Verfahrensverzeichnis gem. § 7 LDSG-SH

1. **Aktenzeichen:**

511.04.10.05.10

2. **Name und Art des Verfahren (ggf. Versions-Nr.):**

LÄMMkom Jugendhilfe, Client-Verfahren,
aktuelle Version 9.1.5.8a
Das LÄMMkom-Verfahren beinhaltet noch eine integrierte Rechtsdatenbank für Sozialleistungen; der Name lautet SOLEX press.

3. **Name und Anschrift der Daten verarbeitenden Stelle (= Verfahrensanwender) [I]:**

Hansestadt Lübeck
4.511 Städtische Kindertageseinrichtungen
2.500 Soziale Sicherung / Team Kita-Entgeltermäßigung
4.510 Familienhilfe / Jugendamt Abt. Kindertagespflege
Verwaltungszentrum Mühlentor
Kronsforder Allee 2-6
23560 Lübeck

4. **Zweckbestimmung des Verfahrens [II]:**

4.511 städt. Kindertageseinrichtungen:
Verwaltung der städtischen Kindertageseinrichtungen
Festlegen der Entgelte für die Betreuung von Kindern,
Erstellen der Entgeltfestsetzungen für die Eltern,
2.500 Bereich Soziale Sicherung / Team Kita-Entgeltermäßigung:
Bearbeitung der Kita-Entgeltermäßigungen gem. § 90 SBG VIII
4.510 Familienhilfe / Jugendamt Abt. Kindertagespflege:
Verwaltung der Kinder in Tagespflege

5. **Rechtsgrundlage des Verfahrens:**

ohne - freiwillige Aufgabe

6. **Kreis der Betroffenen [III]:**

- Kinder und Erziehungsberechtigte, die in Kindertagesstätten (Kitas) betreut werden und deren gewöhnlicher Aufenthaltsort Lübeck ist
- Bezüglich Pflegekinder ist maßgebend die Betreuung durch das Jugendamt der HL.

7. **Kategorien der verarbeiteten Daten [IV]:**

Angaben zur betreuten Person und der Erziehungsberechtigten und deren Adressdaten,
Angaben von Einkommen und Ausgaben der Familien, Kontoverbindungen

8. **Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden [V]:**

Herkunft: Angaben aus Betreuungsverträgen und Anträgen für Kita-Ermäßigung
Empfänger: Daten werden nur verwaltungsintern verarbeitet

9. Geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union [VI]:

keine

10. Datenschutzrechtliche Beurteilung des behördlichen Datenschutzbeauftragten / ULD [VII]:

Negativ, da kein behördlicher Datenschutzbeauftragter ernannt wurde.

11. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen [VIII]:

- Die HL befindet sich in einem Zertifizierungsverfahren und wird durch das ULD–SH entsprechend begleitet.
  Server- und Clientkonzepte sind vorhanden.

- Zugang zu Datenträgern, Servern etc.
  Der Zugang zu Servern und Datenträgern, die in einem separat gesicherten Rechenzentrum stehen, ist nur autorisierten IT-Personen erlaubt.

- Wer darf die Daten verarbeiten?
  Stamm- und Systemdaten sind den datenverarbeitenden Stellen 4.511 städt. Kindertageseinrichtungen und 2.500 Soziale Sicherung / Team Kita-Entgeltermäßigung zugeordnet und werden von dort verwaltet.

- Protokollierung, wer, wann auf welche Daten zugegriffen hat
  DB-seitig (Oracle) findet keine besondere Protokollierung statt.

- Benutzerverwaltung
  Die datenverarbeitenden Stellen regeln die Benutzerverwaltung in eigener Verantwortung. Zugriffsberechtigungen werden von 4.511 – städt. Kindertages-einrichtungen, 2.500 Soziale Sicherung / Team Kita-Entgeltermäßigung und 4.510 Familienhilfe / Jugendamt Abt. Kindertagespflege verwaltet.

- Verschlüsselung von Daten
  Die personenbezogenen Daten werden von den Sachbearbeiterinnen und Sachbearbeitern der zugriffsberechtigten Bereiche bearbeitet.
  Die Verarbeitung findet nicht außerhalb der Räumlichkeiten der HL statt.
  Eine Verschlüsselung der Daten ist daher nicht notwendig.

- Datenschutz-Siegel für LÄMMkom
  Das ULD-SH hat der Firma LÄMMERZAHL 2003 mit seinem Gütesiegel bescheinigt, dass die Software mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde.

- Die Anwendung ist dezentral auf den PC´s der Anwender installiert. Die Datenbank ist zentral auf einem Server installiert, auf den nur MitarbeiterInnen des Bereiches 1.105 Informationstechnik zugreifen können.

Die PC's und das Verfahren sind jeweils durch Passworteingabe geschützt.

- Risikoanalyse:
  - Da die Software auf dem jeweiligen Rechner installiert wurde, kann nur über diese Clients auf das Verfahren zugegriffen werden.
  - Die Clients werden über die AD-Richtlinie verwaltet. Standardmäßig werden nach 10 Minuten die Clients per Richtlinie gesperrt.
    Auf jedem Client befindet sich ein aktueller Virenscanner.
    Der Serverbetrieb jeglicher Art findet ausschließlich im Rechenzentrum der HL statt.
  - Downloadmöglichkeiten, Datenexport
    nur intern von den zugriffsberechtigten MitarbeiterInnen möglich.
  - Zugriff extern auf Intranet:
    nicht möglich.

12. Gespeicherte personenbezogene Daten angeben (sofern unter 6. Kategorie „Diverse" angegeben ist):

entfällt

Interne Informationen (Nicht verschicken !!)

13. Schutzbedarfsfeststellung (intern) (n=normal, m=mittel, h=hoch):

Vertraulichkeit: normal
Integrität: normal
Verfügbarkeit: normal

14. Verfahrensbetreuer (Ansprechpartner):

Bereich: 4.511 städtische Kindertageseinrichtungen Frau Gudrun Habeck (Tel. 0451/122-5112) 2.500 Soziale Sicherung / Team Entgeltermäßigung Herr Riccardo Behm (Tel. 0451/122-5747) 4.510 Familienhilfen / Jugendamt Abt. Tagespflege kein Ansprechpartner
1.105 Informationstechnik Tilo-C. Fuhl (Tel. 0451/122-7443) Jens-Peter Herrmann (Tel. 0451/122-7414)
Firma/Firmen: Lämmerzahl Am Uhlenhorst 1 44225 Dortmund Tel: 02 31 / 1 77 94 - 0 Fax: 02 31 / 1 77 94 - 50 eMail: info@laemmerzahl.de www: www.laemmerzahl.de

Erläuterungen

I **Daten verarbeitende Stelle** ist jede öffentliche Stelle im Sinne von § 3 Abs. 1 LDSG, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt (vgl. § 2 LDSG Abs. 3).

II Angaben über den **Zweck** und die **Rechtsgrundlage** des Verfahrens (z.B.: Führung des Melderegisters, Landesmeldegesetz, Dienstvereinbarung mit dem Personalrat, § 11 Abs. 1 Nr. 3 LDSG).

III Der **Kreis der Betroffenen**. Die Personengruppe, deren Daten in dem Verfahren gespeichert wird, ist in abstrakter Weise zu beschreiben (*z.B. Alle Personen, die ihren Wohnsitz in der Gemeinde haben und meldepflichtig sind, oder: Empfänger von Schreiben der jeweiligen Daten verarbeitenden Stelle*).

IV Die **Kategorie** der **verarbeiteten Daten**. Soweit eine spezielle Rechtsgrundlage mit einem abschließenden Datenkatalog existiert, sind die darin genannten Datenarten aufzuzählen. Entsprechendes gilt, wenn die Kategorien der Daten auf andere Weise vorgegeben sind. Bei allgemeinen Verfahren der Büroautomation können die Angaben nach Nr. 3 bis 6 häufig nicht näher festgelegt werden. Hier genügt die Angabe „Diverse".

V Die tatsächlichen und die nur potenziellen **Empfänger** der Daten. Zu den Stellen und Personen, die die Daten erhalten dürfen, gehören nicht solche Empfänger, an die lediglich ausnahmsweise und auf Grund besonderer Umstände im Einzelfall Daten weitergegeben werden. In das Verzeichnis aufzunehmen sind aber solchen Stellen, an die mit einer gewissen Regelmäßigkeit in bestimmten Fällen oder bei Eintritt gewisser wiederkehrender Umstände die Daten weitergegeben werden. Zu den Empfängern gehören auch die Auftragsdatenverarbeiter; auch diese sind zu melden.

VI Geplante **Übermittlungen** an Stellen **außerhalb** der **Mitgliedsstaaten der EU**. Die Übermittlung in sog. Drittstaaten unterliegt nach § 16 Abs. 2 LDSG besonderen Voraussetzungen. Die Angaben im Verzeichnis sollen sicherstellen, dass das Vorliegen dieser Voraussetzungen nachprüfbar bleibt und dass die Beteiligung des ULD nach § 16 Abs. 3 LDSG gewährleistet ist.

VII Die Beurteilung des Verfahrens durch die **behördliche Datenschutzbeauftragte** oder den behördlichen Datenschutzbeauftragten, soweit eine solche vorliegt. Eine Beurteilung wird in der Regel im Rahmen der Vorabkontrolle nach § 9 abgegeben werden. Diese obliegt gem. § 10 Abs. 4 Nr. 5 LDSG in erster Linie der oder dem behördlichen Datenschutzbeauftragten.

VIII Die allgemeine Beschreibung der zur Einhaltung der **Datensicherheit** nach den §§ 5 und 6 LDSG getroffenen Maßnahmen. Eine solche Beschreibung ist das nach § 8 Abs. 1 der DSVO zu erstellende Sicherheitskonzept.

Verfahrensverzeichnis gem. § 7 LDSG-SH

1. **Aktenzeichen + Lfd. Nr.:**

AZ 4.416 P1

2. **Name und Art des Verfahren (ggf. Versions-Nr.):**

Bibliotheksverwaltungssystem Concerto, Client-Server-Verfahren und Web-Anwendung

3. **Name und Anschrift der Daten verarbeitenden Stelle (= Verfahrensanwender) [I]:**

Bibliothek der Hansestadt Lübeck
Hundestraße 5 - 17
23552 Lübeck

4. **Zweckbestimmung des Verfahrens [II]:**

Integriertes Bibliotheksverwaltungssystem zum Erwerb, zur Katalogisierung und zur Ausleihe von Medien

5. **Rechtsgrundlage des Verfahrens:**

ohne
Gebührenordnung, Benutzungssatzung

6. **Kreis der Betroffenen [III]:**

MitarbeiterInnen der Stadtbibliothek, Bibliothekskundinnen und -kunden

7. **Kategorien der verarbeiteten Daten [IV]:**

Adressdaten der nutzenden Personen

8. **Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden [V]:**

Herkunft: Angaben der Bibliothekskundinnen und -kunden

Empfänger: MitarbeiterInnen der Stadtbibliothek

9. Geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union [VI]:

keine

10. Datenschutzrechtliche Beurteilung des behördlichen Datenschutzbeauftragten / ULD [VII]:

Negativ, da kein behördlicher Datenschutzbeauftragter ernannt wurde.

11. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen [VIII]:

- Die Hansestadt Lübeck befindet sich in einem Zertifizierungsverfahren und wird durch das ULD–SH entsprechend begleitet.
  Server- und Clientkonzepte sind vorhanden.

- Zugang zu Datenträgern, Servern etc.
  Der Zugang zu Servern und Datenträgern, die in einem separat gesicherten Rechnerraum stehen, ist nur autorisierten IT-Personen erlaubt.

- Wer darf die Daten verarbeiten?
  Daten können nur von berechtigten MitarbeiterInnen der Stadtbibliothek der Hansestadt Lübeck eingesehen und bearbeitet werden.

- Protokollierung, wer, wann auf welche Daten zugegriffen hat
  Serverprotokolle der Programme und Daten.
  Zugriffe können nur von berechtigten MitarbeiterInnen der Stadtbibliothek nach verfolgt werden.

- Benutzerverwaltung
  Die Daten verarbeitende Stelle regelt die Benutzerverwaltung in eigener Verantwortung.

- Verschlüsselung von Daten
  Die Verarbeitung findet nicht außerhalb der Räumlichkeiten der Stadtbibliothek Lübeck statt.
  Eine Verschlüsselung der Daten ist daher nicht notwendig.
  Beim Zugriff der Kundinnen und Kunden über den elektronischen Katalog findet eine Verschlüsselung statt.

- Die Anwendung befindet sich zentral auf einem Datenbankserver und wird dem Anwender zur Ausführungszeit lokal zur Verfügung gestellt.
  Die PCs und das Verfahren sind jeweils durch Passworteingabe geschützt.

- Risikoanalyse:
  - Ein Zugriff auf das Verfahren erfolgt über den seitens der Infotechnik vorgeschriebenen Standard-Browser.
    Der Datenbankserver wird sich in Zukunft im Rechenzentrum der HL befinden.

- Downloadmöglichkeiten, Datenexport
  Nur durch berechtigte Personen
- Zugriff extern auf Intranet
  Der externe Zugang zur internen Datenbankanwendung erfolgt über das seitens der Infotechnik vorgeschriebene Fernwartungsprogramm

12. Gespeicherte personenbezogene Daten angeben (sofern unter 6. Kategorie „Diverse" angegeben ist):

Verfahrensverzeichnis gem. § 7 LDSG-SH

1. **Aktenzeichen + Lfd. Nr.:**

10.71.15.45.1.1

2. **Name und Art des Verfahren (ggf. Versions-Nr.):**

Ratsinformationssystem ALLRIS, Client-Server-Verfahren und Web-Anwendung,
V 3.8.5

3. **Name und Anschrift der Daten verarbeitenden Stelle (= Verfahrensanwender) [I]:**

Hansestadt Lübeck
Büro der Bürgerschaft
Rathaus
Breite Straße 62
23539 Lübeck

Hansestadt Lübeck
Bürgermeisterkanzlei
Rathaus
Breite Straße 62
23539 Lübeck

4. **Zweckbestimmung des Verfahrens [II]:**

Erstellung von Vorlagen, Berichten, Anträgen und deren Einbringung in den Beratungsgang,
Abwicklung des gesamten internen Sitzungsdienstes (Terminplanung, Vorbereitung, Durchführung und Nachbereitung von Sitzungen),
Bürgerinformations- und Ratsinformationssystem für Politiker,
Abrechnung des Sitzungsgeldes.

5. **Rechtsgrundlage des Verfahrens:**

ohne - freiwillige Aufgabe

6. **Kreis der Betroffenen [III]:**

a) Amtsinformationssystem
Personen, die mit der Bearbeitung (Erstellung, Freigabe) von Vorlagen, Berichten und Anträgen betraut sind,
Personen, die mit der Durchführung von Ausschusssitzungen befasst sind,
Personen, die mit der Abwicklung des Sitzungsdienstes befasst sind (1.100 – Büro der Bürgerschaft und 1.101- Bürgermeisterkanzlei),
b) Ratsinformationssystem
Personen in den politischen Gremien (Bürgerschaft und Ausschüsse),
Personen, die das Verfahren über Internet/Intranet nutzen.

7. **Kategorien der verarbeiteten Daten [IV]:**

Angaben zur nutzenden Person und deren Adressdaten,
Funktionen/Ämter von Bürgerschafts- und Ausschussmitgliedern,
Vorlagen, Berichte, Anträge und deren Anlagen,
Besprechungsprotokolle, bei Nutzung Modul Sitzungsgeld auch Bankdaten

8. Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden [V]:

Herkunft: Vorlagenersteller, Gremienverwalter, Kommunalpolitiker
Empfänger: Verwaltungspersonal, Kommunalpolitiker, bürgerliche Mitglieder, Internetnutzer

9. Geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union [VI]:

keine

10. Datenschutzrechtliche Beurteilung des behördlichen Datenschutzbeauftragten / ULD [VII]:

Negativ, da kein behördlicher Datenschutzbeauftragter ernannt wurde.

11. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen [VIII]:

- Die HL befindet sich in einem Zertifizierungsverfahren und wird durch das ULD–SH entsprechend begleitet.
  Server- und Clientkonzepte sind vorhanden.

- Zugang zu Datenträgern, Servern etc.
  Der Zugang zu Servern und Datenträgern, die in einem separat gesicherten Rechenzentrum stehen, ist nur autorisierten IT-Personen erlaubt.

- Wer darf die Daten verarbeiten?
  Stamm- und Systemdaten sind den datenverarbeitenden Stellen 1.100 – Büro der Bürgerschaft und 1.101 – Bürgermeisterkanzlei zugeordnet und werden von dort verwaltet.
  Vorlagen- und Niederschriftsdaten können von allen berechtigten Personen eingesehen und weiterverarbeitet werden.

- Protokollierung, wer, wann auf welche Daten zugegriffen hat
  Der Server protokolliert alle Zugriffe auf die Programme und Daten.
  DB-seitig (Oracle) findet keine Protokollierung statt.
  ALLRIS selbst liefert keine Daten zum Zugriff auf Protokolle oder Daten.

- Benutzerverwaltung
  Die datenverarbeitenden Stellen regeln die Benutzerverwaltung in eigener Verantwortung. Zugriffsberechtigungen werden vom 1.100 – Büro der Bürgerschaft und von der 1.101 – Bürgermeisterkanzlei verwaltet.

- Verschlüsselung von Daten
  Die einzigen personenbezogenen Daten werden im Sitzungsgeldmodul (Zugriff erfolgt ausschließlich über C/S-Modul) bearbeitet.
  Die Verarbeitung findet nicht außerhalb der Räumlichkeiten der HL statt.
  Eine Verschlüsselung der Daten ist daher nicht notwendig.

- Datenschutz-Siegel für ALLRIS
  Das ULD-SH hat durch sein Gütesiegel bescheinigt, dass die Vereinbarkeit des Ratsinformationssystems ALLRIS mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde.

- Die Anwendung befindet sich zentral auf einem **Citrixserver** und wird dem Anwender zur Ausführungszeit lokal virtuell zur Verfügung gestellt.
  Die PC's und das Verfahren sind jeweils durch Passworteingabe geschützt.

- Risikoanalyse:
  Amtsinformationssystem (ALLRIS intern)
  - In allen Räumlichkeiten der HL kann über den Webclient auf das Verfahren zugegriffen werden (nicht Modul Sitzungsgeld).
    Die Clients werden über die AD-Richtlinie verwaltet. Standardmäßig werden nach 10 Minuten die Clients per Richtlinie gesperrt.
    Auf jedem Client befindet sich ein aktueller Virenscanner.
    Serverbetrieb findet ausschließlich im Rechenzentrum der HL statt.
  - Datenbestände i. V. mit der Aktenkofferfunktion können auf dienstlichen mobilen Geräten unverschlüsselt abgelegt werden. Private Geräte haben keinen Zugang.
  - Downloadmöglichkeiten, Datenexport
    Nur durch berechtigte Personen auf dienstlichen mobilen Geräten.
  - Zugriff extern auf Intranet
    Der externe Zugang zum internen ALLRIS-Net-Modul erfolgt über ein VPN-Gateway, Token-Verschlüsselung und CITRIX-ACCESS-GATEWAY mit entsprechender Zugangsauthentifizierung.
  -
- Ratsinformationssystem (ALLRIS extern)
  - Das Ratsinformationssystem ist extern eine mehrmals täglich replizierte Version des internen Verfahrens ohne Änderungsmöglichkeit.
  - Datenbestände i. V. mit der Aktenkofferfunktion können auf privaten mobilen Geräten unverschlüsselt abgelegt werden. Eine Zugangskennung zum externen System ist notwendig.
  - Druck von nicht öffentlichen Vorlagen
    Im Ratsinformationssystem immer mit Wasserzeichen (Vorname, Name und Datum)

12. Gespeicherte personenbezogene Daten angeben (sofern unter 6. Kategorie „Diverse" angegeben ist):

Verfahrensverzeichnis gem. § 7 LDSG-SH

1. **Aktenzeichen + Lfd. Nr.:**

.....

2. **Name und Art des Verfahren (ggf. Versions-Nr.):**

FAUST, Client -Verfahren, V 7 Professional

3. **Name und Anschrift der Daten verarbeitenden Stelle (= Verfahrensanwender) [I]:**

Hansestadt Lübeck
Kulturstiftung Hansestadt Lübeck
Die LÜBECKER MUSEEN
Schildstraße 12
23539 Lübeck

4. **Zweckbestimmung des Verfahrens [II]:**

FAUST ist ein Datenbank-und Retrievalsystem für Museen, Archive und Bibliotheken. Es wird benutzt für die digitale Inventarisierung und Archivierung von Sammlungsobjekten und Archivbeständen sowie für die Bibliotheksverwaltung.

5. **Rechtsgrundlage des Verfahrens:**

ohne - freiwillige Aufgabe

6. **Kreis der Betroffenen [III]:**

Personen, die dem Museum Exponate oder Archivalien zur Verfügung stellen.
Personen, die in den Archivalien erwähnt sind

7. **Kategorien der verarbeiteten Daten [IV]:**

Diverse

8. **Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden [V]:**

Herkunft: Vorlagenersteller
Empfänger: Verwaltungspersonal, Internetnutzer (erhalten nur ausgewählte Daten)

9. **Geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union [VI]:**

keine

10. Datenschutzrechtliche Beurteilung des behördlichen Datenschutzbeauftragten / ULD [VII]:

Negativ, da kein behördlicher Datenschutzbeauftragter ernannt wurde.

11. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen [VIII]:

- Die HL befindet sich in einem Zertifizierungsverfahren und wird durch das ULD–SH entsprechend begleitet.
  Server- und Clientkonzepte sind vorhanden.

- Zugang zu Datenträgern, Servern etc.
  Der Zugang zu Servern und Datenträgern, die in einem separat gesicherten Rechenzentrum stehen, ist nur autorisierten IT-Personen erlaubt.

  Wer darf die Daten verarbeiten?
  Die Daten sind der datenverarbeitenden Stelle 4.041.7 – Kulturstiftung Hansestadt Lübeck die LÜBECKER MUSEEN zugeordnet und werden von dort verwaltet.

- Protokollierung, wer, wann auf welche Daten zugegriffen hat.
  Verfahrensseitig findet keine Protokollierung statt. (Die Datenbank ist im Verfahren integriert)

- Benutzerverwaltung
  Die datenverarbeitende Stelle regelt die Benutzerverwaltung in eigener Verantwortung. Zugriffsberechtigungen werden vom Bereich 4.041.7 – Kulturstiftung Hansestadt Lübeck die LÜBECKER MUSEEN verwaltet.

- Verschlüsselung von Daten
  Die Verarbeitung findet nicht außerhalb der Räumlichkeiten der HL statt.
  Eine Verschlüsselung der Daten ist daher nicht notwendig.

- Die Anwendung befindet sich zentral auf einem Laufwerk (g) und wird dem Anwender zur Ausführungszeit per Verknüpfung zur Verfügung gestellt.
  Die PC's sind jeweils durch Passworteingabe geschützt.

- Risikoanalyse:
  - Die Clients werden über die AD-Richtlinie verwaltet. Standardmäßig werden nach 10 Minuten die Clients per Richtlinie gesperrt.
    Auf jedem Client befindet sich ein aktueller Virenscanner.
    Serverbetrieb findet ausschließlich im Rechenzentrum der HL statt.
  - Datenexport
    Zurzeit nicht vorgesehen, Im Anwendungsfall nur durch organisatorisch berechtigte Personen.

12. Gespeicherte personenbezogene Daten angeben (sofern unter 6. Kategorie „Diverse" angegeben ist):

Zugangsdaten der Mitarbeiter, die mit dem Programm arbeiten; Namen, Lebensdaten, evtl. Adressdaten von Personen, die in Archivalien erwähnt sind; Namen von Leihgebern

Interne Informationen (Nicht verschicken !!)

13. Schutzbedarfsfeststellung (intern)(n=normal, m=mittel, h=hoch):

Vertraulichkeit: normal
Integrität: normal
Verfügbarkeit: normal

14. Verfahrensbetreuer (Ansprechpartner):

Bereich: Britta Dittmann (Tel. 0451/122-7546)
1.105 Informationstechnik Tilo-C. Fuhl (Tel. 0451/122-7443) Oliver Klapmeier (Tel. 0451-1227423)
Firma/Firmen: Land Software Entwicklung Magdeburger Straße 2 90522 Oberasbach Tel.: +49 (0911) 69 6911 Fax: +49 (0911) 69 51 73 eMail: info@land-software.de www: www.land-software.de Irina Daßler E-Mail: support@land-software.de

Verfahrensverzeichnis gem. § 7 LDSG-SH

Erläuterungen

I **Daten verarbeitende Stelle** ist jede öffentliche Stelle im Sinne von § 3 Abs. 1 LDSG, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt (vgl. § 2 LDSG Abs. 3).

II Angaben über den **Zweck** und die **Rechtsgrundlage** des Verfahrens (z.B.: Führung des Melderegisters, Landesmeldegesetz, Dienstvereinbarung mit dem Personalrat, § 11 Abs. 1 Nr. 3 LDSG).

III Der **Kreis der Betroffenen**. Die Personengruppe, deren Daten in dem Verfahren gespeichert wird, ist in abstrakter Weise zu beschreiben (*z.B. Alle Personen, die ihren Wohnsitz in der Gemeinde haben und meldepflichtig sind, oder: Empfänger von Schreiben der jeweiligen Daten verarbeitenden Stelle*).

IV Die **Kategorie** der **verarbeiteten Daten**. Soweit eine spezielle Rechtsgrundlage mit einem abschließenden Datenkatalog existiert, sind die darin genannten Datenarten aufzuzählen. Entsprechendes gilt, wenn die Kategorien der Daten auf andere Weise vorgegeben sind. Bei allgemeinen Verfahren der Büroautomation können die Angaben nach Nr. 3 bis 6 häufig nicht näher festgelegt werden. Hier genügt die Angabe „Diverse".

V Die tatsächlichen und die nur potenziellen **Empfänger** der Daten. Zu den Stellen und Personen, die die Daten erhalten dürfen, gehören nicht solche Empfänger, an die lediglich ausnahmsweise und auf Grund besonderer Umstände im Einzelfall Daten weitergegeben werden. In das Verzeichnis aufzunehmen sind aber solchen Stellen, an die mit einer gewissen Regelmäßigkeit in bestimmten Fällen oder bei Eintritt gewisser wiederkehrender Umstände die Daten weitergegeben werden. Zu den Empfängern gehören auch die Auftragsdatenverarbeiter; auch diese sind zu melden.

VI Geplante **Übermittlungen** an Stellen **außerhalb** der **Mitgliedsstaaten der EU**. Die Übermittlung in sog. Drittstaaten unterliegt nach § 16 Abs. 2 LDSG besonderen Voraussetzungen. Die Angaben im Verzeichnis sollen sicherstellen, dass das Vorliegen dieser Voraussetzungen nachprüfbar bleibt und dass die Beteiligung des ULD nach § 16 Abs. 3 LDSG gewährleistet ist.

VII Die Beurteilung des Verfahrens durch die **behördliche Datenschutzbeauftragte** oder den behördlichen Datenschutzbeauftragten, soweit eine solche vorliegt. Eine Beurteilung wird in der Regel im Rahmen der Vorabkontrolle nach § 9 abgegeben werden. Diese obliegt gem. § 10 Abs. 4 Nr. 5 LDSG in erster Linie der oder dem behördlichen Datenschutzbeauftragten.

VIII Die allgemeine Beschreibung der zur Einhaltung der **Datensicherheit** nach den §§ 5 und 6 LDSG getroffenen Maßnahmen. Eine solche Beschreibung ist das nach § 8 Abs. 1 der DSVO zu erstellende Sicherheitskonzept.

Verfahrensverzeichnis gem. § 7 LDSG-SH

1. **Aktenzeichen + Lfd. Nr.:**

1017/2013

2. **Name und Art des Verfahren (ggf. Versions-Nr.):**

Archivverwaltungsprogramm AUGIAS-Archiv, Client-Server-Verfahren,
V 8.3

3. **Name und Anschrift der Daten verarbeitenden Stelle (= Verfahrensanwender) [I]:**

Hansestadt Lübeck
4.415 Archiv
Mühlendamm 1-3
23539 Lübeck

4. **Zweckbestimmung des Verfahrens [II]:**

a) Aktenverwaltung: Erfassung und Verwaltung der im Stadtarchiv verwahrten Archivalien
b) Kundenverwaltung: Erfassung und Verwaltung der Kunden im Lesesaal des Archivs

5. **Rechtsgrundlage des Verfahrens:**

ohne - freiwillige Aufgabe

6. **Kreis der Betroffenen [III]:**

a) Personen, die die im Archiv verwahrten und mit AUGIAS verwalteten Akten betreffen und deren Namen in den Inhaltsangaben der Akten erwähnt werden (z.B. Personalakten)
b) Kunden des Archivs, die im Lesesaal des Archivs der Hansestadt Lübeck Recherchen durchführen

7. **Kategorien der verarbeiteten Daten [IV]:**

a) Namen und ggf. Berufsbezeichnung, Geburts- und Sterbedatum

b) Angaben zur nutzenden Person und deren Adressdaten, Forschungsvorhaben und Auftraggeber

8. **Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden [V]:**

Herkunft: a) Archivmitarbeiter, b) Kunden

Empfänger:
a) Kunden, Archivmitarbeiter
b) Archivmitarbeiter

9. Geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union [VI]:

keine

10. Datenschutzrechtliche Beurteilung des behördlichen Datenschutzbeauftragten / ULD [VII]:

Negativ, da kein behördlicher Datenschutzbeauftragter ernannt wurde.

11. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen [VIII]:

- Die HL befindet sich in einem Zertifizierungsverfahren und wird durch das ULD–SH entsprechend begleitet. Server- und Clientkonzepte sind vorhanden.

- Zugang zu Datenträgern, Servern etc.
  Der Zugang zu Servern und Datenträgern, die in einem separat gesicherten Rechenzentrum stehen, ist nur autorisierten IT-Personen erlaubt.

- Wer darf die Daten verarbeiten?
  Stamm- und Systemdaten sind der datenverarbeitenden Stelle 4.415 Archiv zugeordnet und werden von dort verwaltet.

- Protokollierung, wer, wann auf welche Daten zugegriffen hat
  Der Server protokolliert alle Zugriffe auf die Programme und Daten.
  DB-seitig (MS SQL-Server) findet keine Protokollierung statt.
  AUGIAS selbst liefert ein Löschprotokoll.

- Benutzerverwaltung
  Die datenverarbeitende Stelle regelt die Benutzerverwaltung in eigener Verantwortung. Zugriffsberechtigungen werden vom 4.415 Archiv verwaltet.

- Verschlüsselung von Daten
  Die Verarbeitung findet nicht außerhalb der Räumlichkeiten der HL statt.
  Eine Verschlüsselung der Daten ist daher nicht notwendig.

- Die Anwendung befindet sich zentral auf einem MS SQL-Server und lokal auf den Clients der Archivmitarbeiter sowie auf vier lokalen Stationen, darunter 2 Notebooks. Die PC's einschließlich der lokalen Stationen und das Verfahren sind jeweils durch Passworteingabe geschützt.

- Risikoanalyse:
  Akten- und Kundenverwaltung
  - Nur in den Räumlichkeiten des Archivs kann über die Clients auf das Verfahren zugegriffen werden.
    Die Clients werden über die AD-Richtlinie verwaltet. Standardmäßig werden nach 10 Minuten die Clients per Richtlinie gesperrt.
    Auf jedem Client befindet sich ein aktueller Virenscanner.
    Serverbetrieb findet ausschließlich im Rechenzentrum der HL statt.

- Datenbestände können auf dienstlichen mobilen Geräten unverschlüsselt abgelegt werden. Private Geräte haben keinen Zugang.
- Downloadmöglichkeiten, Datenexport
  Nur durch berechtigte Personen auf dienstlichen stationären und mobilen (drivelock gesteuerte zertifizierte USB-Sticks) Geräten.
- Zugriff extern auf Intranet
  nicht möglich

- Kundenrecherche
  - Im Lesesaal des Archivs stehen für Kunden zwei Clients zur Recherche zur Verfügung. Der Zugriff über die Funktion „Gastrecherche" ist eingeschränkt, die Freigabe von dort sichtbaren Aktentiteln erfolgt durch Archivmitarbeiter unter Beachtung datenschutzrechtlicher Bestimmungen.

12. Gespeicherte personenbezogene Daten angeben (sofern unter 6. Kategorie „Diverse" angegeben ist):