liegen unter anderem folgende Aufgaben:

- Erstellung, Aktualisierung und Bereitstellung der Informationen (Art. 12 – 14 DSGVO)
- die Meldung geplanter Auftragsdatenverarbeitungen (§ 16 DSGVO)
- Erstellung des Verzeichnisses vorgenommener Verarbeitungstätigkeiten in der Organisationseinheit und Übergabe bzw. Weiterleitung an den*die Datenschutzbeauftragte*n (§ 17 DSGVO)
- Koordination und Durchführung der Datenschutz-Folgenabschätzungen (§ 18 DSGVO)
- Erarbeitung von organisationsinternen Regelungen zum Datenschutz unter Beteiligung des*der behördlichen Datenschutzbeauftragten
- Unterstützung und rechtzeitige Information des*der Datenschutzbeauftragten in allen Datenschutzbelangen

- Stellungnahmen zu Anfragen des*der Datenschutzbeauftragten und Mitwirkung bei Bürgeranfragen, sofern sie nicht unmittelbar an die Organisationseinheit direkt gestellt wurden

- Entscheidung über die Zulässigkeit von Datenübermittlungen an Dritte innerhalb und außerhalb der Stadt Hattingen

- Meldungen von Datenschutzverstößen an die*den behördliche*n Datenschutzbeauftragte*n sowie gegebenenfalls Benachrichtigung von Betroffenen gem. Art. 34 DSGVO nach Durchführung einer entsprechenden Risikobewertung (vgl. § 15).

(3) Die Leitungen der Organisationseinheiten nehmen an Fortbildungen teil und wirken innerhalb der eigenen Organisationseinheit als Multiplikator. Diese Aufgaben können auf geeignete Beschäftigte innerhalb der Organisationseinheiten delegiert werden. Delegationen sind schriftlich zu dokumentieren.

§ 7 Zentrale Datenschutzfunktion (behördliche*r Datenschutzbeauftragte*r)

(1) Der*die Bürgermeister*in bestellt den*die Datenschutzbeauftragte*n und ggfs. eine Vertretung. In ihrer Funktion sind sie dem*der Bürgermeister*in unmittelbar unterstellt und in der Aufgabenwahrnehmung weisungsfrei.

(2) Im Rahmen der zentralen Datenschutzfunktion ist ihm*ihr das ungehinderte Vorspracherecht bei dem*der Bürgermeister*in eingeräumt.

(3) Der*Die Datenschutzbeauftragte ist zuständig für die Beantwortung aller Fragen, die den Datenschutz betreffen. Er*Sie übernimmt die in den Art. 38 und 39 DSGVO genannten Mindestaufgaben und Befugnisse. Beispielhaft sind zu nennen:

- Unterrichtung und Beratung des Verwaltungsvorstandes in Grundsatzfragen zum Datenschutz,

- Unterrichtung, Beratung und Unterstützung der in § 3 genannten Stellen in allen Fragen des Datenschutzes,

- unmittelbare Ansprechperson aller Beschäftigten der Stadt Hattingen in Angelegenheiten des Beschäftigtendatenschutzes,

- unmittelbare Ansprechperson der Bürgerinnen und Bürger der Stadt Hattingen in Fragen des Datenschutzes,

- Zusammenarbeit mit den zuständigen Aufsichtsbehörden für Datenschutz und Informationsfreiheit,

- Mitwirkung bei Projekten mit datenschutzrelevanten Komponenten, insbesondere bei der Erarbeitung verwaltungsinterner Regelungen, Satzungen und Formulare, mit denen personenbezogene Daten verarbeitet werden sowie bei Verträgen mit Externen,

- Überwachung der Organisationseinheiten (§ 3) im Hinblick auf die Einhaltung der Vorgaben zum Datenschutz (Stichproben und anlassbezogene Überprüfung),

- Teilnahme an internen Arbeitskreisen und Vertretung der Stadt Hattingen in externen Arbeitskreisen und Gremien mit datenschutzrechtlichem Bezug.

Darüber hinaus können ihm*ihr Prüfaufträge und weitere Aufgaben übertragen werden, soweit die Erfüllung der gesetzlich übertragenen Aufgaben dadurch nicht beeinträchtigt wird bzw. dieser entgegenstehen.

(4) Der*Die Datenschutzbeauftragte ist bei allen Anlässen, soweit sie die Verarbeitung personenbezogener Daten betreffen, von der zuständigen Organisationseinheit

- unaufgefordert,
- umfassend und
- frühestmöglich in einer Vorlaufzeit von mindestens 14 Tagen

zu informieren und schriftlich einzubinden.

Insbesondere sind dem*der Datenschutzbeauftragten in datenschutzrechtlichen Belangen alle Planungen, Beschaffungen und Beschaffungsvorbereitungen einschließlich der Erstellung von Vergabeunterlagen, Vertragsentwürfen und Aufträgen an Externe vor Begründung von Rechtspflichten für die Stadt Hattingen vorzulegen.

(5) Dem*Der Datenschutzbeauftragten ist zur Durchführung seiner*ihrer Aufgaben Einsicht und Zugang in alle Räume, Akten und Dateien zu gewähren.

(6) Stellt der*die Datenschutzbeauftragte Verstöße gegen Vorgaben zum Datenschutz fest, kann er*sie diese beanstanden und die betroffene Organisationseinheit zu einer Stellungnahme auffordern. Mit der Beanstandung können Empfehlungen zur Beseitigung der Mängel und zur Verbesserung des Datenschutzes verbunden werden. Bei Verstößen gegen den Beschäftigtendatenschutz kann der*die Datenschutzbeauftragte darüber hinaus die Personalvertretung informieren.

§ 8 Korrespondenz mit dem*der Datenschutzbeauftragten und Beratung

(1) Beratungsanfragen sind grundsätzlich schriftlich an den*die Datenschutzbeauftragte*n zu richten oder mit ihm*ihr vorab entsprechende Beratungstermine zu vereinbaren.

(2) Für den elektronischen Kommunikationsweg ist die Adresse datenschutz@hattingen.de als zentrale Funktionsmailadresse für die interne und externe Nutzung eingerichtet.

(3) An den*die Datenschutzbeauftragte*n adressierte Brief-und Postsendungen sind an ihn*sie ungeöffnet weiterzuleiten.

§ 9 Ziele in der Datenverarbeitung

Die Ziele der DSGVO, namentlich der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO) sowie der Schutz des freien Verkehrs personenbezogener Daten (Art. 1 Abs. 3 DSGVO), sollen durch die festgelegten Grundsätze zur Datenverarbeitung (Art. 5 DSGVO) erreicht werden, namentlich der Grundsatz der

- Rechtmäßigkeit (Art. 6)
- Transparenz (Art. 5, 12-15)

- Zweckbindung (Art. 5)
- Datenminimierung (Art. 5)
- Richtigkeit (Art. 5, 16)
- Speicherbegrenzung (Art. 5)
- Integrität (Art. 5)
- Vertraulichkeit (Art. 5)
- Rechenschaftspflicht (Art. 5)
- Authentizität und Verfügbarkeit von Daten

III. Umgang mit personenbezogenen Daten

§ 10 Datenverarbeitung (Begriff und Zulässigkeit)

(1) Datenverarbeitung umfasst gem. Art. 4 Nr. 2 DSGVO u.a.

das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

personenbezogener Daten.

Die Datenverarbeitung in teilautomatisierten Verfahren oder in Schriftgut (Papierform) ist Datenverarbeitung gem. Art. 4 Nr. 2 DSGVO.

(2) Die Datenverarbeitung ist gem. Art. 6 Abs. 1 DSGVO nur dann rechtmäßig, wenn

- eine Rechtsvorschrift sie erlaubt,
- die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat,
- die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen,
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, die der Verantwortliche unterliegt
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen,
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die den Verantwortlichen übertragen wurde,

- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder Dritter erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dies gilt nicht für Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(3) Die Verarbeitung personenbezogener Daten unterliegt der Zweckbindung (Art. 5 Abs. 1 DSGVO). Es dürfen nur die Daten verarbeitet werden, die für die Erfüllung der jeweiligen Aufgaben erforderlich sind. Sie dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden. Ausnahmen bedürfen einer gesetzlichen Grundlage oder der Einwilligung von Betroffenen.

(4) Unzulässig sind die Erhebung und Speicherung von Daten „auf Vorrat" (Vorratsdatenspeicherung).

§ 11 Datenübermittlung an Dritte

Vor einer Übermittlung personenbezogener Daten an Dritte ist die Rechtmäßigkeit zu prüfen. Sofern keine spezialgesetzlichen Regelungen vorliegen, sind hierbei die diesbezüglichen Regelungen des Datenschutzgesetzes NRW (DSG NRW) und der DSGVO maßgebend.

§ 12 Datenübermittlung (Datenweitergabe) innerhalb der Stadtverwaltung

Für die Übermittlung von personenbezogenen Daten innerhalb der Verwaltung der Stadt Hattingen gelten die übermittlungsrechtlichen Vorschriften gleichermaßen. Automatisierte Abrufverfahren dürfen nur eingerichtet werden, wenn dies spezialgesetzlich erlaubt ist oder die Voraussetzungen nach den Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen in der jeweils geltenden Fassung erfüllt sind.

§ 13 Rechte von Betroffenen

(1) Betroffenen ist auf Antrag eine Bestätigung darüber zu erteilen, ob sie betreffende personenbezogene Daten bei der Stadt Hattingen (grundsätzlich als Gesamtverwaltung) verarbeitet werden. Es besteht grundsätzlich verwaltungsübergreifend das gesetzliche Recht auf Auskunft, u.a.

- über die zu ihrer Person gespeicherten Daten
- den Zweck der Verarbeitung der Daten,
- die Herkunft dieser Daten,
- die Empfänger in der Übermittlung ihrer Daten seitens der Stadt Hattingen sowie
- die geplante Dauer der Speicherung ihrer Daten (Art. 15 Abs. 1 DSGVO).

Die Betroffenen sind auf ihr Beschwerderecht bei der zuständigen Aufsichtsbehörde hinzuweisen.

(2) Auskunftsersuchen sind unmittelbar dem*der Datenschutzbeauftragten zuzuleiten.

(3) Vor Erteilung der Auskunft sind, wie bei der Gewährung von Akteneinsicht, die schutzwürdigen Interessen anderer Personen zu berücksichtigen (z. B. Informantenschutz) und die Auskunft gegebenenfalls einzuschränken oder zu versagen; im Zweifel ist die*der Datenschutzbeauftragte zu beteiligen.

(4) Auskünfte an Betroffene erteilt grundsätzlich die zuständige Organisationseinheit, sofern sich der Antrag lediglich auf deren Aufgabenbereich bezieht. Erteilte Auskünfte sind dem*der Datenschutzbeauftragten zur Kenntnis zu geben.

Auskünfte, die mehrere Organisationseinheiten betreffen, koordiniert der*die Datenschutzbeauftragte.

(5) Personenbezogene Daten sind nach Art. 16 DSGVO zu berichtigen, wenn sie unrichtig sind.

(6) Nach Art. 17 DSGVO sind personenbezogene Daten unverzüglich zu löschen, wenn diese für die Zwecke, für die sie erhoben worden sind,

- nicht mehr erforderlich sind,
- die betreffende Person ihre Einwilligung widerrufen hat (nur für die Zukunft wirkend),
- Widerspruch gegen die Verarbeitung eingelegt wurde,
- eine unrechtmäßige Datenverarbeitung vorliegt oder
- wenn die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Die Löschung personenbezogener Daten für die Stadt Hattingen ist in den einzelnen und fachspezifischen Aufbewahrungsfristen konkret festzulegen, zu dokumentieren und im Bedarfsfall durch die Verantwortlichen anzupassen. Als Orientierungsgrundlage dienen die Aufbewahrungsfristen für Kommunalverwaltungen der Kommunalen Gemeinschaftsstelle (KGST); letzter Stand: Bericht Nr. 4/2006, darin insbesondere Anlage. 1.

Gesetzliche oder auf anderen Rechtsvorschriften beruhende Aufbewahrungsfristen stehen einer Löschung nach den Fristen der KGST entgegen.

Allgemeine und pauschalierte Hinweise auf bestehende Aufbewahrungsfristen sind unzulässig.

§ 14 Informationspflichten

(1) Für natürliche Personen soll Transparenz (Art. 12 DSGVO) dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, weitergegeben oder anderweitig verarbeitet worden sind und in welchem Umfang diese personenbezogenen Daten jetzt oder künftig verarbeitet werden.

(2) Die Stadt Hattingen ist schon im Vorfeld der personenbezogenen Datenverarbeitung – also vor der Datenerhebung – verpflichtet, betroffenen Personen alle Informationen zur Verfügung zu stellen, die Art, Zweck und Umfang der Verarbeitungstätigkeit beschreiben. Es wird unterschieden, ob die Daten direkt bei Betroffenen (Art. 13 DSGVO) oder bei Dritten (Art. 14

DSGVO) erhoben werden. Die Art. 13 und 14 DSGVO enthalten jeweils einen Katalog an Informationspflichten. Die Aufzählungen sind abschließend. Spezialgesetzliche Beschränkungen der Informationspflichten sind zu beachten.

(3) Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und in allgemein verständlicher Sprache abgefasst sind.

Die Informationspflichten für die Stadt Hattingen werden deshalb – allgemein zugänglich – auf deren Internetseite veröffentlicht; das einheitliche Formular dafür wird im Intranet bereitgestellt (Anlage 2).

Daneben kann Betroffenen eine schriftliche Abfassung ausgehändigt werden.

(4) Die veröffentlichten Informationspflichten sind von den Verantwortlichen bei eintretenden Änderungen umgehend anzupassen; darüber hinaus regelmäßig (mindestens einmal jährlich) auf deren aktuellen Inhalt zu überprüfen.

§ 15 Verletzung des Schutzes personenbezogener Daten (Datenschutzpannen/Datenschutzverstöße)

(1) Verletzungen des Schutzes personenbezogener Daten (Datenschutzverstöße) im Sinne der DSGVO sind – auch unbeabsichtigt – deren Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder deren Abgriff.

(2) Kommt es zum Datenschutzverstoß bei personenbezogenen Daten, besteht eine Meldepflicht nach Maßgabe der Art. 33 und 34 DSGVO.

(3) Im Falle einer Verletzung des Schutzes personenbezogener Daten ist diese unverzüglich und möglichst binnen 72 Stunden nach dem Bekanntwerden formell der zuständigen Aufsichtsbehörde zu melden, es sei denn, dass der Datenschutzverstoß voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 DSGVO).

(4) Für einen vorliegenden Datenschutzverstoß ist deshalb zunächst die Risikostufe auf der Grundlage einer Risikoanalyse zu ermitteln. Dabei ist neben der Eintrittswahrscheinlichkeit des Schadens auch seine Schwere zu beurteilen. Aus der Eintrittswahrscheinlichkeit und der Schwere der möglichen Schäden ergibt sich die Risikostufe. Die Risikostufe entscheidet dann darüber, ob eine Meldung an die Aufsichtsbehörde erforderlich ist. Eine vollständig risikolose Datenverarbeitung kann es nicht geben. Insofern ist die in Art. 33 DSGVO gewählte Formulierung „nicht zu einem Risiko" von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko führend" zu verstehen. Damit ergeben sich für die Risikobeurteilung die Abstufungen „geringes Risiko", „Risiko" und „hohes Risiko". Kommt der*die Verantwortliche in seiner*ihrer Risikoanalyse zu dem Ergebnis, dass nur ein geringes Risiko vorliegt, ist keine Meldung an die Aufsichtsbehörde erforderlich.

(5) Der Prozess der Risikoanalyse ist für die Stadt Hattingen im Einzelnen in der Anlage 3 (Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen" der DSK) beschrieben und festgelegt.

Die formgebundene Meldung (Anlage 4) wird über den*die Datenschutzbeauftragte*n für die Verantwortlichen im Intranet bereitgestellt.

(6) Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, wenn ihnen

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzielle Verluste,
- unbefugte Aufhebung der Pseudonymisierung,
- Rufschädigung,
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder
- andere erhebliche, gesundheitliche, wirtschaftliche oder gesellschaftliche Nachteile drohen.

(7) Sofern das Risiko für betroffene Personen hoch ist, ist neben der Meldepflicht an die Aufsichtsbehörde außerdem der*die Betroffene unverzüglich zu benachrichtigen (Art. 34 DSGVO).

Ein hohes Risiko kann zum Beispiel beim Bekanntwerden einer mittels melderechtlicher Auskunftssperre geschützten Wohn-oder Aufenthaltsanschrift entstehen; ebenso bei Verlust von Datenträgern mit personenbezogenen Daten.

(8) Über jeglichen Datenschutzverstoß ist unmittelbar der*die Datenschutzbeauftragte zu informieren; im Falle eines voraussichtlich drohenden Schadens von betroffenen Personen zeitgleich der*die Bürgermeister*in.

(9) Verstöße gegen diese Regelungen/DA können disziplinarische, arbeitsrechtliche sowie strafrechtliche Konsequenzen nach sich ziehen.

§ 16 Auftragsverarbeitungen

(1) Verarbeitet die Stadt Hattingen personenbezogene Daten nicht selbst, dürfen Aufträge zur externen Verarbeitung personenbezogener Daten nur erteilt werden, wenn die Auftragnehmenden Garantien dafür bieten, diese Daten nur im Einklang mit der DSGVO und den sie ergänzenden nationalen Bestimmungen zu verarbeiten. Der Vertrag bedarf der Schriftform; dies kann auch ein elektronisches Format sein. Notwendige Regelungen zur Einhaltung des Datenschutzes durch die Auftragnehmenden sind in die Verträge aufzunehmen.

(2) Die Auftragsverarbeitung ist nur nach vorheriger Beteiligung des*der Datenschutzbeauftragten unter Vorlage der Checkliste zur Auftragsverarbeitung (Anlage 5) zulässig.

§ 17 Verzeichnis der Verarbeitungstätigkeiten

(1) Sämtliche Tätigkeiten, mit denen personenbezogene Daten verarbeitet werden, sind von den Organisationseinheiten (§ 3) in ein Verzeichnis der Verarbeitungstätigkeiten aufzunehmen und an den*die Datenschutzbeauftragte*n zu übergeben bzw. weiterzuleiten. Auf Anfrage ist das Verzeichnis über den*die behördliche*n Datenschutzbeauftragte*n der zuständigen Aufsichtsbehörde zur Verfügung zu stellen.

(2) Ein Verzeichnis ist auch zu führen, wenn die Stadt Hattingen personenbezogene Daten für Dritte verarbeitet (Auftragsverarbeitung).

(3) Form und Inhalt des jeweiligen Verzeichnisses sowie Hinweise zum jeweiligen Verzeichnis werden durch den*die Datenschutzbeauftragte*n zur Verfügung gestellt (Anlage 6, 6a, 6b). Die Umsetzung wird von ihm*ihr überwacht.

§ 18 Datenschutz-Folgenabschätzungen

(1) Vor einer geplanten Verarbeitung personenbezogener Daten, die mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen behaftet sind, ist eine Datenschutz-Folgenabschätzung durch die Organisationseinheiten (§ 3) vorzunehmen.

(2) Im Rahmen der Datenschutz-Folgenabschätzung sind darin die Risiken für die Rechte und Freiheiten der Betroffenen einzuschätzen, die durch die Verarbeitung entstehen können. In der Durchführung einer Datenschutz-Folgenabschätzung hat die Organisationseinheit den*die Datenschutzbeauftragte*n beratend hinzuzuziehen.

Für die Durchführung steht eine Checkliste zur Datenschutz-Folgenabschätzung zur Verfügung (Anlage 8).

(3) In der „Positivliste" (Anlage 9) werden von den Aufsichtsbehörden Verarbeitungen aufgeführt, die immer und zwingend einer Datenschutz-Folgenabschätzung zu unterziehen sind.

(4) Die Entscheidung, dass eine Datenschutz-Folgenabschätzung nicht durchzuführen ist, ist zu dokumentieren.

(5) Näheres zum Inhalt und Ausgestaltung der Datenschutz-Folgenabschätzung ergeben sich aus der Checkliste (Abs. 2) und der Positivliste der Aufsichtsbehörde (Abs. 3).

§ 18a Besonderer Umgang mit Meldedaten

(1) Zugriff und Berechtigungen

- Der Zugriff auf das Meldedatenportal ist ausschließlich autorisierten Mitarbeitenden und zwecks dienstlicher Notwendigkeit gestattet.
- Die Zugriffsberechtigung wird von FB 30 erteilt und verwaltet. Personelle Veränderungen sind umgehend mitzuteilen.
- Der Zugriff auf Meldedaten wird protokolliert und turnusmäßig stichprobenartig auf Rechtmäßigkeit überprüft.

(2) Rechtsgrundlagen

Die Verarbeitung von Meldedaten erfolgt auf Grundlage der folgenden gesetzlichen Regelungen:

- Bundesmeldegesetz
- Meldesetz NRW
- Meldedatenübermittlungsverordnung
- Art. 5 und 6 DSGVO

(3) Unzulässige Nutzung

Der Abruf von Meldedaten ohne dienstlichen Grund ist ausdrücklich untersagt.
Darunter fällt insbesondere:

- die Einsichtnahme zu privaten Zwecken
- die Nutzung von Daten zur Vorbereitung oder Durchführung unzulässiger Datenabgleiche
- die Verwendung für kommerzielle Zwecke ohne gesetzliche Grundlage oder Einwilligung
- die Verarbeitung der Daten außerhalb der städtischen IT-Systeme

IV. Gewährung von Informationszugängen

§ 19 Rechtliche Grundlagen (Informationszugang)

(1) Das Umweltinformationsgesetz des Landes Nordrhein-Westfalen (UIG) gewährt in Verbindung mit dem Umweltinformationsgesetzes des Bundes weitgehend freien Zugang zu Umweltinformationen.

Das UIG und das VIG gehen als spezialgesetzliche Regelungen dem Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz Nordrhein-Westfalen – IFG NRW) vor, so dass das IFG NRW nachrangiges Recht darstellt.

(2) Das Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen (Informationsweiterverwendungsgesetz – IWG) gilt für die Weiterverwendung von vorhandenen Informationen bei öffentlichen Stellen, insbesondere zur Bereitstellung von Produkten und Dienstleistungen der digitalen Wirtschaft.

(3) Alle Informationszugangsregelungen berücksichtigen den Schutz personenbezogener Daten, von Betriebs-und Geschäftsgeheimnissen und des Urheberrechts in unterschiedlicher Ausprägung. Diese Schutzbestimmungen, die den jeweiligen Informationszugangsanspruch begrenzen, sind in jedem Einzelfall zu prüfen.

§ 20 Zuständigkeiten und Verfahren (IFG NRW)

(1) Zuständig sind die Organisationseinheiten (§ 3) in ihrer Eigenschaft als informationspflichtige Stellen im funktionalen Sinne.

(2) Der*die Datenschutzbeauftragte ist die zentrale Stelle für Anträge von Bürgerinnen und Bürgern nach den unter § 19 genannten Gesetzen.
Die Organisationseinheiten legen deshalb alle Anträge auf einen Informationszugang unmittelbar dem*der Datenschutzbeauftragten zur Prüfung vor, ob personenbezogene Daten, Betriebs-oder Geschäftsgeheimnisse oder Urheberrechte der Verwaltung sowie Dritter betroffen sind. Vorab fertigt die zuständige Organisationseinheit eine Stellungnahme, in der sie ihre Einschätzung bezüglich des Antrages auf Informationszugang abgibt. Die Stellungnahme ist dem*der Datenschutzbeauftragten zusammen mit dem Antrag vorzulegen. Der*die Datenschutzbeauftragte gibt den Rahmen des zu gewährenden Informationszuganges vor und fertigt den (Teil-)Ablehnungsbescheid samt Begründung. Er*sie stellt den Ablehnungsbescheid der zuständigen Organisationseinheit zur Verfügung.

(3) Die zuständige Organisationseinheit gewährt den Informationszugang bzw. erteilt die beantragten Auskünfte, erstellt und verschickt erforderliche Kopien oder Dateien. Bei der Bereitstellung von Dateien ist darauf zu achten, dass diese um die darin (ggfs. automatisiert) gespeicherten Meta-Informationen zur Wahrung des Beschäftigtendatenschutzes zu

bereinigen sind; hierzu sind die jeweiligen Datei-Eigenschaften aufzurufen und namentliche Bezüge in Abstimmung mit der für IT-Sicherheit zuständigen Stelle zu löschen. Soweit ein Informationszugang gewährt wird, bedarf es keines Bescheides, da ein Realakt vorliegt.

(4) Sind für den Informationszugang Gebühren und Auslagen nach einer Gebührenordnung zu erheben, erstellt die zuständige Organisationseinheit die Gebührenfestsetzung und erstellt einen eigenständigen Bescheid.

V. Inkrafttreten

§ 21 Inkrafttreten

Diese Dienstanweisung tritt am Tag der Unterzeichnung in Kraft. Gleichzeitig wird die Dienstanweisung 5/2001 „Datenschutz und Datensicherheit" vom 27.07.2001 aufgehoben.

Dirk Glaser
Bürgermeister