



Verfahrensverzeichnis

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

Verfahren	Mikropro Impftool
-----------	-------------------

Version: 1.0.0.5 gültig ab: 24.08.2015 bis (sofern bestimmbar): _____

1. Daten verarbeitenden Stelle:

	<i>Landeshauptstadt Kiel, Fleethörn 9 (Rathaus), 24103 Kiel</i>
Amt/Abteilung	<i>Amt für Gesundheit, Abteilung 50.2 Kinder- und jugendärztlicher Dienst</i>
Aktenzeichen	
Kontakt	<i>Fachanwendungsbetreuer/in (Key User): Nico Meinert, Tel. 901-3255 Datenschutzbeauftragter: Herr Amann, Tel. 901 2771, datenschutz@kiel.de</i>

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Zweckbestimmung	Erfassung und Auswertung von durchgeführten Impfungen in den einzelnen Gesundheitsbehörden
Rechtsgrundlage	§ 21d Abs. 3 SGB V

3. Kreis der Betroffenen:

1	Personen, an denen eine Impfung durchgeführt wird
2	

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, Geburtsdatum, Versicherungsart sind Pflichtfelder	nein
4.1.2	Vorname, Anschrift, Geschlecht, Nationalität, Krankenkasse, Versicherungsnummer, Impfstoffe sind keine Pflichtfelder	ja

zu Daten aus	4.2 Löschungs- und Aufbewahrungsfristen
Nr. 4.1.1	<i>wird geprüft</i>
Nr. 4.1.2	<i>wird geprüft</i>

zu Daten aus	4.3 Zugriffsberechtigte Personen oder Personengruppen
Nr. 4.1.1	<i>ArzthelferInnen und ÄrztInnen aus dem Bereich Abteilung 50.2, über eine Nutzerverwaltung mit Kennwort gesteuert, Mitarbeiter der zentralen IT und die Systemkoordinatoren aus dem Amt 53</i>
Nr. 4.1.2	<i>ArzthelferInnen und ÄrztInnen aus dem Bereich Abteilung 50.2, über eine Nutzerverwaltung mit Kennwort gesteuert, Mitarbeiter der zentralen IT und die Systemkoordinatoren aus dem Amt 53</i>

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

zu Daten aus	5.1 Empfänger von zu übermittelnden Daten
Nr. 4.1.1	<i>Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung für Schleswig-Holstein, ansässig in Kiel Daten werden verschlüsselt per CD übergeben</i>
Nr. 4.1.2	<i>Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung für Schleswig-Holstein, ansässig in Kiel Daten werden verschlüsselt per CD übergeben</i>

zu Daten aus	5.2 Herkunft empfangener Daten
Nr. 4.1.1	von Personen, an denen eine Impfung durchgeführt wird
Nr. 4.1.2	von Personen, an denen eine Impfung durchgeführt wird

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

Keine

Alternativ (ggf. bitte streichen)

ja	(aufgeführt in Punkt 5.1)
----	---------------------------

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-Schutzziele 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
-----	--------------------------------------

Verfügbarkeit (Verfahren und Daten stehen zeitgerecht zur Verfügung):

- › Die Daten werden regelmäßig gemäß der Datensicherungskonzeption der Landeshauptstadt Kiel gesichert. Das Verfahren wird auf zentralen Systemen gesichert.
- › Es sind 2 Laptops für mobile Impfungen in Außenstellen in Betrieb. Diese sind verschlüsselt. Die Übertragung der verschlüsselten Daten in das Hauptsystem erfolgt unmittelbar nach dem Außendienst im Büro. Nur dort ist der Zugriff auf das Hauptsystem möglich.
- › Das Verfahren kann bei einem Ausfall in einem definierten Zeitraum (Sicherheitskonzeption) wieder hergestellt werden.

Vertraulichkeit (es können nur befugte Personen auf Daten und Verfahren zugreifen):

- › 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).
- › Innerhalb des Verfahrens wird durch eine dokumentierte Berechtigungsvergabe sichergestellt, dass nur berechtigte Personen auf die Datenbestände zugreifen dürfen. Die Prüfung der Berechtigung erfolgt passwortbasiert.
- › Übermittlungen von und an Dritte erfolgen verschlüsselt.

Integrität (es wird gewährleistet, dass Daten unverändert, vollständig, zurechenbar und aktuell bleiben):

- › 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).
- › Innerhalb des Verfahrens haben nur die fachliche Administration dieses Verfahrens und die Personen, die die Datenpflege betreiben, Zugriff auf die Datenbestände (Schutz vor Veränderung durch unberechtigten Zugriff).
- › Übermittlungen von und an Dritte erfolgen verschlüsselt.

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.

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.
- › Der Auftragsdatenverarbeiter (falls vorhanden) wird regelmäßig durch die verantwortliche Stelle überprüft.
- › 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.*
- *Auf die Datenbestände des Verfahrens können ausschließlich die in Abschnitt 4.3 genannten Personengruppen zugreifen.*

9. Freigabe des Verfahrensverzeichnis

Kiel,

gezeichnet