**A.3 - Muster für eine Dienstanweisung zum Datenschutz**

Dienstanweisung über die Organisation des Datenschutzes in der Kommune, Stadt, Gemeinde oder dem Landkreis.

Inhalt

Erster Teil: Allgemeine Regelungen

§ 1 Grundlagen

§ 2 Zweck der Dienstanweisung

§ 3 Geltungsbereich

§ 4 Begriffsbestimmungen

Zweiter Teil: Regelungen über die datenschutzrechtlichen Zuständigkeiten

§ 5 Die/der Hauptverwaltungsbeamte/Hauptverwaltungsbeamtin

§ 6 Organisationseinheiten

§ 7 IT-Organisationseinheit

§ 8 Datenschutzbeauftragte/r

§ 9 Vertrauensvolle Zusammenarbeit und gegenseitige Information

Dritter Teil: Besondere Zuständigkeiten

§ 10 Hauptamt

§ 11 Personalamt

§ 12 Rechtsamt/Justiziariat

§ 13 Einhaltung des Datenschutzes bei der Vergabe öffentlicher Aufträge

4. Teil Organisation der datenschutzrechtlichen Abläufe

§ 14 Richtigkeit, Vollständigkeit und Aktualität des Verzeichnisses der Verarbeitungstätigkeiten

§ 15 Nachweis für die Sicherheit der Verarbeitung gem. Art. 32 DSGVO, §§ 17, 32 NDSG

§ 16 Datenschutzfolgenabschätzung

§ 17 Verfahren bei Datenschutzverletzungen nach Art. 33, 34 DSGVO, §§ 41, 42 NDSG

§ 18 Auftragsverarbeitung

§ 19 Datenschutzbericht

§ 20 Beteiligung der/des Datenschutzbeauftragten

§ 21 Inkrafttreten dieser Dienstanweisung

Erster Teil – Allgemeine Regelungen

**§ 1 Grundlagen**

Grundlagen dieser Dienstanweisung sind:

a) die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). Soweit Ordnungswidrigkeiten bearbeitet werden, ist die Richtlinie 2016/680 (Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr) zu beachten.

b) spezialgesetzliche Regelungen des bereichsspezifischen Datenschutzes, insbesondere die Sozialgesetzbücher I, VIII und X,

c) das Niedersächsische Datenschutzgesetz (NDSG),

d) das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit (NDiG)

**§ 2 Zweck der Dienstanweisung**

Zweck dieser Dienstanweisung ist, den Schutz personenbezogener Daten zu gewährleisten.

**§ 3 Geltungsbereich**

Diese Dienstanweisung gilt für Organisationseinheiten und Eigenbetriebe der Musterkommune, die personenbezogene Daten verarbeiten oder im Wege der Auftragsverarbeitung durch einen Dritten verarbeiten lassen. Werden Dritte mit einer Datenverarbeitung beauftragt, ist sicherzustellen, dass diese die Anforderungen an eine rechtmäßige Datenverarbeitung ebenfalls erfüllen.

 **§ 4 Begriffsbestimmungen**

Es gelten die Definitionen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), der Justizrichtlinie, des NDSG sowie der spezialgesetzlichen Regelungen des bereichsspezifischen Datenschutzes, insb. des SGBI, VIII und SGB X.

Zweiter Teil: Regelungen über die datenschutzrechtlichen Zuständigkeiten

**§ 5 Hauptverwaltungsbeamter/Hauptverwaltungsbeamtin**

(1) Der/die Hauptverwaltungsbeamte/Hauptverwaltungsbeamtin stellt mit der Unterstützung der nachfolgend genannten Stellen sicher, dass personenbezogene Daten rechtmäßig verarbeitet werden.

(2) Der/die Hauptverwaltungsbeamte/Hauptverwaltungsbeamtin benennt eine/n Datenschutzbeauftragte/n und dessen Stellvertretung.

**§ 6 Organisationseinheiten**

(1) Im Rahmen ihres Zuständigkeitsbereichs sind die Organisationseinheiten für die Einhaltung der jeweils anzuwendenden Vorschriften über den Datenschutz verantwortlich.

(2) Die Organisationseinheiten sind im Rahmen ihres Zuständigkeitsbereichs insbesondere zuständig für

1. die Erstellung und Pflege des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DSGVO,
2. soweit erforderlich die Erstellung und Pflege des Verzeichnisses der Auftragsverarbeitung gem. Art. 30 Abs. 2 DSGVO,
3. die Erstellung von Risikoanalysen für Verarbeitungstätigkeiten gem. Art 32. DSGVO, § 52 NDSG im Benehmen mit der IT-Organisationseinheit,
4. die Erstellung von Datenschutzfolgenabschätzungen gem. Art. 35 DSGVO,

§ 39 NDSG im Benehmen mit der IT-Organisationseinheit,

1. die Erfüllung der Informationspflichten gem. Art. 13 ff. DSGVO, insbesondere bei Antragsformularen oder Vordrucken,
2. die Entscheidung über Auskunftsersuchen nach Art. 15 DSGVO, § 51 NDSG sowie die Rechtsbehelfe nach Art. 15 ff DSGVO, § 52 NDSG
3. die Erstellung fachspezifischer organisatorischer Maßnahmen oder Anweisungen,
4. die Entscheidung über den Versand von Akten, Vorgängen oder sonstigen Datenträgern im Rahmen der Amtshilfe,
5. die Entscheidung über die Übermittlung von personenbezogenen Daten,
6. für die Führung und Vernichtung von Akten,
7. das Festlegen von Löschfristen sowie das Löschen personenbezogener Daten

(3) *Optional:* Die Leiter/innen der Organisationseinheiten benennen einen oder mehrere Datenschutzkoordinatoren, die bei der Umsetzung des Datenschutzes mitwirken. Diese sind Ansprechpartner/innen für Vorgesetzte und Bedienstete.

(4) Im Rahmen des Geltungsbereichs dieser Dienstanweisung ist die Personalvertretung und das Rechnungsprüfungsamt eine Organisationseinheit. Der besonderen Aufgabe und Stellung der Personalvertretung und des Rechnungsprüfungsamts ist Rechnung zu tragen.

**§ 7 IT-Organisationseinheit**

Die IT-Organisationseinheit ist verantwortlich für

1. das Vorhalten und Zusammenführen der in Art. 30 Abs. 1 und Abs. 2 DSGVO, §8 NDSG genannten Verzeichnisse sowie das Bereitstellen einer EDV-Anwendung zu diesem Zweck,
2. das Festlegen geeigneter technischer Maßnahmen zum Schutz personenbezogener Daten im Rahmen von Risikoanalysen (Art. 32 DSGVO, § 34 NDSG) oder Datenschutzfolgenabschätzungen (Art. 35 DSGVO, § 39 NDSG) in Abstimmung/im Benehmen mit den Organisationseinheiten,
3. das Festlegen geeigneter technischer Maßnahmen zum Schutz personenbezogener Maßnahmen nach Art. 24 Abs. 1, Art. 25 Abs. 1 DSGVO sowie nach §§ 17, 34 NDSG in Abstimmung/im Benehmen mit den Organisationseinheiten,
4. Optional: die Bestellung eines/einer Informationssicherheitsbeauftragten
5. den Abschluss von AV-Verträge bei der Einführung von IuK

 **§ 8 Datenschutzbeauftragte/r**

(1) Die Benennung des/der Datenschutzbeauftragten gem. Art 37 DSGVO erfolgt durch ein förmliches an sie/ihn persönlich gerichtetes Schreiben. Soweit kein/e externe/r Datenschutzbeauftragte/r bestellt wird, unterliegen die Benennung sowie die Abberufung der Mitbestimmung der Personalvertretung.

(2) Bei der Bestellung der/des Datenschutzbeauftragten ist sicherzustellen, dass hierdurch keine Unvereinbarkeit mit ihrer/seiner Funktion entsteht. Unzulässig ist daher insbesondere die Bestellung von Bediensteten aus der Personalverwaltung, des Organisationswesens, der Informations- und Kommunikationstechnik oder bei Mitgliedern des Personalrats. Unzulässig ist ferner die Bestellung von Mitarbeitenden in leitenden Funktionen, deren Bestellung Interessenkonflikte hervorrufen würde.

(3) Die/der Datenschutzbeauftragte ist bei der Wahrnehmung ihrer/seiner Aufgaben weisungsfrei.

(4). Die/der Datenschutzbeauftragte hat das Recht, Stellungnahmen innerhalb der Dienststelle einzuholen. Stellt die/der Datenschutzbeauftragte Datenschutzverstöße fest, kann sie/er diese beanstanden und die betroffene Organisationseinheit zu einer Stellungnahme auffordern. Die/der Datenschutzbeauftragte kann mit der Beanstandung Vorschläge zur Beseitigung der Mängel oder zur sonstigen Verbesserung des Datenschutzes verbinden.

(5) Die/der Datenschutzbeauftragte hat ein direktes Vortragsrecht bei der/dem Hauptverwaltungsbeamten/Hauptverwaltungsbeamtin. Die/der Datenschutzbeauftragte kann der/dem Hauptverwaltungsbeamten/Hauptverwaltungsbeamtin regelmäßig Bericht erstatten.

**§ 9 Vertrauensvolle Zusammenarbeit und gegenseitige Information**

(1). Dem/der Datenschutzbeauftragten ist auf Anfrage Auskunft zu erteilen und der Zugang zu allen dienstlich genutzten Räumen und den Anlagen der IT-Technik, ohne Zugriff auf Passwörter der IT, sowie Einsicht in Akten und Dateien zu gewähren. Die Einsicht in Personalakten oder Daten, die einem besonderen Berufsgeheimnis unterliegen, bedarf grundsätzlich der Zustimmung der/des Betroffenen.

Dritter Teil: Besondere Zuständigkeiten

 **§ 10 Hauptamt**

Das Hauptamt ist zuständig für

1. die Pflege und Aktualisierung dieser Dienstanweisung im Benehmen mit der/dem Datenschutzbeauftragten.
2. Optional: die Erstellung und Pflege anderer interner Regelungen mit Bezug zum Datenschutzrecht, soweit diese hausweite Bedeutung haben und über die Zuständigkeit einer Organisationseinheit hinausgehen.

 **§ 11 Personalamt**

Das Personalamt ist zuständig für

1. die Verarbeitung personenbezogener Daten von Beschäftigten und Bewerbenden,
2. die Einhaltung des Beschäftigtendatenschutzes, insbesondere der §§ 12 NDSG; 88 ff. NBG,
3. das Ergreifen dienst- oder arbeitsrechtlicher Maßnahmen bei datenschutzrechtlichen Verstößen sowie bei Verstößen gegen andere Schutz- oder Geheimhaltungsvorschriften,
4. die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 59 NDSG

 **Optional: § 12 Rechtsamt/Justiziariat**

Das Rechtsamt/Justiziariat ist zuständig für

1. die Bearbeitung besonderer datenschutzrechtlicher Fragen mit grundsätzlichem Charakter im Benehmen/in Abstimmung mit dem/der Datenschutzbeauftragten,
2. die Bearbeitung von Schadensersatz- und Entschädigungsansprüchen,
3. die Bearbeitung von Strafanträgen

 **§ 13 Einhaltung des Datenschutzes bei der Vergabe öffentlicher Aufträge**

(1) Soweit bei der Durchführung eines Vergabeverfahrens personenbezogene Daten erhoben werden, ist die beschaffende Organisationseinheit für die Einhaltung des Datenschutzes verantwortlich.

(2) Werden bei der Durchführung eines Vergabeverfahrens personenbezogene Daten erhoben, dürfen diese nur für Zwecke des Vergabeverfahrens verwendet werden. Dies gilt insbesondere für Eignungs- und Zuschlagskriterien. Die Bestimmungen der Dienstanweisung für die Vergabe öffentlicher Aufträge bleiben unberührt.

(3) Für die Einhaltung der Vorgaben des Verpflichtungsgesetzes ist die beschaffende Organisationseinheit zuständig.

Fünfter Teil: Organisation der datenschutzrechtlichen Abläufe

 **§ 14 Richtigkeit, Vollständigkeit und Aktualität des Verzeichnisses der Verarbeitungstätigkeiten**

(1) *Optional:* Die IT-Organisationseinheit, bzw. die für die Führung des Verarbeitungsverzeichnisses zuständige Organisationseinheit, hält für die Führung des Verzeichnisses eine Anwendung vor. Diese Anwendung ist von allen Organisationseinheiten zu nutzen.

(2) Die Organisationseinheiten melden der IT-Organisationseinheit, bzw. der für die Führung des Verarbeitungsverzeichnisses zuständigen Organisationseinheit, unaufgefordert die neu aufgenommenen Verarbeitungstätigkeiten sowie die Änderungen bereits gemeldeter Verarbeitungstätigkeiten.

(3) Die Organisationseinheiten überprüfen das Verarbeitungsverzeichnis regelmäßig auf dessen Richtigkeit, Vollständigkeit und Aktualität.

 **§ 15 Nachweis für die Sicherheit der Verarbeitung gem. Art. 32 DSGVO, §§ 17, 34 NDSG**

(1) Die Organisationseinheiten erstellen im Benehmen mit der IT-Organisationseinheit Risikoanalysen für Verarbeitungstätigkeiten oder Auftragsverarbeitungen. Bei der Risikoanalyse findet die Eintrittswahrscheinlichkeit eines Schadens für personenbezogene Daten sowie dessen Schwere Berücksichtigung. Zur Bemessung der Schwere des Schadens ist das Schutzstufenkonzept der niedersächsischen Aufsichtsbehörde für den Datenschutz zu berücksichtigen. Das Ergebnis der Risikoanalyse ist aktenkundig zu machen.

(2) Die IT-Organisationseinheit legt im Benehmen mit der Organisationseinheit die technischen Abhilfemaßnahmen fest. Grundlage hierfür ist das Ergebnis der Risikoanalyse. Die Organisationseinheiten legen im Benehmen mit der IT-Organisationseinheit die organisatorischen Abhilfemaßnahmen fest.

(3) Die IT-Organisationseinheit hält für die Dokumentation der Risikoanalysen eine Anwendung vor. Diese Anwendung ist von allen Organisationseinheiten zu nutzen.

(4) Die Risikoanalysen sind regelmäßig/innerhalb eines Abstands von zwei Jahren regelmäßig zu überprüfen.

(4) Für die Erstellung der Risikoanalyse ist das als Anlage beigefügte Formular zu verwenden.

 **§ 16 Datenschutzfolgenabschätzung**

(1) In den Fällen des Art. 35 Abs. 1, Abs. 3 DSGVO, § 39 NDSG ist für eine Verarbeitungstätigkeit eine Datenschutzfolgenabschätzung durchzuführen. In einer Datenschutzfolgenabschätzung sind mehrere Verarbeitungstätigkeiten zu betrachten, sofern die einzelnen Verarbeitungstätigkeiten auf einen übergreifenden, gemeinsamen Zweck gerichtet sind.

(2) Soweit bei der Datenschutzfolgenabschätzung die Risiken für personenbezogene Daten und zu deren Bewältigung Abhilfemaßnahmen zu beschreiben sind, ist auf das Ergebnis der Risikoanalyse zurückzugreifen.

(3) Die Organisationseinheiten sind zuständig für

1. die Einleitung und Erstellung der Datenschutzfolgenabschätzung,
2. für die Beschreibung der Verarbeitungsvorgänge sowie der hiermit verfolgten Zwecke,
3. die Bewertung der Erforderlichkeit der Verarbeitung im Hinblick auf den hiermit verfolgten Zweck,
4. das Festlegen organisatorischer Abhilfemaßnahmen

(4) Die IT-Organisation ist im Benehmen mit den Organisationseinheiten zuständig für die Festlegung der technischen Abhilfemaßnahmen.

(5) Optional: Die IT-Organisationseinheit hält für die Dokumentation der Datenschutzfolgenabschätzung eine Anwendung vor. Diese Anwendung ist von allen Organisationseinheiten zu nutzen.

(6) Die IT-Organisationseinheit stellt die frühzeitige Einbindung des Datenschutzbeauftragten sicher.

**§ 17 Verfahren bei Datenschutzverletzungen nach Art. 33, 34 DSGVO, §§ 41, 42 NDSG**

(1) Bei Hinweisen auf eine meldepflichtige Verletzung personenbezogener Daten i. S. d. Art. 33, 34 i. V. m. Art. 4 Nr. 12 DSGVO; §§ 41, 42 NDSG informieren die Organisationseinheiten unverzüglich das Hauptamt, die IT-Organisationseinheit sowie den/die Datenschutzbeauftragte/n.

(2) Der/die Datenschutzbeauftragte gibt eine Stellungnahme ab, ob eine Meldepflicht nach Art. 33, 34 DSGVO; §§ 41, 42 NDSG besteht.

(3) Das Hauptamt bzw. die IT-Organisation prüft unter der Berücksichtigung der Einschätzung des/der Datenschutzbeauftragten, ob eine Meldepflicht gem. Art. 33, 34 DSGVO; §§ 41, 42 NDSG besteht. Alternative: Die IT-Organisation erstellt unter der Berücksichtigung der Einschätzung des/der Datenschutzbeauftragten eine Entscheidungsvorlage an den/die Hauptverwaltungsbeamten/Hauptverwaltungsbeamtin.

Sofern ein Fall der Art. 33, 34 DSGVO; §§ 41, 42 NDSG vorliegt, meldet die IT-Organisation, möglichst innerhalb einer Frist von 72 Stunden, den Vorfall an die Niedersächsische Behörde für den Datenschutz. Ist eine Meldung innerhalb dieses Zeitraums nicht möglich, ist die Meldung unverzüglich nachzuholen. Die IT-Organisation macht den Vorgang aktenkundig.

(4) Die Organisationseinheiten sind zuständig für die Information der Betroffenen gem. Art. 34 DSGVO, § 42 NDSG.

(5) Sind Sozialdaten von der Datenschutzverletzung betroffen, informiert die Organisationseinheit gem. § 83a SGB X die jeweils zuständige Fach- oder Rechtsaufsichtsbehörde.

(6) Nach der Abgabe der Meldung prüfen die IT-Organisationseinheit und die Organisationseinheiten in Abstimmung mit dem/der Datenschutzbeauftragten, ob zusätzliche technische und organisatorischer Maßnahmen getroffen werden müssen.

 **§ 18 Auftragsverarbeitung**

(1) Vor der Beschaffung oder Einführung einer IT-Leistung prüft die IT-Organisationseinheit, ob der Abschluss eines Vertrags über die Auftragsverarbeitung notwendig ist. Die IT-Organisationseinheit verpflichtet den Auftragsverarbeiter zur Einhaltung des Datenschutzes sowie zur Gewährleistung der erforderlichen technisch-organisatorischen Abhilfemaßnahmen.

(2) Soweit keine IT-Leistung eingeführt oder beschafft wird, prüfen die Organisationseinheiten bei der Erstellung der Vergabeunterlagen oder vor dem Abschluss sonstiger Verträge, ob ein Vertrag zur Auftragsverarbeitung zu schließen ist. Die Organisationseinheit verpflichtet den Auftragsverarbeiter zur Einhaltung des Datenschutzes sowie zur Gewährleistung der erforderlichen technisch-organisatorischen Abhilfemaßnahmen.

(3) Von den Auftragsverarbeitern können entsprechende Nachweise, Eigenerklärungen oder Zertifikate eingeholt werden

(4) Bei der Erstellung des Auftragsverarbeitungsvertrags ist die Stellungnahme der/des Datenschutzbeauftragten einzuholen.

 **§ 19 Datenschutzbericht**

(1) Die/der Datenschutzbeauftragte legt der/dem Hauptverwaltungsbeamten/ Hauptverwaltungsbeamtin regelmäßig, bzw. einmal pro Jahr, einen Datenschutzbericht vor. In dem Datenschutzbericht sind zumindest die festgestellten Datenschutzverstöße darzustellen.

(2) Optional: Die/der Hauptverwaltungsbeamte/Hauptverwaltungsbeamtin erörtert den Datenschutzbericht gemeinsam mit den Organisationseinheiten.

 **§ 20 Beteiligung des Datenschutzbeauftragten**

(1) Die/der Datenschutzbeauftragte ist frühzeitig in alle (optional: wesentlichen) Datenschutzfragen einzubinden. Die Organisationseinheiten und die IT-Organisation unterstützen den/die Datenschutzbeauftragte/n bei der Erfüllung ihrer/seiner Aufgaben.

(2) Die Organisationseinheiten stellen im Vorfeld von Vergabeverfahren die Einbindung der/des Datenschutzbeauftragten sicher, wenn Gegenstand des Auftrags die Verarbeitung personenbezogener Daten ist.

(3) Die IT-Organisationseinheit stellt vor der Beschaffung von IT-Leistungen wie Hard- und Software die frühzeitige Einbindung der/des Datenschutzbeauftragten sicher.

**§ 21 Inkrafttreten dieser Dienstanweisung**

Diese Dienstanweisung tritt mit dem Tag ihrer Unterschrift in Kraft.