IT-PLANUNGSRAT

Hamburg
11.08.2025

Eckpunktepapier behördenübergreifende Datennutzung Teil 1

IST-Analyse behördenübergreifende Datennutzung
Kompetenzteam Datenschutz

Version	Datum	Autor:in	Aktion
1.0	11.08.2025	Kord Ellermann, Miriam von Fintel, Susan Gonscherowski, Eva Liebich, Katja Weber, Lothar Walther	Erstellung

Inhaltsverzeichnis

1 Einleitung 4

2 Management Summary 4

2.1 Proaktive Verwaltung/Push-Government 5

2.2 Datenbasierte Daseinsvorsorge 6

3 Analyse 6

3.1 Rechtliche Voraussetzung behördenübergreifender Datennutzung 7

3.1.1 Rechtsgrundlagen bestehen bereits bzw. können geschaffen werden 7

3.1.2 Zweckbindungsgrundsatz und behördenübergreifende Nutzung von Daten 9

3.1.3 Vorgangsbezogener Datenaustausch 10

3.2 Use case: Umzug mit einem gefährlichen Hund 11

3.2.1 Vergleich der Tatbestandsmerkmale 12

3.2.2 Modellierung des Antragsprozesses 15

3.2.3 Optimierung nach datenschutzrechtlichen Gesichtspunkten 16

3.2.4 Zwischenfazit 17

4 Hindernisse 19

4.1 Vorgangsbezogene Speicherung 19

4.2 Fehlende technische Interoperabilität 19

4.3 Mangelnde semantische Interoperabilität 20

4.4 Fehlende organisatorische Interoperabilität 21

4.5 Offene Fragen bezüglich der Aktualität und Validität der Daten 21

4.6 Finanzierung und Vendor-Lock-in-Effekte 22

4.7 Kritische und sensible Daten 23

4.8 Unkenntnisse über Datenschutz 23

1 Einleitung

Dieses Eckpunktepapier fasst die zentralen Ergebnisse des ehemaligen Maßnahmenclusters „Behördenübergreifende Datennutzung" des Kompetenzteams Datenschutz im Schwerpunktthema Datennutzung des IT-Planungsrates zusammen. Diese Arbeit führt im Jahr 2025 das „Thementeam Eckpunktepapier" fort.
Wir vertreten mit dem Eckpunktepapier die These, dass in Bezug auf die datenschutzkonforme, behördenübergreifende Datennutzung weniger ein Problem des Datenschutzrechts als vielmehr ein Vollzugsproblem vorliegt.
Die hier dargestellten Probleme beziehen sich vornehmlich auf den interföderalen Austausch von Verwaltungsdaten, also den Austausch zwischen Behörden über Bundesländer- und föderale Ebenengrenzen hinweg. Viele der beschriebenen Probleme betreffen jedoch – vor allem in Flächenländern - auch den Datenaustausch zwischen Gebietskörperschaften und Ebenen eines Bundeslandes. Im Bereich „Registermodernisierung" wird der behördenübergreifende Datenaustausch bereits vorangetrieben. Dies betrifft aber den Austausch von Daten, die in Verwaltungsregistern vorliegen.

Dieses Eckpunktepapier bezieht sich auf sonstige Verwaltungsdaten, die nicht in Registern, sondern beispielsweise in E-Akten und Fachverfahren vorliegen bzw. gespeichert sind. Der Teil I beinhaltet eine Ist-Analyse, die Hindernisse beschreibt, an denen typischerweise ein Datenaustausch zwischen Behörden scheitert. In einem Teil II, der voraussichtlich Ende 2025 veröffentlicht wird, werden Maßnahmenvorschläge erläutert, die zur Lösung der beschriebenen Probleme beitragen können. Das Eckpunktepapier nähert sich der Problemanalyse und -lösung über einen datenschutzrechtlich geprägten Blickwinkel an.

2 Management Summary

Im Rahmen der im KT Datenschutz durchgeführten Analyse zeigte sich, dass es im Kontext der behördenübergreifenden Datennutzung vorrangig ein Vollzugsproblem und kein normatives (also rechtliches) Defizit gibt. Die bestehenden (datenschutz-)rechtlichen Handlungsspielräume werden derzeit nicht ausgeschöpft. Der bestehende datenschutzrechtliche Rechtsrahmen stellt sicher, dass

1. ein Erlaubnisvorbehalt durch bestehende Rechtsgrundlagen übergreifend gewährleistet ist,
2. der Zweckbestimmungsgrundsatz einem behördenübergreifenden Datenaustausch nicht entgegensteht und
3. Datenübermittlungen und -abrufe zwischen öffentlichen Stellen – auch automatisiert – möglich sind, ohne dass ein Legitimitätsdefizit im datenschutzrechtlichen Sinne entsteht.

Mithin sind die Kernanforderungen einer datenschutzkonformen, behördenübergreifenden Datennutzung erfüllt bzw. mit den der Verwaltung zur Verfügung stehenden Mitteln erfüllbar. Da es keine normativen Gründe gibt, die einer datenschutzkonformen behördenübergreifenden Datennutzung endgültig im Wege stehen, ist davon auszugehen, dass die Gründe hierfür im Vollzug der Regelungen liegen. Dafür spricht auch, dass es in der Diskussion über behördenübergreifende Datennutzung an konkreten Beispielen fehlt, die den mangelnden Datenaustausch belegen. Der Nutzen eines behördenübergreifenden Datenaustausches ist weithin bekannt. Oft genannt werden die Vorteile, die unmittelbar für den einzelnen Verwaltungsvorgang greifbar sind, nämlich dass

- Informationen ebenen- oder organisationsübergreifend zur Verfügung gestellt werden;
- Informationen maschinenlesbar und automatisiert verarbeitet werden können;
- Informationen, die der Verwaltung bereits bekannt sind, nicht erneut erhoben werden müssen (Once-Only-Prinzip);
- Fehler auf Grund von fehlenden, unvollständigen oder falschen Informationen minimiert werden;
- Fälle/Vorgänge verlustfrei von einer Zuständigkeit in eine andere (perspektivisch automatisiert) übergeben werden können.

Zudem liegt in der behördenübergreifenden, interföderalen Datennutzung Potential für neue Handlungsformen der Verwaltung über den einzelnen Verwaltungsvorgang hinaus: Die Möglichkeiten der proaktiven Verwaltung und der datenbasierten Daseinsvorsorge.

2.1 Proaktive Verwaltung/Push-Government

Perspektivisch ist denkbar, dass im Rahmen einer behördenübergreifenden Datennutzung proaktives Verwaltungshandeln ermöglicht bzw. vereinfacht wird. Proaktive Verwaltung ist

dadurch gekennzeichnet, dass sie Bürgern und Unternehmen Verwaltungsleistungen eigeninitiativ im Voraus (proaktiv) anbietet.

Ein mögliches Szenario wäre die Übernahme von bereits ergangenen Verwaltungsakten nach einem Umzug durch die neu zuständige Behörde. Zum Beispiel könnten Wohngeldbehörden nach einem Wohnortwechsel alle bereits vorliegenden Informationen übernehmen, um einen möglichen Folgeantrag zu initiieren. Darüber hinaus wäre proaktives Verwaltungshandeln dadurch denkbar, dass eine stärkere Verknüpfung von Leistungs- und Förderverwaltung etabliert wird. Im Rahmen der Einschulung könnten Schulen nicht nur die schulpflichtigen Kinder bei den Meldebehörden erfragen, sondern im Anschluss den Sozialämtern die neu schulpflichtigen Kinder melden. Die Sozialämter könnten aus den Informationen zu den Schulanfängern für Bildungs- und Teilhabepaket-berechtigte Kinder direkt Unterstützungen und Zuschüsse für Erstausstattungen sowie Klassenfahrten etc. initiieren und an die Schulen übermitteln. Die Schulen als unmittelbare Ansprechstellen für die Eltern könnten bereits mit Schulstart die erforderlichen Anträge einleiten, sodass alle Informationen fristgerecht vorliegen und Anträge darüber hinaus frühzeitig bearbeitet werden.

2.2 Datenbasierte Daseinsvorsorge

Eine behördenübergreifende Datennutzung kann auch die Daseinsvorsorge durch Behörden unterstützen, indem vorliegende Verwaltungsdaten anonymisiert nachgenutzt werden, um die Daseinsvorsorge zu steuern und Mängel vorherzusehen bzw. diesen vorzubeugen. Indem Daten, die in verschiedenen Verwaltungsverfahren erhoben wurden, zusammengeführt und anonymisiert werden, könnte ein höherer Erkenntnisgewinn geschaffen werden. Denkbar sind sogar datenbasierte Prognose- und Entscheidungsassistenzen, die aufgrund von in verschiedenen Behörden gesammelten Daten die intelligente Nutzung von Daten ermöglichen.

3 Analyse

Um zu eruieren, warum die interföderale Datennutzung trotz der evidenten Vorteile in vielen Fällen nicht stattfindet, hat das Kompetenzteam Datenschutz eine Ist-Analyse der Möglichkeiten des interföderalen Datenaustausches anhand eines Fallbeispiels durchgeführt: des Umzugs eines Hundehalters von Hamburg nach Schleswig-Holstein, dessen Hund in Hamburg als gefährlich eingestuft wurde.

Das Halten und Führen gefährlicher Hunde unterliegt in Deutschland strengen gesetzlichen Regelungen, die je nach Bundesland variieren. Hundehalter:innen, die ihren Wohnsitz von

einem Bundesland in ein anderes verlegen, müssen oft die Erlaubnis für das Halten gefährlicher Hunde neu beantragen. Im dynamischen Lebensalltag stellt der Umzug von einem Bundesland in ein anderes eine Realität von Bürger:innen dar. Insbesondere für Hundehalter:innen von gefährlichen Hunden, bringt dies zusätzliche bürokratische Hürden mit sich. These war, dass die unterschiedlichen Regelungen und Antragsverfahren in den Bundesländern zu Doppelarbeit und einem unnötig hohen Verwaltungsaufwand führen. Zentrale Fragestellung war, ob bzw. wie der erneute Antragsprozess und dessen Prüfung durch einen interföderalen Datenaustausch vereinfacht werden kann (auch und insbesondere in datenschutzrechtlicher Hinsicht).

3.1 Rechtliche Voraussetzung behördenübergreifender Datennutzung

Häufig wird vermutet, „der Datenschutz" sei der Verhinderer von behördenübergreifendem Datenaustausch. Dabei verhindert der bestehende Rechtsrahmen die Datenaustausche nicht grundsätzlich/nachhaltig, denn etwaige notwendige Anpassungen können in den jeweiligen Fachgesetzen erfolgen.

3.1.1 Rechtsgrundlagen bestehen bereits bzw. können geschaffen werden

Zentrales Prinzip des deutschen und europäischen Datenschutzrechtes ist das **Verbot mit Erlaubnisvorbehalt**, d.h. personenbezogene Daten dürfen nur dann verarbeitet werden, wenn deren Verarbeitung von einer hinreichenden Rechtsgrundlage abgedeckt ist. Diese muss rechtsstaatlichen und datenschutzrechtlichen Anforderungen genügen.

Eine **Rechtsgrundlage** der Weiterverarbeitung durch die Behörde, die Daten empfängt, besteht ebenfalls, denn die Nutzung der übermittelten Daten im jeweiligen behördlichen Kontext ist bereits **durch die jeweilige Zuständigkeit sowie den Aufgabenbereich** der jeweiligen Behörde legitimiert. Jede Behörde verarbeitet die personenbezogenen Daten, die sie für die Erfüllung ihrer Aufgaben benötigt im Bereich der ihr durch Gesetz zugewiesenen Zuständigkeit. Die Datenverarbeitung im Rahmen der Aufgabenerfüllung der jeweiligen Behörde und damit der jeweilige Zweck der Verarbeitung sind durch Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit dem jeweiligen Fachgesetz erlaubt. Eine gem. Art. 6 DSGVO erforderliche **Rechtsgrundlage für die Übermittlung** personenbezogener Daten zwischen öffentlichen Stellen im Allgemeinen ist meist entweder in den Landesdatenschutzgesetzen, im Bundesdatenschutzgesetz oder in den jeweiligen Verwaltungsverfahrensgesetzen geregelt. Diese werden ergänzt durch spezialgesetzliche Regelungen, insbesondere im Kontext der Weiterverarbeitung besonderer Kategorien personenbezogener Daten.

Doppeltür-Rechtsprechung BVerfG: Demnach muss der Gesetzgeber nach dem Bild einer Doppeltür sowohl für die Übermittlung von Daten durch eine Behörde als auch für den Abruf dieser Daten durch eine andere Behörde jeweils verhältnismäßige Rechtsgrundlagen schaffen. Übermittlungs- und Abrufregelungen müssen die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen. Denn im Datenaustausch erfolgen korrespondierende Eingriffe durch Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, sowohl nur die Tür zur Übermittlung von Daten öffnen, als auch die Tür zu deren Abfrage.

Die bestehenden Rahmenbedingungen bieten bereits einen weiten Spielraum in Bezug auf die behördenübergreifende Datennutzung. Sowohl die Erhebung durch Mitteilung und Übermittlung durch andere öffentliche Stellen in Ergänzung zur Direkterhebung, als auch das Ersuchen bei anderen Stellen durch eine zuständige Behörde wird meist bereits durch das anwendbare LDSG oder das BDSG ermöglicht. Regelungen wie § 5 Abs. 5 LDSG SH stellen darüber hinaus klar, unter welchen Bedingungen ein automatisierter Abruf personenbezogener Daten möglich ist. Hier treffen die datenhaltende Stelle keine Prüfpflichten hinsichtlich der Weiterverarbeitung mehr, sondern die abrufende Stelle allein ist für die Legitimität und Rechtmäßigkeit der Weiterverarbeitung verantwortlich. Ähnliche Regelungen finden sich auch in anderen Landesdatenschutzgesetzen oder im Bundesdatenschutzgesetz (vgl. § 25 BDSG, Art. 5 Abs. 4 BayDSG). Dabei beachten diese Normen auch die sog. Doppeltür-Anforderungen des BVerfG[1].

Nach dem Bundesverwaltungsgericht[2] können aufgrund von Generalklauseln in Verbindung mit den - nicht spezifisch datenschutzrechtlichen - Regelungen des jeweiligen Fachrechts Datenverarbeitungen mit geringer Eingriffsintensität, die zur Erfüllung von Aufgaben im öffentlichen Interesse erforderlich sind, gestützt werden. In dem seitens des BVerwG entschiedenen Fall betraf dies die Erhebung, Speicherung und Verwendung der Postanschrift der eine Auskunft begehrenden Person durch das Bundesinnenministerium zwecks Beantwortung dieser Auskunft.

Sofern diese geringe Eingriffsintensität aber überschritten ist, bedarf es allerdings der Schaffung fachspezifischer datenschutzrechtlicher Rechtsgrundlagen:

[1] BVerfG, Urteil vom 24.01.2012; AZ. 1 BvR 1299/05.
[2] BVerwG, Urteil vom 20.03.2024; AZ 6 C 8.22.

Steht der Gesetzgeber vor der Notwendigkeit, neue **Rechtsgrundlagen schaffen**, ist vorab zu prüfen, welche Rechtsgrundlagen im jeweiligen Fachrecht ergänzt werden könnten bzw. sollten, um einen Datenaustausch zu erleichtern und Rechtssicherheit für die Anwendenden herzustellen. Hierzu zählen insbesondere **Übermittlungsbefugnisse** oder eine **Abruferlaubnis** in den jeweiligen Fachgesetzen. Hierdurch wird der Arbeitsschritt der Prüfung der Rechtmäßigkeit im Einzelfall vor die Klammer gezogen und für die Zwecke des jeweiligen Fachgesetzes erlaubt.

Da im Kontext von Verwaltungsdaten regelmäßig bereits Rechtsgrundlagen für deren Verarbeitung vorliegen, bietet es sich an, diese jeweils um **Regelungen zur behördenübergreifenden Datennutzung zu ergänzen** und wie in ErwG 50 der DSGVO vorgeschlagen wird, die Aufgaben und Zwecke näher zu bestimmen, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird.
In der **Eingriffsverwaltung** muss eine solche proaktive bzw. antizipierende Datenverarbeitung jedoch an höhere Voraussetzungen geknüpft sein. Denn die Auswirkung des Verwaltungshandelns ist nicht Teilhabe und Begünstigung, sondern den Bürgerinnen und Bürgern wird ein Tun, Handeln oder Unterlassen abverlangt, was mindestens einen Eingriff in Art. 2 Abs. 1 GG bedeutet. Das heißt nicht, dass in der Eingriffsverwaltung ein Datenaustausch per se unmöglich ist. Gerade hier sind **klare rechtliche Regelung erforderlich**, welche Daten unter welchen Voraussetzungen mit wem geteilt werden sollen, um den verfassungsrechtlichen Anforderungen an Eingriffsgrundlagen Genüge zu tun.

Rechtsgrundlagen für Datenaustausche existieren oder können geschaffen werden.

3.1.2 Zweckbindungsgrundsatz und behördenübergreifende Nutzung von Daten

Eine solche Anforderung ist der **Zweckbindungsgrundsatz** aus Art. 5 Abs. 1 Buchst. b DSGVO. Personenbezogene Daten, die im Kontext einer Verwaltungsleistung erhoben werden, dürfen nur in einem anderen Kontext, d.h. zu anderen Zwecken durch eine andere Behörde weiterverarbeitet werden, wenn diese Zwecke mit dem ursprünglichen Zweck vereinbar sind. Eine „Generalermächtigung" zur behördenübergreifenden Datennutzung ist vor dem Hintergrund europäischer und deutscher Grundrechte daher keine Option.
Sollen personenbezogene Daten weiterverarbeitet werden, ist die Vereinbarkeit der Zwecke der Verarbeitung vorab eindeutig festzustellen. Da der Verarbeitungsbegriff im europäischen Datenschutzverständnis neben der Erhebung auch die Übermittlung und die Weiterverarbeitung von Daten umfasst, stellt sich nun die Frage, ob Behörde 1 legitimer Weise Daten an Behörde 2 übermitteln darf bzw. ob Behörde 2 legitimer Weise die benötigten Daten von

Behörde 1 abrufen darf. Diese datenschutzrechtliche Anforderung scheint zunächst eine Herausforderung zu sein, denn im Kontext der behördenübergreifenden Datennutzung ist zunächst einmal von einer Vielzahl möglicher Nutzungszwecke auszugehen.
Einem behördenübergreifenden Datenaustausch steht dies jedoch nicht entgegen. Im Kontext der Leistungsverwaltung kann die **Vereinbarkeit der Zwecke** u. a. daraus **abgeleitet werden, dass die jeweils benötigten Angaben ohnehin im Rahmen des Antrags beigebracht werden müssen, da eine Bearbeitung sonst nicht möglich ist**. Hinzu kommt, dass die Weiterverarbeitung bereits vorliegender personenbezogener Daten im Interesse der Betroffenen ist, welche die Daten bei den zuständigen Stellen nicht einholen müssen, sich weitere Antragsverfahren sparen und auch die Zustellungs- und Übermittlungszeiten sich verkürzen. Eventuell entfallen sogar Verwaltungsgebühren für die Betroffenen. Die Antragstellenden müssen nur die Daten zum Verfahren beisteuern, die der Verwaltung nicht bekannt sind. Dieser Ansatz wird auch in Erwägungsgrund (ErwG) 50 DSGVO erläutert. Hier wird ausdrücklich darauf verwiesen, dass „[d]ie Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, nur zulässig sein [sollte], wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten."

Der Zweckbindungsgrundsatz erlaubt die behördenübergreifende Datennutzung.

3.1.3 Vorgangsbezogener Datenaustausch

Dass Verwaltungsdaten nicht bereits behördenübergreifend genutzt werden, ist daher auf weitere Faktoren zurückzuführen.
Verwaltungsdaten werden derzeit aus den Fachverfahren kommend vorgangsbezogen in E-Akten (oder analogen Akten) gespeichert. Da die E-Akte in der Regel pdf-Dokumente abspeichert, können aus ihr einzelne Daten ohne entsprechende Vor- oder Aufbereitung der Datei nicht isoliert anderen Behörden verfügbar gemacht werden. Eine Bereitstellung der gesamten E-Akte, wenn die andere Behörde nur ein einzelnes Datum verwenden muss, steht jedoch im **Konflikt mit dem Grundsatz der Datenminimierung** (Art. 5 Abs. 1 Buchstabe c DSGVO) und bedeutet vermeidbaren Bürokratieaufwand.
Die Möglichkeit eines flächendeckenden Datenaustauschs ist daher nur gegeben, wenn Daten im Verwaltungsverfahren in einer **datenbasierten** statt dokumenten-basierten Form bereitgestellt werden. Derzeit werden Daten in Verwaltungsverfahren vorgangsbezogen gespeichert und ggf. im Wege der Amtshilfe bereitgestellt. Beispielsweise wird das Datum, dass ein

gefährlicher Hund einem Wesenstest unterzogen wurde, derzeit in Bezug auf ein konkretes Verfahren zur Erlaubniserteilung für das Halten und Führen gefährlicher Hunde bei einer konkreten Behörde für einen konkreten Halter gespeichert.
In der derzeitigen Ausgestaltung ist es daher ungleich schwieriger, aus (menschenlesbaren) Dokumenten die für die Datennutzung benötigten Daten zu extrahieren und in nutzbare Datenformate umzuwandeln. Bildlich gesprochen lassen sich aus Eiern und Milch sowohl Pfannkuchen als auch Omeletts zubereiten. Aus einem Omelett die Zutaten für Pfannkuchen herauszuarbeiten ist hingegen mit einem enormen Ressourceneinsatz verbunden, ohne dass es eine Garantie für ein verwertbares Ergebnis gibt.
Hinzu kommt, dass ein großer Anteil der Verwaltungsdaten in den E-Akten derzeit als textbasierte unstrukturierte Informationen (z. B. PDFs) vorliegen. Diese sind oft nicht maschinenlesbar und – wenn überhaupt – nur umständlich nutzbar zu machen.

Der vorgangsbezogene Datenaustausch ist datenschutzrechtlich problematisch.

3.2 Use case: Umzug mit einem gefährlichen Hund

Um zu untersuchen, wie der **interföderale Datenaustausch** stattfinden kann und wo Hürden bestehen, hat das KT Datenschutz als **Use Case** den Umzug von Hamburg nach Schleswig-Holstein mit einem in Hamburg als gefährlich eingestuften Hund analysiert. Der Use Case wurde ausgewählt, weil die Hundegesetze in beiden Bundesländern unterschiedlich aufgebaut und geregelt sind und es sich um einen alltäglichen Sachverhalt handelt, der einen praktischen Bürger:innenbezug hat. Zudem ist die Regulierung von Hunden ein Rechtsgebiet, das in Anforderungen und Vollzug bisher nicht durch Bundes- oder EU-Recht harmonisiert ist. Das KT Datenschutz hat hier besonders viele typische Hürden der datengestützten interföderalen Zusammenarbeit vermutet.
Das KT Datenschutz hat geprüft, welche Angaben die Behörde in Schleswig-Holstein benötigt, damit eine **Haltererlaubnis für einen gefährlichen Hund**, die von einer Hamburger Behörde ausgestellt wurde, anerkannt werden kann.

3.2.1 Vergleich der Tatbestandsmerkmale

Hierzu hat das KT Datenschutz zunächst die gesetzlichen Voraussetzungen verglichen, indem die Erlaubnistatbestände modelliert wurden:

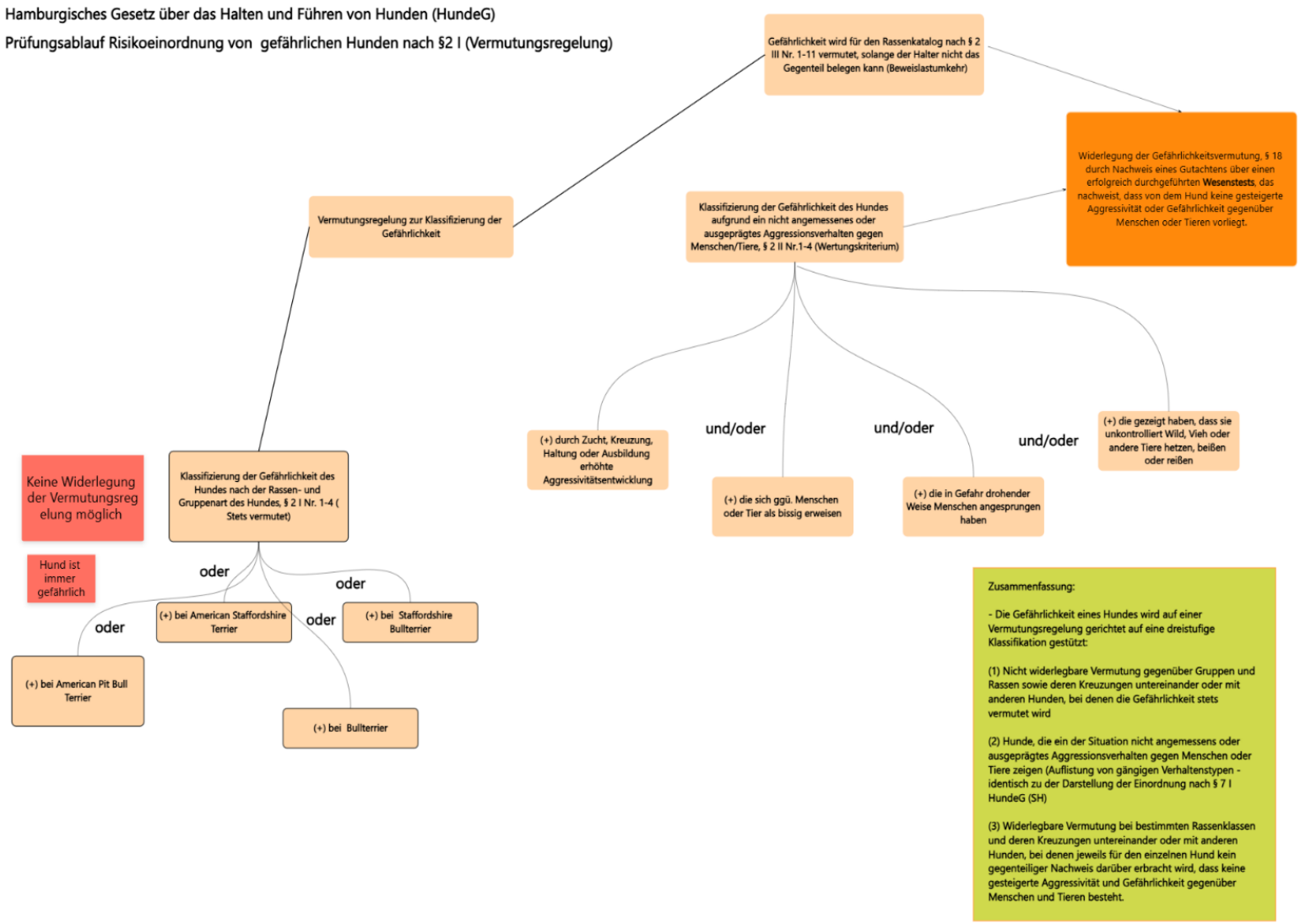


Abbildung 1: Hamburgisches Gesetz über das Halten und Führen von Hunden

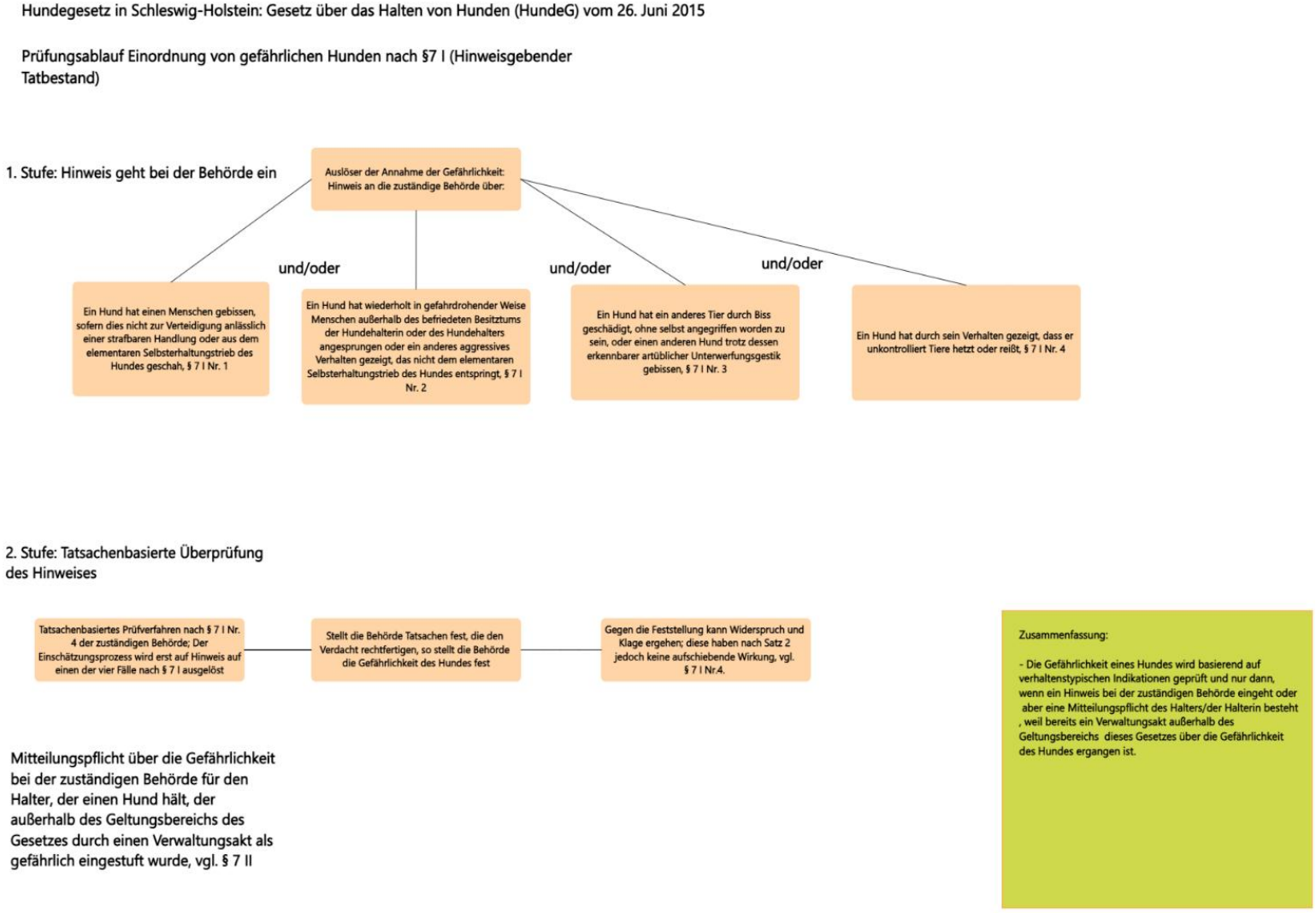


Abbildung 2: Gesetz über das Halten von Hunden Schleswig-Holstein

Das Hamburger Hundegesetz stuft Hunde sowohl verhaltensabhängig als auch verhaltensunabhängig als gefährlich ein, das Schleswig-Holsteinische Hundegesetz Hunde nur aufgrund vorangegangenen aggressiven Verhaltens. Daher hat sich das KT Datenschutz auf die Einstufung der Gefährlichkeit aufgrund des Verhaltens des Hundes konzentriert und die gesetzlichen Tatbestände und Tatbestandsmerkmale für eine Erteilung der Haltererlaubnis analysiert:
So wird die Gefährlichkeit in Hamburg angenommen, wenn ein Hund ein der Situation nicht angemessenes oder ausgeprägtes **Aggressionsverhalten** gegen Menschen oder Tiere zeigt. Dass der Hund dies nicht aufweist und somit nicht gefährlich ist, kann durch einen **Wesenstest** nachgewiesen werden. Ferner gibt es in Hamburg eine **Gehorsamsprüfung**, wodurch die Person nachzuweisen hat, dass sie den Hund im Alltag unter Kontrolle hat und so halten und führen kann, dass von ihm voraussichtlich keine Gefahren oder erheblichen Belästigungen für Menschen, Tiere oder Sachen ausgehen.
In Schleswig-Holstein gilt ein Hund als gefährlich und seine Haltung bedarf der Erlaubnis, wenn er durch **aggressives Verhalten** gegenüber Menschen und anderen Tieren aufgefallen ist. Um die Erlaubnis zu erhalten, muss der Halter eine **Sachkundeprüfung** ablegen über seine Kenntnisse und Fähigkeiten, den Hund so zu halten und zu führen, dass von diesem voraussichtlich keine Gefahr für die öffentliche Sicherheit ausgeht.

Die jeweiligen Tatbestandsmerkmale heißen also unterschiedlich, haben aber einen ähnlichen Inhalt, auch wenn dies auf den ersten Blick nicht immer offensichtlich ist. In den Landesgesetzes werden die Tatbestandsmerkmale unter **unterschiedlichen Begriffen** geprüft, auch wenn sie **inhaltlich weitgehend kongruent** sind.

3.2.2 Modellierung des Antragsprozesses

Anschließend hat das KT Datenschutz anhand der unterschiedlichen gesetzlichen Anforderungen den **Antragsprozess modelliert**. Teil dieses Prozesses wäre die Übermittlung der Akte aus Hamburg. Dieser Prozess umfasst eine Vielzahl an aus Hamburg übermittelten Daten, die für das Verfahren in Schleswig-Holstein nicht von Belang wären. Das betrifft insbesondere mögliche verhaltensunabhängige Gründe, derentwegen ein Hund in Hamburg als gefährlich eingestuft wurde. Diese Daten sind in Schleswig-Holstein jedoch von Gesetzes wegen nicht zu beachten. Das bloße Übermitteln der Information, dass der Hund in Hamburg als gefährlich eingestuft wurde, wäre an sich daher nicht ausreichend, da die Anforderungen voneinander abweichen (s.o.). Hundehalter:innen, deren Hund in Hamburg durch die Rasse als gefährlich eingestuft wurden, ansonsten aber nicht auffällig geworden sind, brauchen in Schleswig-Holstein gar keinen Antrag stellen, weil ihr Hund dort nicht genehmigungspflichtig ist.

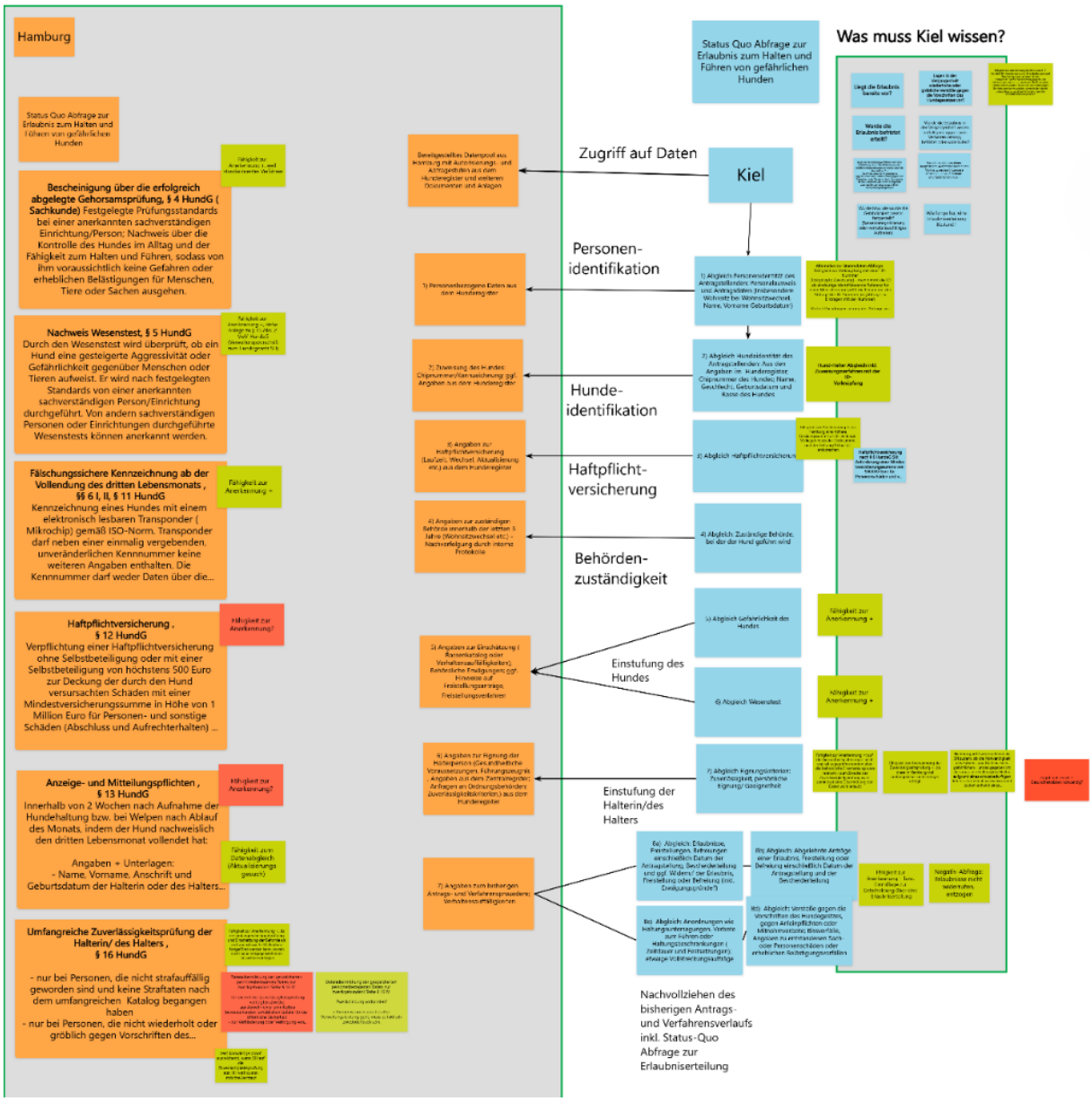


Abbildung 3: Modellierung Antragsprozess

3.2.3 Optimierung nach datenschutzrechtlichen Gesichtspunkten

Diesen Prozess hat das KT sodann nach **datenschutzrechtlichen Gesichtspunkten optimiert**, sodass möglichst wenige personenbezogene Daten ausgetauscht werden müssen und diese möglichst spät im Prozess übermittelt werden. Hierzu wurde modelliert, dass die Verwaltungsdaten nicht gesammelt in einer Akte übermittelt werden, sondern nur bestimmte einzelne Daten, die für das konkrete Verfahren von Belang sind.

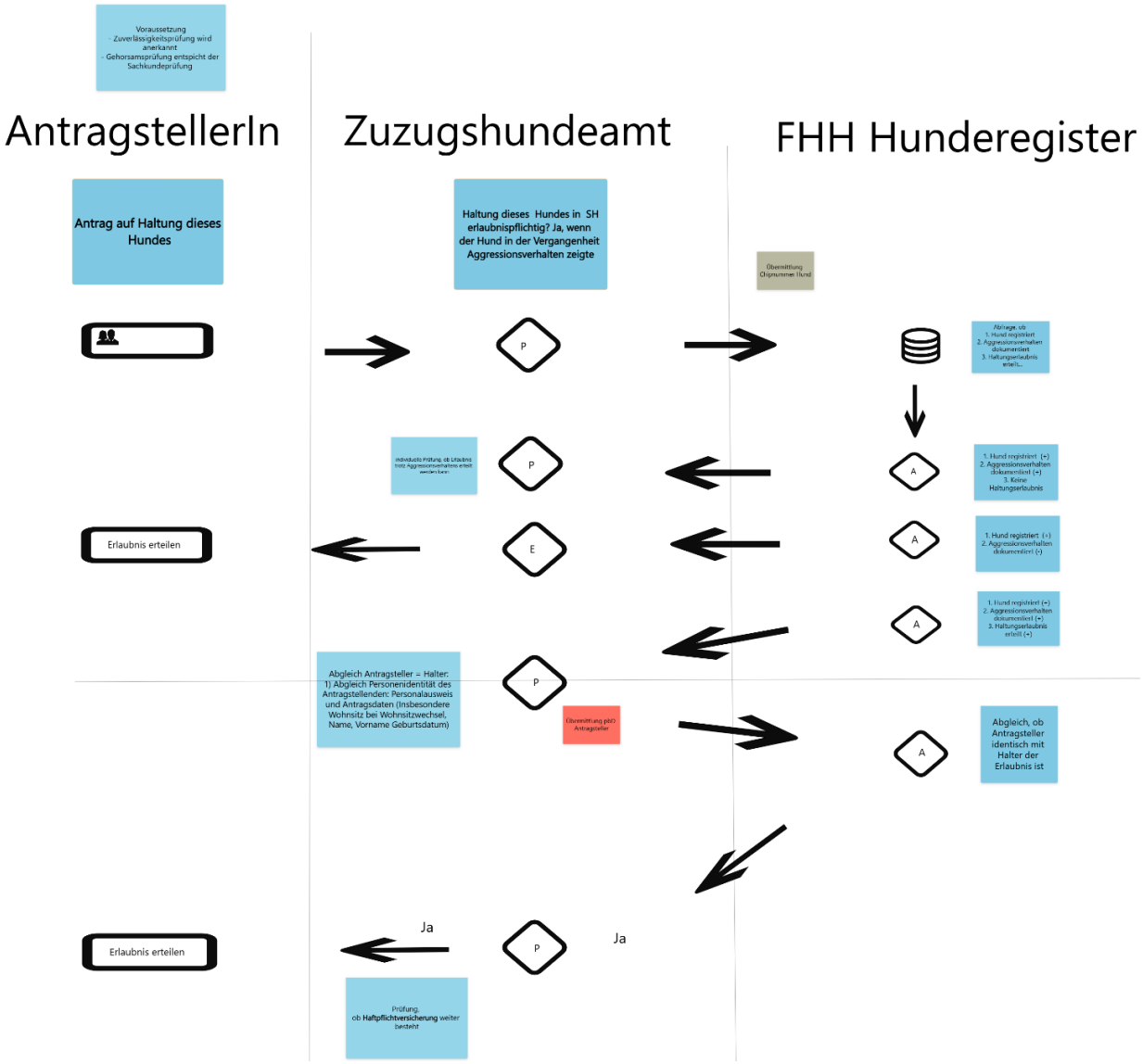


Abbildung 4: Optimierung nach datenschutzrechtlichen Gesichtspunkten[3]

3.2.4 Zwischenfazit

Key Learning dieser Prozessoptimierung war, dass der interföderale Datenaustausch im Sinne des Grundsatzes der Datenminimierung optimiert werden könnte, wenn Verwaltungsdaten einzeln ausgetauscht werden könnten. Um Optimierung zu erreichen, ist ein **Verständnis** der erforderlichen Daten und damit der **Tatbestände** in den jeweiligen Gesetzen Grundvoraussetzung. Dieses Verständnis muss sich sodann auch auf die konkrete Bedeutung der auszutauschenden Daten beziehen. Nur durch die Herstellung von **semantischer Interoperabilität**

[3]Diese Grafik finden Sie im Großformat auch im Anhang.

können die Verwaltungsdaten so ausgetauscht werden, dass die datenempfangende Behörde die Bedeutung der übermittelten Daten versteht und in ihrem Verfahren übernehmen kann.
Wäre die datenfeldbezogene Speicherung in der Verwaltung umgesetzt, stellt sich die Frage, wie der Prozess des Datenaustausches optimal gestaltet werden kann. Im Zuge der Analyse des Fallbeispiels Hundegesetze Hamburg und Schleswig-Holstein hat sich herausgestellt, dass durch eine kluge Strukturierung des Datenaustausches die Verarbeitung von personenbezogenen Daten im Sinne der Datenminimierung vermieden oder zumindest stark reduziert werden kann. So ist es bei einem datenfeldbezogenen Austausch von Daten möglich, zunächst nur nicht personenbezogenen Daten auszutauschen und nur bei einer positiven Prüfung und weiterem Bedarf auch die personenbezogenen Daten auszutauschen.

Im Beispiel des Hundegesetzes könnten so bei einem Umzug des Halters eines gefährlichen Hundes von Hamburg nach Schleswig-Holstein im Zuge der Antragsbearbeitung zunächst nur Informationen über den betreffenden Hund von Hamburg nach Schleswig-Holstein übermittelt werden, um eine mögliche Übernahme der Ergebnisse der Antragsbearbeitung in Hamburg zu prüfen. Dabei könnte zunächst abgefragt werden, ob der Hund in der Vergangenheit Aggressionen gezeigt hat. Denn im Unterschied zu Hamburg gelten in Schleswig-Holstein nur solche Hunde als gefährlich und sind damit erlaubnispflichtig. Um dieses Tatbestandsmerkmal zu prüfen, sind keinerlei personenbezogenen Daten erforderlich. Eine Prüfung von personenbezogenen Daten wäre erst später, im Zuge des Abgleichs der Identität des Antragsstellers mit der Identität des Inhabers der Hamburger Haltererlaubnis, erforderlich.

> In ähnlicher Weise könnte auch der Prozess des Datenaustausches in anderen Anwendungsfällen so optimiert werden, dass dem Grundsatz der Datenminimierung entsprechend nur die erforderlichen Daten ausgetauscht werden.

Erforderlich hierfür sind zum einen vertiefte Kenntnisse über das anwendbare Fachrecht und die Begriffsbedeutung in diesem (s.o.). Zum anderem muss bekannt sein, ob ein bestimmtes Datenfeld personenbezogen Daten enthält oder ob die Daten ggf. aus Geheimschutz- oder ähnlichen Gründen kritisch sind.
Dass ein behördenübergreifender Datenaustausch trotzdem nicht bereits flächendeckend und systematisch stattfindet, ist auf die diffuse Gemengelage zurückzuführen, in welcher Verwaltungsdaten derzeit verarbeitet werden.

4 Hindernisse

Die Analyse anhand des use cases hat gezeigt, dass es einige Anhaltspunkte gibt, an denen ein behördenübergreifender Datenaustausch scheitert:

4.1 Vorgangsbezogene Speicherung

Ein Problem, dass der vorgangsbezogene Datenaustausch zwischen Verwaltungseinheiten nicht datenminimiert stattfinden kann, ist die fehlende **datenfeldbezogenen Speicherung** und dass ein datenfeldbezogener Austausch von Verwaltungsdaten nicht möglich ist.

Gemeint ist, dass Verwaltungsdaten nicht nur vorgangsbezogen zu Dokumentationszwecken in einem pdf-Dokument in der E-Akte abgelegt werden, sondern in einer **Struktur**, die einer Datenbank ähnelt. Einzelne Informationen könnten so gezielt angesteuert und ausgetauscht werden.
So müsste im Beispielsfall „Datenaustausch wegen des Umzugs eines Halters eines gefährlichen Hundes von Hamburg nach Schleswig-Holstein" nicht die gesamte (E-)Akte oder ein gesamten Schriftstück in einer Akte ausgetauscht werden, sondern nur diejenigen spezifischen Daten, die für die Antragsbearbeitung in Schleswig-Holstein relevant sind. Dies wäre im Sinne der Datenminimierung wesentlich datenschutzfreundlicher.

Eine vorgangsbezogene Speicherung ist datenschutzrechtlich problematisch im Hinblick auf Datennutzung und Datenaustausche.

4.2 Fehlende technische Interoperabilität

Selbst wenn eine Verwaltungseinheit eine datenfeldbezogene Speicherung und Abrufbarkeit anbieten könnte, müsste die interessierte Stelle auch in der Lage sein, diese Daten anzunehmen. **Interoperabilität** ist die Fähigkeit unabhängiger, heterogener Systeme, nahtlos zusammenzuwirken, um Daten auf effiziente und verwertbare Art und Weise auszutauschen bzw. dem Benutzer zur Verfügung zu stellen, ohne dass dazu besondere Adaptierungen notwendig sind. Anders als an Rechtsgrundlagen scheitert der interföderale Datenaustausch in der Praxis oft an der fehlenden Interoperabilität der Systeme.
Die heterogene IT-, Daten- und Prozesslandschaft in der öffentlichen Verwaltung wird dem Bedarf einheitlicher Datenformate, Datenbeschreibungen und standardisierter Schnittstellen, um über Bundesländer- und Ebenengrenzen hinweg eine Datennutzung zu gewährleisten, oftmals nicht gerecht.
Dabei könnten solche Datenformate sowie portable Softwareprodukte und Services, die auf gemeinsamen Standards beruhen, eine Datennutzung ermöglichen, ohne dass die Möglichkeit,

die jeweils benötigten Dokumente zu generieren, beschnitten wird. Ein Praxisbeispiel für dieses Vorgehen sind eRechnungen, die inzwischen nach dem **Standard xRechnung** erstellt werden. Das xml-Format ermöglicht Visualisierungen in unterschiedlichen Formen und gleichzeitig eine automatisierte Verarbeitung in Buchhaltungssystemen (z. B. SAP). Auch für Verwaltungsdaten werden mit **FIM** bzw. **XÖV** solche einheitlichen und offenen Standards entwickelt.

Bestehende Standards werden ignoriert und nicht umgesetzt.

4.3 Mangelnde semantische Interoperabilität

Selbst wenn die Verwaltungsdaten technisch datenfeldbezogen gespeichert und bereitgestellt werden können, hat die Analyse des Use Case Hundegesetze ergeben, dass ein behördenübergreifender Datenaustausch nur dann gewinnbringend ist, wenn die Daten auch **semantisch interoperabel** nutzbar wären.

Die semantische Interoperabilität beschreibt konkret die Fähigkeit unterschiedlicher Systeme, Informationen nicht nur korrekt auszutauschen, sondern diese auch so zu **interpretieren**, dass ihre **zugrunde liegende Bedeutung erhalten** bleibt.

Die Analyse des Use Cases hat ergeben, dass die Anforderung für die Erlaubniserteilung in den beiden Bundesländern zum Teil inhaltlich voneinander abweichen. Zum Teil werden Begriffe in unterschiedlichem Sinne verwendet. So verlangen beide Bundesländer eine Haftpflichtversicherung des Halters, die erforderlichen Mindestdeckungssummen weichen jedoch voneinander ab. Würde nun die zuständige Stelle in Schleswig-Holstein nach dem Umzug des Halters in Hamburg lediglich abfragen, ob eine Haftpflichtversicherung vorliegt, könnte sie diese Information in ihrem Verwaltungsverfahren daher nicht nutzen (weil sie einen unterschiedlichen Inhalt haben).

Zur effizienten Nachnutzung der Daten aus der Erlaubniserteilung in Hamburg in Schleswig-Holstein wäre daher eine **semantische Harmonisierung** erforderlich, um einen gewinnbringenden Datenaustausch zu ermöglichen.

Die Herausforderung im interföderalen Datenaustausch liegt darin, dass rechtliche Anforderungen oft spezifische Formulierungen, wertungsbezogene Begriffe mit Ermessensspielraum und/oder eine gewisse Interpretations-/Auslegungsoffenheit enthalten, die je nach Bundesland variieren. Diese Unterschiede machen eine direkte semantische Vergleichbarkeit schwierig und erfordern eine tiefergehende Analyse der faktischen Ausgangsbedingungen und systematischen Grundlagen von Rechtsnormen und deren Integration. Es fehlt also an der semantischen Interoperabilität.

Zur digitalen Operationalisierung gesetzlich verankerter Datenverarbeitungen ist es notwendig, semantische Interoperabilität sicherzustellen, indem Legaldefinitionen gleichlautender Rechtsbegriffe vereinheitlicht werden.

4.4 Fehlende organisatorische Interoperabilität

Auf Grund der Vielzahl bestehender Fachverfahren, in denen relevante Daten in unterschiedlichsten Formaten vorgehalten werden, muss ein effizienter Ansatz zur Herstellung von organisatorischer Interoperabilität gewählt werden. Dafür muss u. a. vorab geklärt sein, welche Behörden welche gesichert korrekten bzw. validen Informationen vorhalten. Dieser jeweilige Single-Point-of-Truth (SPoT) muss den abfragenden Stellen bekannt sein.

Ein Datenaustausch im Sinne des proaktiven Verwaltungshandelns ist zudem nur dann sinnvoll, wenn die Verknüpfungen zwischen den unterschiedlichen Leistungen den jeweiligen Behörden bekannt bzw. die Daten für diese verfügbar sind. Hierin liegt ein zentraler Hinderungsgrund für einen effektiven behördenübergreifenden Datenaustausch:
Behörden kennen in der Regel ihre eigene Zuständigkeit, können hingegen den Aufwand und die Anforderungen daran angrenzender Verfahren nur begrenzt oder gar nicht abschätzen. Entsprechend ist auch nicht transparent, welche Daten im Einzelnen von einer Behörde sinnvollerweise an eine andere übermittelt werden sollten. Daher können auch keine speziellen gesetzliche Übermittlungsbefugnisse für diese konkreten Datenaustausche geschaffen werden bzw. bestehende Befugnisse angepasst werden. Um den Wert eines möglichen Datenaustausches zu maximieren, sind demnach neben konkreten Anwendungsfällen Kenntnisse der Anknüpfungspunkte zwischen den Verwaltungsverfahren erforderlich. Hierbei kann es sowohl Verknüpfungen zwischen unterschiedlichen Behörden einer Ebene wie auch ebenen-übergreifende Anknüpfungspunkte geben.

Es bedarf eines Single Point of Truth, der die Richtigkeit der Daten garantiert.

4.5 Offene Fragen bezüglich der Aktualität und Validität der Daten

Der Single Point of Truth (SPoT) ist auch in Bezug auf die Integrität und Validität ein zu lösendes Hindernis:

Zu klären ist u. a. die Frage, inwieweit eine behördenübergreifende Datennutzung sich bspw. auf das Widerspruchsverfahren auswirkt. Werden Daten nicht bei Antragstellenden direkt erhoben, müsste die Prüfung von Widersprüchen nicht nur das Ergebnis des Verwaltungsaktes einbeziehen sondern ggf. auch eine Integritäts- bzw. Validitätsprüfung der verwendeten Daten – also eine Quellenprüfung –, um die Richtigkeit der dem Verfahren zu Grunde liegenden Daten zu verifizieren. Hier stellt sich dann die Frage, ob eine solche Integritätsprüfung mit verhältnismäßigem Aufwand durchführbar ist und wie eine solche Prüfung realisiert werden kann oder ob in solchen Fällen zwangsläufig eine Direkterhebung erfolgen sollte. Des Weiteren ist zu prüfen, ob und wie im Rahmen von Verwaltungsvorschriften bestehende Anerkennungen einbezogen werden müssen bzw. sollen. Hier schließt sich der Kreis zum Datenschutz, denn die gegenseitige Anerkennung von bereits erlassenen Verwaltungsakten ist besonders datensparsam, reduziert Risiken für die Betroffenen auf ein Minimum und beschleunigt die Antragsbearbeitung.

Auch um den Anforderungen der DSGVO bzgl. Richtigkeit personenbezogener Daten nachzukommen, muss eine Methode zur Sicherstellung der Integrität der übermittelten Daten etabliert werden. Ohne eine Integritätssicherung wäre die Direkterhebung bei den Betroffenen ansonsten dem Austausch – also der indirekten Erhebung – vorzuziehen, da Datenintegrität und insbesondere Aktualität auf diesem Weg am einfachsten und sichersten gewährleistet werden kann.

> Die Frage nach dem Single Point of Truth einer Datenquelle korreliert mit der datenschutzrechtlichen Anforderung an die Richtigkeit und Integrität der Daten.

4.6 Finanzierung und Vendor-Lock-in-Effekte

Die föderale Aufgabenteilung hat im Bereich des Aufbaus von eGovernment-Strukturen und diversen Digitalisierungsprojekten zu einer heterogenen Daten- und IT-Landschaft geführt, die den Datenaustausch und die gemeinsame Datennutzung hemmen. Hinzukommen „Vendor-lock-in"-Effekte[4] im Bereich der Fachverfahren bzw. Fachanwendungen, die die behördenübergreifende Datennutzung zusätzlich erschweren.

Es besteht daher eine Notwendigkeit, die bestehenden individuellen technischen Strukturen und Anwendungen in ein **interoperables Datennutzungskonzept** zu integrieren. Investitionsschutz und Investitionsbedarf konkurrieren dabei um begrenzte Haushaltsmittel. Häufig wurden digitale Strukturen erst vor wenigen Jahren aufgebaut. Eine übergreifende Datennutzung

[4] Lock-in-Effekte sind enge Kundenbindung an Produkte/Dienstleistungen oder einen Anbieter, die es dem Kunden erschweren das Produkt oder den Anbieter zu wechseln.

oder Open-Source-Ansätze waren jedoch in der Regel keine Anforderung im Rahmen der Beschaffung, sodass diese nun nachträglich realisiert werden müssen und entsprechend neue bzw. zusätzliche Kosten verursachen können.

Die Fachverfahrenslandschaft muss sich mithilfe eines Datennutzungskonzeptes unter Berücksichtigung bestehender Standards für die interoperable Datennutzung ertüchtigen.

4.7 Kritische und sensible Daten

Zudem begegnen bestehende Bemühungen um den effizienten Austausch von Verwaltungsdaten einigen offenen rechtlichen Fragen abseits des datenschutzrechtlichen Erlaubnisvorbehalts. Ein solches Problemfeld ist, dass für einen effektiven interföderalen Datenaustausch auch **kritische und sensible Daten** übermittelt werden müssen. Dabei müssen zum einen die besonderen Kategorien personenbezogener Daten gem. **Art. 9 und 10 DSGVO** beachtet werden, die zum Schutz der Betroffenen als besonders sensibel bewertet werden. Der Datenschutz steht einem Datenaustausch nicht entgegen (s.u.) – muss aber gerade bei sensiblen Daten möglichst von Anfang an mitgedacht und angemessen berücksichtigt werden.

Darüber hinaus gibt es Informationen, die aus verwaltungsinterner Sicht als besonders schützenswert gelten, etwa Verschlusssachen. Für diese Daten müssen die jeweiligen „Verschlusssachenanweisungen“ berücksichtigt werden, die eine Übermittlung der Daten nur unter bestimmten Bedingungen erlaubt. Verschlusssachen betreffen allerdings nur einen sehr kleinen Teil von Verwaltungsdaten

4.8 Unkenntnisse über Datenschutz

Im Unterschied zum Datenschutzrecht, das den interföderalen Datenaustausch nicht verhindert, ist die Unsicherheit über die datenschutzrechtlichen Anforderungen und Möglichkeiten in der Verwaltung ein Hemmnis für den interföderalen Datenaustausch.

Insbesondere darüber, dass der Grundsatz der Zweckbindung gem. Art. 5 Abs. 1 Buchst. b DSGVO der sinnvollen und legitimen Datennutzung und dem Datenaustausch nicht entgegensteht, besteht zum Teil Unkenntnis. Diese Unsicherheit führt oft dazu, dass die Möglichkeiten der Digitalisierung nicht ausgeschöpft werden, um keine Fehler zu machen.
Datenschutz wird zudem meist nicht als Ermöglicher von Digitalisierung, sondern als Verhinderer gesehen. Dabei ist die Datenübertragbarkeit sogar ein durch die DSGVO garantiertes Recht der Betroffenen (Art. 20 DSGVO). Selbstverständlich gilt dieses Recht auch für die

Verarbeitung von Daten auf Grundlage von Einwilligungen und Verträgen. Die DSGVO steht aber erkennbar einem Datenaustausch nicht entgegen.

Es besteht weiterhin ein erheblicher Unterstützungsbedarf, um den Kompetenzaufbau im Datenschutz in der öffentlichen Verwaltung gezielt voranzutreiben.

Hundegesetz in Schleswig-Holstein: Gesetz über das Halten von Hunden (HundeG) vom 26. Juni 2015

Prüfungsablauf Einordnung von gefährlichen Hunden nach §7 I (Hinweisgebender Tatbestand)

1. Stufe: Hinweis geht bei der Behörde ein

Auslöser der Annahme der Gefährlichkeit: Hinweis an die zuständige Behörde über:

- Ein Hund hat einen Menschen gebissen, sofern dies nicht zur Verteidigung anlässlich einer strafbaren Handlung oder aus dem elementaren Selbsterhaltungstrieb des Hundes geschah, § 7 I Nr. 1
- und/oder
- Ein Hund hat wiederholt in gefahrdrohender Weise Menschen außerhalb des befriedeten Besitztums der Hundehalterin oder des Hundehalters angesprungen oder ein anderes aggressives Verhalten gezeigt, das nicht dem elementaren Selbsterhaltungstrieb des Hundes entspringt, § 7 I Nr. 2
- und/oder
- Ein Hund hat ein anderes Tier durch Biss geschädigt, ohne selbst angegriffen worden zu sein, oder einen anderen Hund trotz dessen erkennbarer artüblicher Unterwerfungsgestik gebissen, § 7 I Nr. 3
- und/oder
- Ein Hund hat durch sein Verhalten gezeigt, dass er unkontrolliert Tiere hetzt oder reißt, § 7 I Nr. 4

2. Stufe: Tatsachenbasierte Überprüfung des Hinweises

Tatsachenbasiertes Prüfverfahren nach § 7 I Nr. 4 der zuständigen Behörde; Der Einschätzungsprozess wird erst auf Hinweis auf einen der vier Fälle nach § 7 I ausgelöst

→ Stellt die Behörde Tatsachen fest, die den Verdacht rechtfertigen, so stellt die Behörde die Gefährlichkeit des Hundes fest

→ Gegen die Feststellung kann Widerspruch und Klage ergehen; diese haben nach Satz 2 jedoch keine aufschiebende Wirkung, vgl. § 7 I Nr.4.

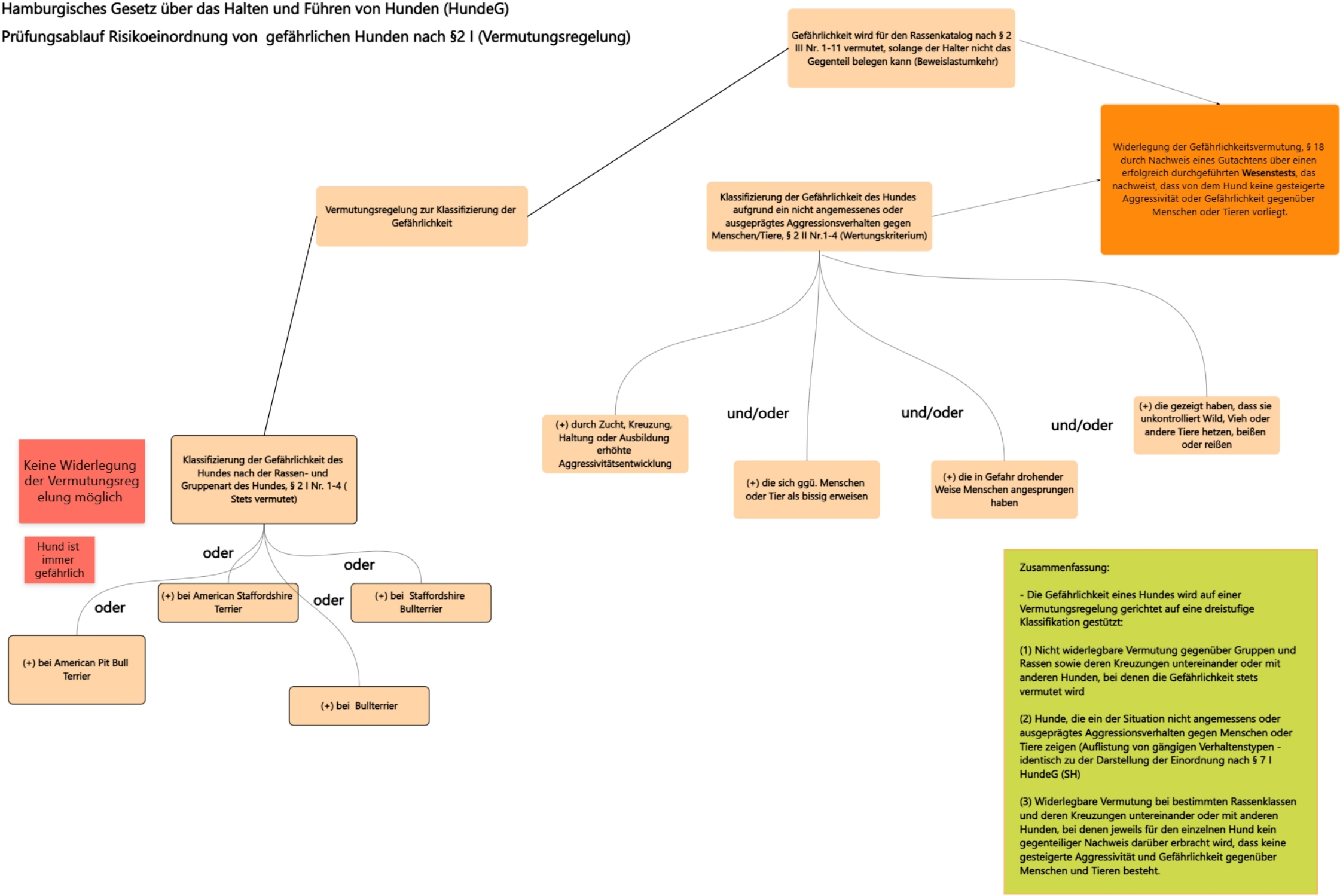
Mitteilungspflicht über die Gefährlichkeit bei der zuständigen Behörde für den Halter, der einen Hund hält, der außerhalb des Geltungsbereichs des Gesetzes durch einen Verwaltungsakt als gefährlich eingestuft wurde, vgl. § 7 II

Zusammenfassung:

- Die Gefährlichkeit eines Hundes wird basierend auf verhaltenstypischen Indikationen geprüft und nur dann, wenn ein Hinweis bei der zuständigen Behörde eingeht oder aber eine Mitteilungspflicht des Halters/der Halterin besteht , weil bereits ein Verwaltungsakt außerhalb des Geltungsbereichs dieses Gesetzes über die Gefährlichkeit des Hundes ergangen ist.

Hamburgisches Gesetz über das Halten und Führen von Hunden (HundeG)

Prüfungsablauf Risikoeinordnung von gefährlichen Hunden nach §2 I (Vermutungsregelung)



Zusammenfassung:

- Die Gefährlichkeit eines Hundes wird auf einer Vermutungsregelung gerichtet auf eine dreistufige Klassifikation gestützt:

(1) Nicht widerlegbare Vermutung gegenüber Gruppen und Rassen sowie deren Kreuzungen untereinander oder mit anderen Hunden, bei denen die Gefährlichkeit stets vermutet wird

(2) Hunde, die ein der Situation nicht angemessens oder ausgeprägtes Aggressionsverhalten gegen Menschen oder Tiere zeigen (Auflistung von gängigen Verhaltenstypen - identisch zu der Darstellung der Einordnung nach § 7 I HundeG (SH)

(3) Widerlegbare Vermutung bei bestimmten Rassenklassen und deren Kreuzungen untereinander oder mit anderen Hunden, bei denen jeweils für den einzelnen Hund kein gegenteiliger Nachweis darüber erbracht wird, dass keine gesteigerte Aggressivität und Gefährlichkeit gegenüber Menschen und Tieren besteht.

Datenpool

Hamburg

Status Quo Abfrage zur Erlaubnis zum Halten und Führen von gefährlichen Hunden

Bescheinigung über die erfolgreich abgelegte Gehorsamsprüfung, § 4 HundG (Sachkunde) Festgelegte Prüfungsstandards bei einer anerkannten sachverständigen Einrichtung/Person; Nachweis über die Kontrolle des Hundes im Alltag und der Fähigkeit zum Halten und Führen, sodass von ihm voraussichtlich keine Gefahren oder erheblichen Belästigungen für Menschen, Tiere oder Sachen ausgehen.

Fähigkeit zur Anerkennung +, weil standardisiertes Verfahren

Nachweis Wesenstest, § 5 HundG
Durch den Wesenstest wird überprüft, ob ein Hund eine gesteigerte Aggressivität oder Gefährlichkeit gegenüber Menschen oder Tieren aufweist. Er wird nach festgelegten Standards von einer anerkannten sachverständigen Person/Einrichtung durchgeführt. Von andern sachverständigen Personen oder Einrichtungen durchgeführte Wesenstests können anerkannt werden.

Fähigkeit zur Anerkennung +, siehe Anlage zu § 13 Abs. 2 VwV-HundeG (Verwaltungsvorschrift zum Hundegesetz SH)

Fälschungssichere Kennzeichnung ab der Vollendung des dritten Lebensmonats , §§ 6 I, II, § 11 HundG
Kennzeichnung eines Hundes mit einem elektronisch lesbaren Transponder (Mikrochip) gemäß ISO-Norm. Transponder darf neben einer einmalig vergebenden, unveränderlichen Kennnummer keine weiteren Angaben enthalten. Die Kennnummer darf weder Daten über die...

Fähigkeit zur Anerkennung +

Haftpflichtversicherung , § 12 HundG
Verpflichtung einer Haftpflichtversicherung ohne Selbstbeteiligung oder mit einer Selbstbeteiligung von höchstens 500 Euro zur Deckung der durch den Hund versursachten Schäden mit einer Mindestversicherungssumme in Höhe von 1 Million Euro für Personen- und sonstige Schäden (Abschluss und Aufrechterhalten) ...

Fähigkeit zur Anerkennung?

Anzeige- und Mitteilungspflichten , § 13 HundG
Innerhalb von 2 Wochen nach Aufnahme der Hundehaltung bzw. bei Welpen nach Ablauf des Monats, indem der Hund nachweislich den dritten Lebensmonat vollendet hat:

Angaben + Unterlagen:
- Name, Vorname, Anschrift und Geburtsdatum der Halterin oder des Halters...

Fähigkeit zur Anerkennung?

Fähigkeit zum Datenabgleich (Aktualisierungs-gesuch)

Umfangreiche Zuverlässigkeitsprüfung der Halterin/ des Halters , § 16 HundG

- nur bei Personen, die nicht strafauffällig geworden sind und keine Straftaten nach dem umfangreichen Katalog begangen haben
- nur bei Personen, die nicht wiederholt oder gröblich gegen Vorschriften des...

Fähigkeit zur Anerkennung +, da die umfangreiche Vorabprüfung und Einschätzung der Behörde als vertrauensbasierte Maßnahme fortgeführt werden kann, soweit nicht neue entgegenstehende Tatsachen vorliegen

Datenübermittlung der gespeicherten personenbezogenen Daten nur zweckgebunden! Siehe § 16 IV

- für die mit der Zuverlässigkeitsprüfung verfolgten Zwecke
- zur Abwehr einer unmittelbar bevorstehenden, erheblichen Gefahr für die öffentliche Sicherheit
- zur Verhinderung oder Verfolgung von...

Datenübermittlung der gespeicherten personenbezogenen Daten nur zweckgebunden! Siehe § 16 IV

Zweckbindung vorhanden?

> Immer wenn es um dieselbe Verwaltungsleistung geht, muss es faktisch zweckidentisch sein.

zero knowledge proof ausreichend, wenn SH auf die Zuverlässigkeitsprüfung aus HH vertrauenn möchte/vertraut

Sondervoraussetzung für die Erteilung der Erlaubnis: Darlegen besonderes Interesse an der Haltung des gefährlichen Hundes § 15 Abs. 1 Nr. 3 a) HundG
Die Halterin/der Halter muss ein besonderes Interesse an der Haltung eines gefährlichen Hundes darlegen; liegt vor, wenn die Halterin /der Halter ein besonders geschütztes Interesse glaubhaft macht, auf Grund desesn die Untersagung der Haltung des...

Fähigkeit zum Abgleich: (ein strengeres Prüfverfahren ist per se erstmal leichter anzuerkennen, weil die Standards höher wirken) und dies Vertrauen schafft.

Sondervoraussetzung für die Erteilung der Erlaubnis: Der Hund muss operativ kastriert sein § 15 Abs. 1 Nr. 3 b) HundG

Fähigkeit zum Abgleich: (ein strengeres Prüfverfahren ist per se erstmal leichter anzuerkennen, weil die Standards höher wirken) und dies Vertrauen schafft.

Sondervoraussetzung für die Erteilung der Erlaubnis: Vorlage eines amtlichen Gesundheitszeugnisses bei Hunden der Rassenkategorie nach § 2 Abs. 1 gilt § 15 Abs. 1 S. 2 a) HundG

Amtliches Gesundheitszeugnis der Halterin/ des Halters, dass die Person geistig und körperlich geeignet und zuverlässig ist, einen gefährlichen Hund zu führen...

Fähigkeit zur Anerkennung, ohne dass auf die Daten aus dem Gesundheitszeugnis zugegriffen werden muss + (Tatsachenbasierte Annahme, dass die Voraussetzung vorliegt, reicht schon aus)

Sondervoraussetzung für die Erteilung der Erlaubnis: Behördliche Bescheinigung über Geeignetheit beim Führen des Hundes (Nachweis über mind. 2 Bescheinigungen für Hunde nach § 2 Abs. 1 § 15 Abs. 1 S. 2 b) HundG

Fähigkeit zum Abgleich und der Anerkennung aufgrund der strengeren Rassenkategorisierung in HH (ein strengeres Prüfverfahren ist per se erstmal leichter anzuerkennen, weil die Standards höher wirken) und dies Vertrauen schafft.

Sondervoraussetzung für die Erteilung der Erlaubnis: Nachweis über die Teilnahme an Schulungsveranstaltungen im Umgang mit gefährlichen Hunden für Hunde nach § 2 Abs. 1 § 15 Abs. 1 S. 2 c) HundG

Fähigkeit zum Abgleich und der Anerkennung aufgrund der strengeren Rassenkategorisierung in HH (ein strengeres Prüfverfahren ist per se erstmal leichter anzuerkennen, weil die Standards höher wirken) und dies Vertrauen schafft.

Sondervoraussetzung für die Erteilung der Erlaubnis: Nachweis, dass Hund nicht aus einer illegalen Haltung (Verbotene Zucht) oder nach illegaler Einfuhr erlangt wurde - für Hunde nach § 2 Abs. 1 § 15 Abs. 1 S. 2 d) HundG

Fähigkeit zum Abgleich und der Anerkennung aufgrund der strengeren Rassenkategorisierung in HH (ein strengeres Prüfverfahren ist per se erstmal leichter anzuerkennen, weil die Standards höher wirken) und dies Vertrauen schafft.

Bereitgestelltes Datenpool aus Hamburg mit Autorisierungs- und Abfragestufen aus dem Hunderegister und weiteren Dokumenten und Anlagen

1) Personenbezogene Daten aus dem Hunderegister

2) Zuweisung des Hundes: Chipnummer/Kennzeichnung; ggf. Angaben aus dem Hunderegister

3) Angaben zur Haftpflichtversicherung (Laufzeit, Wechsel, Aktualisierung etc.) aus dem Hunderegister

4) Angaben zur zuständigen Behörde innerhalb der letzten 5 Jahre (Wohnsitzwechsel etc.) - Nachverfolgung durch interne Protokolle

5) Angaben zur Einschätzung (Rassenkatalog oder Verhaltensauffälligkeiten); Behördliche Erwägungen; ggf. Hinweise auf Freistellungsanträge, Freistellungsverfahren

6) Angaben zur Eignung der Halterperson (Gesundheitliche Voraussetzungen, Führungszeugnis , Angaben aus dem Zentralregister; Anfragen an Ordnungsbehörden; Zuverlässigkeitskriterien,) aus dem Hunderegister

7) Angaben zum bisherigen Antrags- und Verfahrensprozedere; Verhaltensauffälligkeiten

Status Quo Abfrage zur Erlaubnis zum Halten und Führen von gefährlichen Hunden

Zugriff auf Daten

Kiel

Personen-identifikation

1) Abgleich Personenidentität des Antragstellenden: Personalausweis und Antragsdaten (Insbesondere Wohnsitz bei Wohnsitzwechsel, Name, Vorname Geburtsdatum)

Alternative zur Stammdaten-Abfrage:
Fähigkeit zur Verknüpfung mit einer ID-Nummer (festgelegte Zuweisung) - man nimmt die ID als eindeutige identifizierende Referenz für einen Menschen und prüft die Person mit der Abfrage der ID-Nummer ab (Abfrage zu Einträgen mit der Nummer)

Vorteil: Pseudonymisierung der Abfrage zu...

Hunde-identifikation

2) Abgleich Hundeidentität des Antragstellenden: Aus den Angaben im Hunderegister; Chipnummer des Hundes; Name, Geschlecht, Geburtsdatum und Rasse des Hundes

Hund-Halter Abgleich inkl. Zuweisungsverfahren mit der ID-Verknüpfung

Haftpflicht-versicherung

3) Abgleich Haftpflichtversicherun

Fähigkeit zur Anerkennung +, da Hamburg eine höhere Deckungssumme als SH verlangt: Vorliegen muss der Decksumme und der Geltung/Aktualität entsprechen

Haftpflichtversicherung nach § 6 HundeG SH: Anforderung einer Mindestversicherungssumme von 500.000 Euro für Personenschäden und v...

Behörden-zuständigkeit

4) Abgleich: Zuständige Behörde, bei der der Hund geführt wird

Einstufung des Hundes

5) Abgleich Gefährlichkeit des Hundes

Fähigkeit zur Anerkennung +

6) Abgleich Wesenstest

Fähigkeit zur Anerkennung +

Einstufung der Halterin/des Halters

7) Abgleich Eignungskriterien: Zuverlässigkeit, persönliche Eignung/ Geeignetheit

Fähigkeit zur Anerkennung +; auf die Gesundheitsdaten muss nicht explizit zugegriffen werden aber die behördliche Einschätzung wäre relevant - zum Zwecke der Zuverlässigkeitsprüfung wäre zumindest eine Übermittlung der Daten wohl erlaubt

Fähigkeit zur Anerkennung der Zuverlässigkeitsprüfung +, da diese in Hamburg viel umfangreicher und strenger erfolgt

Hamburg prüft weitergehend als SH zudem, ob die Notwendigkeit des Führens und Haltens eines gefährlichen Hundes gegeben ist; dies muss die Halterin/der Halter aufgrund eines schutzbedürftigen Interesses erstmal nachweisen und zudem anhand eines...

Zugriff auf sensible Gesundheitsdaten notwendig?

8a) Abgleich: Erlaubnisse, Freistellungen, Befreiungen einschließlich Datum der Antragstellung, Bescheiderteilung und ggf. Widerruf der Erlaubnis, Freistellung oder Befreiung (inkl. Erwägungsgründe?)

8b) Abgleich: Abgelehnte Anträge einer Erlaubnis, Freistellung oder Befreiung einschließlich Datum der Antragstellung und der Bescheiderteilung

8c) Abgleich: Anordnungen wie Haltungsuntersagungen, Verbote zum Führen oder Haltungsbeschränkungen (Zeitdauer und Festsetzungen); etwaige Vollstreckungsaufträge

8d) Abgleich: Verstöße gegen die Vorschriften des Hundegestzes, gegen Anleinpflichten oder Mitnahmverbote; Bissvorfälle, Angaben zu entstandenen Sach- oder Personenschäden oder erheblichen Belästigungsvorfällen

Fähigkeit zur Anerkennung + bzw. Grundlage zur Entscheidung über eine Erlaubniserteilung

Negativ-Abfrage: Erlaubnisse nicht widerrufen, entzogen

Nachvollziehen des bisherigen Antrags- und Verfahrensverlaufs inkl. Status-Quo Abfrage zur Erlaubniserteilung

Was muss Kiel wissen?

Liegt die Erlaubnis bereits vor?

Lagen in der Vergangenheit wiederholte oder gröbliche Verstöße gegen die Vorschriften des Hundegesetzes vor?

Wurde die Erlaubnis befristet erteilt?

Wurde die Erlaubnis in der Vergangenheit wegen auffälligem aggressiven Verhalten versagt, befristet oder widerrufen?

Liegt ein Freistellungsverfahren oder eine Freistellung durch die Widerlegung der Gefährlichkeitsvermutung im Sinne von § 18 HundeG vor? -
Nachweis, dass keine gesteigerte Aggressivität oder Gefährlichkeit gegenüber Menschen oder Tieren vorliegt. Notwendig ist ein Gutachten über einen erfolgreich durchgeführten Wesenstest, § 5 mit Anerkennungsmöglichkeit.

Handelt es sich um einen langfristigen Aufenthalt oder einen Wohnsitzwechsel? (Längere Verweildauer als 2 Monate ununterbrochen in SH)

Wurde bzw. wie wurde die Gefährlichkeit bereits festgestellt? (Rassenkategorisierung oder verhaltensauffälliges Auftreten)

Wie lange hat eine Erlaubniserteilung Bestand?

Fähigkeit zur Anerkennung im Sinne von § 17 HundeG SH: Anerkennung von Entscheidungen und Bescheinigungen anderer Länder
Erlaubnisse, Sachkundebescheinigungen und Befreiungen, die von zuständigen Stellen anderer Länder erteilt wurden, sollen von der zuständigen Behörde anerkannt werden, wenn sie den durch dieses Gesetz gestellten Anforderungen im Wesentlichen entsprechen.

Voraussetzung
- Zuverlässigkeitsprüfung wird anerkannt
- Gehorsamsprüfung entspicht der Sachkundeprüfung

AntragstellerIn

Zuzugshundeamt

FHH Hunderegister

Antrag auf Haltung dieses Hundes

Haltung dieses Hundes in SH erlaubnispflichtig? Ja, wenn der Hund in der Vergangenheit Aggressionsverhalten zeigte

Übermittlung Chipnummer Hund

P

Abfrage, ob
1. Hund registriert
2. Aggressionsverhalten dokumentiert
3. Haltungserlaubnis erteilt...

A

1. Hund registriert (+)
2. Aggressionsverhalten dokumentiert (+)
3. Keine Haltungserlaubnis

individuelle Prüfung, ob Erlaubnis trotz Aggressionsverhaltens erteilt werden kann

P

Erlaubnis erteilen

E

A

1. Hund registriert (+)
2. Aggressionsverhalten dokumentiert (-)

A

1. Hund registriert (+)
2. Aggressionsverhalten dokumentiert (+)
3. Haltungserlaubnis erteilt (+)

Abgleich Antragsteller = Halter:
1) Abgleich Personenidentität des Antragstellenden: Personalausweis und Antragsdaten (Insbesondere Wohnsitz bei Wohnsitzwechsel, Name, Vorname Geburtsdatum)

P

Übermittlung pbD Antragsteller

A

Abgleich, ob Antragsteller identisch mit Halter der Erlaubnis ist

Erlaubnis erteilen

Ja

P

Ja

Prüfung,
ob **Haftpflichtversicherung** weiter besteht