



## Verfahrensverzeichnis

gemäß § 7 Landesdatenschutzgesetz Schleswig-Holstein (LDSG)  
bestimmt zur Einsichtnahme für jede Person (§ 7 Abs. 4 LDSG)

Verfahren	Finanzbuchhaltung newsystem®kommunal- Neues Kommunales Rechnungswesen (DOPPIK)
-----------	--------------------------------------------------------------------------------

Version: 9 / 15 gültig ab: 2009 / 2015 bis (sofern bestimmbar):     

### 1. Daten verarbeitende Stelle:

	<i>Landeshauptstadt Kiel, Fleethörn 9 (Rathaus), 24103 Kiel</i>
Amt/Abteilung	<i>Amt für Finanzwirtschaft</i>
Aktenzeichen	<i>90</i>
Kontakt	<i>Fachanwendungsbetreuer/in (Key User): Datenschutzbeauftragter: Herr Amann, Tel. 901 2771, <a href="mailto:datenschutz@kiel.de">datenschutz@kiel.de</a></i>

### 2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Zweckbestimmung	<p>Die Landeshauptstadt Kiel hat mit Wirkung vom 01. Januar 2009 das kamerale Haushalts- und Rechnungswesen auf die doppelte Buchführung (Doppik) gemäß den Vorgaben der Gemeindehaushaltsverordnung des Landes Schleswig-Holstein umgestellt.</p> <p>Als Finanzsoftware wird <i>newsystem®kommunal</i> der Firma INFOMA eingesetzt. Diese Software unterstützt derzeit mindestens die folgenden Aufgabenbereiche: Planung / Konsolidierung, Finanzbuchhaltung, Bilanzbuchhaltung mit Jahresabschluss, Stadtkasse, Vollstreckung, Kosten- und Leistungsrechnung, Anlagenbuchhaltung und die Veranlagung.</p>
Rechtsgrundlage	<p>Grundlage für die Einführung sind die Empfehlungen der Innenministerkonferenz, die Empfehlungen des Innovationsringes Schleswig-Holstein in der jeweils aktuellen Fassung, die gesetzlichen Regelungen des Landes Schleswig-Holstein einschließlich Verordnungen, insbesondere die Gemeindeordnung (GO) und die Gemeindehaushaltsverordnung Doppik (GemHVO-Doppik).</p>

### 3. Kreis der Betroffenen:

1	Debitoren aller Art (Steuer- und Gebührenzahler/innen)
2	Kreditoren aller Art (Firmen, Lieferanten, Leistungsempfänger ...)

### 4. Kategorien verarbeiteter Daten, Löschungs-, Aufbewahrungsfristen, Zugriffsberechtigungen

	4.1 Kategorien der verarbeiteten Daten	„Besonders sensible“ Daten gem. § 11 Abs. 3 LDSG
4.1.1	Name und Anschrift aller Debitoren (Steuern- und Gebührenzahler/innen)	nein
4.1.2	Name und Anschrift aller Kreditoren	nein
4.1.3	Kontoverbindungen von Debitoren	nein
4.1.4	Kontoverbindungen von Kreditoren	nein
4.1.5	Debitorische Belegdaten	nein
4.1.6	Kreditorische Belegdaten	nein
4.1.7	Vollstreckungsakten	nein

zu Daten aus	4.2 Löschungs- und Aufbewahrungsfristen
Nr. 4.1.1-7	<i>Löschung nach 10 Jahren</i>

zu Daten aus	4.3 Zugriffsberechtigte Personen oder Personengruppen
Nr. 4.1.1 und 3	<i>Mitarbeiterinnen und Mitarbeiter der Sammel- und Erfassungstellen, der Bilanzabteilung, der Stadtkasse und der Steuerabteilung</i>
Nr. 4.1.2 und 4	<i>Mitarbeiterinnen und Mitarbeiter der Sammel- und Erfassungstellen, der Bilanzabteilung und der Stadtkasse</i>
Nr. 4.1.5 und 6	<i>Mitarbeiterinnen und Mitarbeiter der Sammel- und Erfassungstellen, der Bilanzabteilung, der Stadtkasse, der Steuerabteilung sowie der jeweils betroffenen Fachämter</i>
Nr. 4.1.7	<i>Vollstreckungsabteilung</i>

5. Art und Empfänger zu übermittelnder und empfangener Daten inkl. Auftragsdatenverarbeitung

zu Daten aus	5.1 Empfänger von zu übermittelnden Daten
Nr. 4.1.5	<i>Zahlungsdaten an Banken und Sparkassen</i>
Nr. 4.1.6	<i>Zahlungsdaten von Banken und Sparkassen</i>
Aggregierte Daten ohne Personenbezug	<i>Auswertungen aller Art für Controlling- und Statistikzwecke, Haushaltsplanung und Jahresabschluss</i>

zu Daten aus	5.2 Herkunft empfangener Daten
Nr. 4.1.1/2-5/6	<i>Daten aus vorgelagerten Systemen/Schnittstellen aus den Bereichen Darlehensverwaltung, Feuerwehr(Krankentransporte), Friedhofsverwaltung, KiTa-</i>

	Gebühren

6. Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union:

*Keine*

7. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen

*Die für dieses Verfahren eingesetzte Technik ist in die Netzwerkinfrastruktur und in die Sicherheitskonzeption der Landeshauptstadt Kiel eingebunden. Zur Sicherstellung der Datensicherheit und des Datenschutzes werden technische und organisatorische Maßnahmen eingesetzt. Sie orientieren sich an den sechs Datensicherheits- und Datenschutz-Schutzzielen des § 5 und § 6 LDSG. Die wichtigsten Maßnahmen zur Umsetzung werden nachfolgend aufgeführt. Die vollständigen Maßnahmen sind in der Sicherheits- und Verfahrensdokumentation dokumentiert.*

8. Datenschutzrechtliche Beurteilung

8.1	Stellungnahme der/des Datenschutzbeauftragten (falls vorhanden)

8.2	Technisch-organisatorische Maßnahmen
	<p><b>Verfügbarkeit</b> (Verfahren und Daten stehen zeitgerecht zur Verfügung):</p> <ul style="list-style-type: none"> <li>› Die Daten werden regelmäßig gemäß der Datensicherungskonzeption der Landeshauptstadt Kiel gesichert. Das Verfahren wird auf zentralen Systemen gesichert.</li> <li>› Das Verfahren kann bei einem Ausfall in einem definierten Zeitraum (Sicherheitskonzeption) wieder hergestellt werden.</li> </ul>
	<p><b>Vertraulichkeit</b> (es können nur befugte Personen auf Daten und Verfahren zugreifen):</p> <ul style="list-style-type: none"> <li>› Für das Verfahren gelten die allgemeinen Regeln zur Zutrittskontrolle für Büro- und Serverräume der Landeshauptstadt Kiel sowie für den Zugang zu Client- und Serversystemen (Passwortschutz).</li> <li>› Innerhalb des Verfahrens wird durch eine dokumentierte Berechtigungsvergabe sichergestellt, dass nur berechtigte Personen auf die Datenbestände zugreifen dürfen. Die Prüfung der Berechtigung erfolgt passwortbasiert.</li> </ul>
	<p><b>Integrität</b> (es wird gewährleistet, dass Daten unversehrt, vollständig, zurechenbar und aktuell bleiben):</p> <ul style="list-style-type: none"> <li>› Auf dem Fachverfahrensserver hat nur die technische Administration dieses Servers Zugriff. Es wird zentral sichergestellt, dass das Betriebssystem regelmäßig aktualisiert wird (Schutz vor Veränderung der Daten durch Angriffe oder unberechtigten Zugriff).</li> <li>› Innerhalb des Verfahrens haben nur die fachliche Administration dieses Verfahrens</li> </ul>

*und die Personen, die die Datenpflege betreiben, Zugriff auf die Datenbestände (Schutz vor Veränderung durch unberechtigten Zugriff).*

**Transparenz** *(die automatisierte Verarbeitung von Daten kann mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden):*

- › *Das Verfahren ist in einer Verfahrensakte, die technischen Systeme sind in einer Systemakte LDSG- und DSGVO-konform dokumentiert.*
- › *Die Datenverarbeitung wird innerhalb des Fachverfahrens protokolliert und kann über eine Historien-Funktion dargestellt werden.*

**Intervenierbarkeit** *(die Daten verarbeitende Stelle kann nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht und dass Betroffene die ihnen zustehenden Rechte ausüben können):*

- › *Das Verfahren und die benötigten IT-Komponenten inkl. des E-Mail-Versandes werden durch die Landeshauptstadt Kiel betrieben.*
- › *Das Fachverfahren verfügt über Funktionalitäten zur Auskunftserteilung, Änderungen, Sperrung und Löschung von Daten Betroffener.*

**Nicht-Verkettbarkeit** *(es kann sichergestellt werden, dass Daten nur zu dem ausgewiesenen Zweck automatisiert erhoben, verarbeitet und genutzt werden):*

- › *Die Daten sind auf technisch bzw. logisch getrennten Systemen gespeichert, weiterhin sind die Aufgaben der Systemadministration und Fachanwendungsbetreuung personell und organisatorisch getrennt.*
- › *Die Schnittstellen zu anderen Empfängern (siehe Nr. 5) übertragen ausschließlich die Daten, die für die Funktionalität (z. B. Zahlungen) erforderlich sind.*
- › *Auf die Datenbestände des Verfahrens können ausschließlich die in Abschnitt 4.3 genannten Personengruppen zugreifen.*

## 9. Freigabe des Verfahrensverzeichnis

28.10.2015

Kiel,

Leitung Amt für Finanzwirtschaft

gezeichnet