



Verfahrensverzeichnis

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

Verfahren	Baumkataster
-----------	--------------

Version: 3.7 gültig ab: 01.09.2015 bis (sofern bestimmbar): _____

1. Daten verarbeitenden Stelle:

	<i>Landeshauptstadt Kiel, Holstenstraße 108 (Landwirtschaftskammer), 24103 Kiel</i>
Amt/Abteilung	<i>Grünflächenamt, Grünflächenverwaltung</i>
Aktenzeichen	<i>67.0.3</i>
Kontakt	<i>Fachanwendungsbetreuer/in (Key User): Karsten Breier, 901-3812, karsten.breier@kiel.de Axel Reimann, 901-3831, axel.reimann@kiel.de Datenschutzbeauftragter: Herr Amann, Tel. 901 2771, datenschutz@kiel.de</i>

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Zweckbestimmung	Baumdatenverwaltung, Erfassung Baumzustandsdaten, Dokumentation der Baumkontrollen, Wertermittlung, Historienverwaltung
Rechtsgrundlage	§11 Abs. 1 LDSG SH, allgemeine Rechtsprechung

3. Kreis der Betroffenen:

1	Nur Benutzer/innen
2	

4. Kategorien verarbeiteter Daten, Lösungs-, Aufbewahrungsfristen, Zugriffsberechtigungen

	4.1 Kategorien der verarbeiteten Daten	„Besonders sensible“ Daten gem. § 11 Abs. 3 LDSG
4.1.1	Geogr. Daten wie Baumkoordinaten, Flächen	nein
4.1.2	Baumzustandsdaten	Nein
4.1.3	Historische Baumzustandsdaten	
4.1.4	Name des erfassenden Baumkontrolleurs und Datum der Erfassung für jeden baumzustandsbezogenen Datensatz	ja (?)

zu Daten aus	4.2 Löschungs- und Aufbewahrungsfristen
Nr. 4.1.2	<i>Arbeits-Datenbestand gibt den Ist-Zustand wieder.</i>
Nr. 4.1.3	<i>Historie wird laufend ergänzt und bleibt erhalten. Löschung ist nicht vorgesehen da erforderlich zum Nachweis der Erfüllung der Verkehrssicherungspflicht.</i>
Nr. 4.1.4	<i>Löschung ist nicht vorgesehen da erforderlich zum Nachweis der Erfüllung der Verkehrssicherungspflicht.</i>

zu Daten aus	4.3 Zugriffsberechtigte Personen oder Personengruppen
Nr. 4.1.1 bis 4.1.4	<i>Baumkontrolleure mit eigenen Erfassungsgeräten und Datenkopien, Mitarbeiter der Abteilung 67.0, Grünflächenverwaltung und Grünflächeninformationssystem</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 bis 4.1.4	<i>Datenaustausch mit Erfassungsgeräten der Baumkontrolleure</i>
Nr. 4.1.2 bis 4.1.4	<i>Rechtsamt erhält bei Schadensfällen Datenauszüge als Dokument</i>

zu Daten aus	5.2 Herkunft empfangener Daten
Nr. 4.1.1 bis 4.1.4	<i>Die von Baumkontrolleuren erfassten Daten werden in einer zentralen Datenbank gesammelt.</i>
Nr. 4.1.2	

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

<i>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.</i>
--

8. Datenschutzrechtliche Beurteilung

8.1	Stellungnahme der/des Datenschutzbeauftragten (falls vorhanden)

8.2	Technisch-organisatorische Maßnahmen
<p>Verfügbarkeit (Verfahren und Daten stehen zeitgerecht zur Verfügung):</p> <ul style="list-style-type: none"> ‣ Die Daten werden regelmäßig gemäß der Datensicherungskonzeption der Landeshauptstadt Kiel gesichert. Das Verfahren wird auf zentralen Systemen gesichert. ‣ Das Verfahren kann bei einem Ausfall in einem definierten Zeitraum (Sicherheitskonzeption) wieder hergestellt werden. 	
<p>Vertraulichkeit (es können nur befugte Personen auf Daten und Verfahren zugreifen):</p> <ul style="list-style-type: none"> ‣ 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. 	
<p>Integrität (es wird gewährleistet, dass Daten unverseht, vollständig, zurechenbar und aktuell bleiben):</p> <ul style="list-style-type: none"> ‣ 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. 	
<p>Transparenz (die automatisierte Verarbeitung von Daten kann mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden):</p> <ul style="list-style-type: none"> ‣ 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. 	
<p>Intervenierbarkeit (die Daten verarbeitende Stelle kann nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht und dass Betroffene die ihnen zustehen Rechte ausüben können):</p> <ul style="list-style-type: none"> ‣ 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. ‣ ‣ Personenbezogene Daten werden ausschließlich vom erfassenden Baumkontrol- 	

leur und dem eingabebefugten Sachbearbeiter erfasst. Eine Änderung oder Löschung dieser Daten ist nicht möglich und würde der gesetzlichen Nachweispflicht zuwiderlaufen.

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

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

9. Freigabe des Verfahrensverzeichnis

Kiel,

gezeichnet