# INTEROPERABILITÄT IM KATASTROPHENMANAGEMENT UND DATENSCHUTZ

Erich Schweighofer / Jakob Zanol / Ivan Gojmerac

Professor, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
Erich.Schweighofer@univie.ac.at, https://rechtsinformatik.univie.ac.at

Dissertant und Wissenschaftlicher Mitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
jakob.zanol@univie.ac.at; https://rechtsinformatik.univie.ac.at

Senior Scientist, Austrian Institute of Technology, Digital Safety Security
Giefinggasse 4, 1210 Wien, AT
Ivan.Gojmerac@ait.ac.at; https://www.ait.ac.at/ueber-das-ait/researcher-profiles/?tx_aitprofile_pi1%5Bname%5D=Gojmerac-Ivan

***Schlagworte:*** ***Katastrophenmanagement, Datenschutz, Privacy-by-Design, Informationsaustausch, KIRAS, INTERPRETER***

***Abstract:*** *Das KIRAS-Projekt INTERPRETER erforscht den Ausbau der zivil-militärischen Interoperabilität im Krisen- und Katastrophenmanagement in Österreich, mit dem Ziel eines vollständig automatisierten Datenaustausches zwischen (Führungs-)Informationssystemen sowie der Einbindung der Bevölkerung. Dadurch soll ein gemeinsames, aktuelles Lagebild gepflegt und die Effizienz im Kriseneinsatz erhöht werden. Dieser Beitrag stellt die technische Umsetzung sowie die sich dabei ergebenden Rechtsfragen dar, insbesondere auch jene im Bereich des Datenschutzrechts im Katastrophenmanagement.*

## 1. Einleitung: Interoperabilität im Katastrophenmanagement der nächsten Generation (INTERPRETER)

Elementarereignisse und Unglücksfälle außergewöhnlichen Umfanges erfordern ein effizientes Katastrophenmanagement. Zu diesem Zweck ist die Erstellung eines akkuraten Lagebildes notwendig. Die Anreicherung von Informationen und der Austausch selbiger stellt die Akteure im Katastrophenmanagement vor große Herausforderungen. Neben der fachlichen Expertise der Akteure bedarf es eines raschen und präzisen Informationsaustausches zwischen den öffentlichen Rollenträgern untereinander sowie dem Katastrophenschutz.

Das KIRAS-Projekt INTERPRETER verfolgt das Ziel, in Anknüpfung an den aktuellen Stand der Forschung mittels modernster Softwaredesignmethoden einen medienbruchfreien Datenaustausch zwischen den zivilen und militärischen (Führungs-)Informationssystemen zu ermöglichen und im Rahmen dieses Prozesses die semantische Integrität derselben sicherzustellen.[1] Die unter der Leitung des Austrian Institute of Technology (AIT) entwickelte Systemarchitektur, in die auch Ergebnisse des Vorgängerprojekts KIRAS INKA eingeflossen sind[2], erlaubt nicht nur den Austausch von Informationen über die jeweiligen Führungsinformationssysteme der öffentlichen Akteure des Katastrophenmanagements, sondern auch die Einspeisung von Informationen durch die Bevölkerung über eine eigens entwickelte Smartphone-Applikation. Wie sich zeigte, berührt die Schaffung der INTERPRETER-Systemarchitektur verschiedene Rechtsgebiete, darunter etwa verfassungs- und (landes-)verwaltungsrechtliche Rahmenbedingungen des Katastrophenschutzes sowie Fragen des Urheberechts, des Rechts am eigenen Bild und insbesondere auch des Datenschutzrechts. Aufgrund des vorgege-

[1] Vgl. https://www.kiras.at/gefoerderte-projekte/detail/d/interpreter/ (zuletzt abgerufen 03.01.2019).
[2] Vgl. https://www.kiras.at/gefoerderte-projekte/detail/d/inka/ (zuletzt abgerufen 03.01.2019).

benen Umfangs wird die rechtliche Betrachtung in diesem Beitrag, die an die technische Beschreibung der Systemarchitektur anschließt, auf ausgewählte projektspezifische Besonderheiten aus dem Datenschutzrecht beschränkt.

## 2. Die INTERPRETER-Systemarchitektur

Kern der INTERPRETER-Architektur bildet der INTERPRETER-Datenhub, der die Führungsinformationssysteme der verschiedenen Akteure miteinander verbindet und einen standardkonformen Austausch von Informationen ermöglicht. Die erarbeitete Architektur beruht auf dem Prinzip, dass die einzelnen Akteure im Krisen- und Katastrophenmanagement jene Informationen, die ihnen durch andere Organisationen zur Verfügung gestellt werden, in ihrer eigenen Systemlandschaft darstellen können sollen. Auf diese Art und Weise kann organisationsübergreifend ein gemeinsames Lagebild (engl. Common Operational Picture) gewonnen werden, ohne den Zwang der Verwendung eines einheitlichen Führungsinformationssystems seitens aller Akteure, womit sowohl die bestehenden Workflows als auch die Investitionen der einzelnen Organisationen gewahrt werden. Mittels des INTERPRETER-Datenhubs wird effektiv ein Datenverbund für die Akteure im österreichischen Krisen- und Katastrophenmanagement geschaffen, der neben der Interoperabilität von Führungsinformationssystemen auch die Einbindung weiterer Informationskanäle bzw. -quellen ermöglicht. So ist im Rahmen des Projekts eine Smartphone-Applikation entwickelt worden, die es ermöglicht, die Bevölkerung bzw. geschulte Personengruppen mit Aufgaben in der Katastrophenbewältigung zu betrauen. Typischerweise handelt es sich dabei um die Gewinnung von Informationen vor Ort zwecks Lagebildverdichtung (Foto-Aufnahmen von Schadstellen, Kurzberichte) oder um konkrete Handlungsanweisungen, die einer effizienteren Bewältigung der Lage dienen. Dabei können die Aufgaben an die Personen im Feld in den Führungsinformationssystemen der einzelnen Organisationen erstellt und mittels INTERPRETER-Datenhub an das Smartphone-Applikationsbackend – und von dort wiederum an die einzelnen Smartphones – übertragen werden, und andersherum können die mittels der Applikation gewonnenen Informationen direkt in die einzelnen Führungsinformationssysteme eingespeist werden, wo sie den Krisenmanagern unmittelbar zur Verfügung stehen.

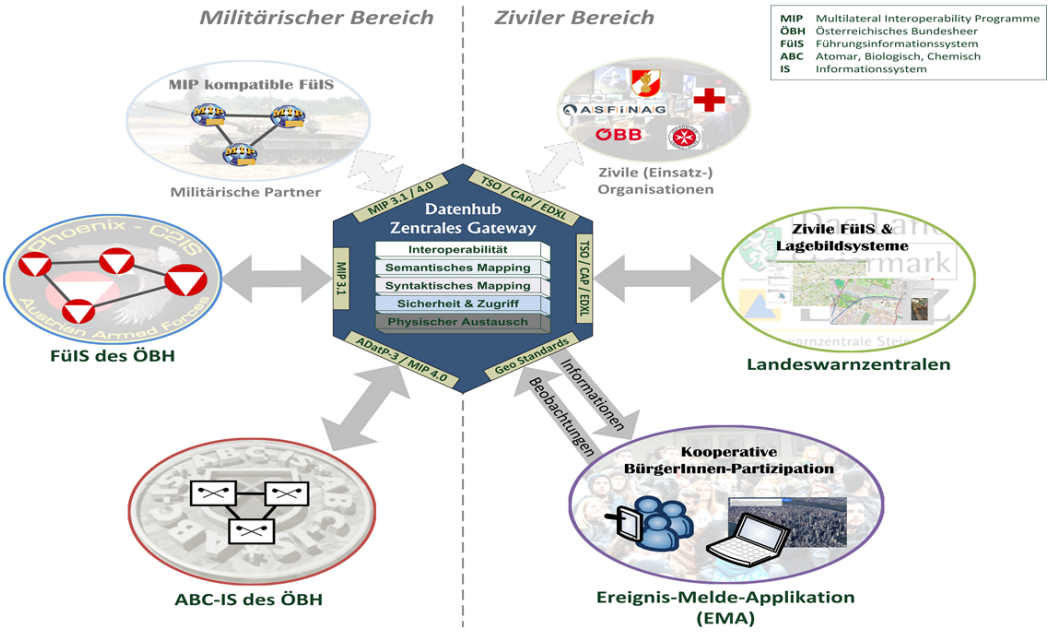


**Abbildung 1: INTERPRETER-Systemarchitektur**

## 3. Informationsaustausch im Katastrophenmanagement und Datenschutz

Die Evaluierung einer Systemarchitektur – wie jene des INTERPRETER-Projektes – bringt zahlreiche Rechtsfragen zutage. Wie einleitend erwähnt, wird sich die folgende rechtliche Betrachtung auf projektspezifische Fragestellungen im Datenschutzrecht beschränken.

Datenschutzrechtliche Fragen berühren hier sowohl den Informationsaustausch zwischen den staatlichen Akteuren und den Hilfsorganisationen untereinander als auch jenen unter Einbeziehung der Bevölkerung. Hier ist die Bestimmung des § 10 DSG[3] zentral. § 10 Abs. 1 DSG ermächtigt den Verantwortlichen des öffentlichen Bereichs und Hilfsorganisationen im Katastrophenfall, personenbezogene Daten gemeinsam zu verarbeiten, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist. Darüber hinaus ergeben sich projektspezifische Besonderheiten aus der Systemarchitektur die in den Kontext der aktuellen Judikatur des europäischen Gerichtshofes gesetzt werden. Abschließend werden Überlegungen zum Datenschutz durch Technikgestaltung für die weitere Umsetzung des Prototypen dargestellt.

### 3.1. Katastrophenschutz im Anwendungsbereich der DSGVO

Während dieser Frage auf nationaler Ebene und damit im Rahmen des Projektes eher geringere Bedeutung zukommt[4], ist die grundsätzliche Frage der Anwendbarkeit der europäischen Datenschutz-Grundverordnung (DSGVO[5]) auf Vorgänge im Rahmen des Katastrophenschutzes insbesondere in Hinblick auf das internatio-

[3] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999.

[4] § 4 DSG; siehe Punkt 3.1 aE.

[5] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 2016/119, 1.

nale Publikum dieser Konferenz durchaus von Interesse und daher zumindest überblicksweise zu problematisieren.

Zunächst ist in diesem Zusammenhang auf Art. 2 Abs. 2 lit. a DSGVO zu verweisen, welcher festlegt, dass die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten findet, welche im Rahmen einer Tätigkeit erfolgt, die nicht in den Anwendungsbereich des Unionsrechts fällt. Demgegenüber wird den Mitgliedstaaten in Art. 23 Abs. 1 DSGVO die Möglichkeit eingeräumt, Beschränkungen für bestimmte Pflichten und Rechte[6] vorzusehen, sofern diese bestimmte nationale Interessen wie etwa die «nationale Sicherheit», die «Landesverteidigung» oder die «öffentliche Sicherheit» sicherstellen.[7]

In der Literatur wird diesbezüglich teilweise vertreten, dass die Einbeziehung der «nationalen Sicherheit» und der «Landesverteidigung» in Art. 23 DSGVO überflüssig sei, da der Europäischen Union in diesen Bereichen bereits gar keine Regelungskompetenz zukommt und diese Tätigkeiten daher auch bereits nach Art. 2 Abs. 2 lit. a und b DSGVO nicht in den Anwendungsbereich der Verordnung fallen.[8] Dies wird teilweise auch hinsichtlich der Anwendbarkeit auf Verarbeitungstätigkeiten im Rahmen der «öffentlichen Sicherheit»[9], wozu auch der Katastrophenschutz zählt[10], vertreten.[11]

Zumindest im Bereich des Katastrophenschutzes wird, in Hinblick auf die Rechtsprechung des EuGH zu differenzieren sein.[12] Der EuGH stellte fest, dass Verarbeitungstätigkeiten zum Zwecke des Schutzes der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit nicht *eo ipso* aus dem Anwendungsbereich der Richtlinie 2002/58/EG fallen würden, da sonst den Regelungen über die Beschränkungen von Rechten und Pflichten im Rahmen dieser Tätigkeiten jede praktische Wirksamkeit genommen wäre.[13] Dieses Ergebnis würde vom EuGH sowohl auf die Datenschutzrichtlinie[14], als auch auf die DSGVO übertragen werden können. So weist die DSGVO mit Art. 2 Abs. 2 lit. a DSGVO (Ausnahmebestimmung) und Art. 23 Abs. 1 DSGVO (Beschränkung von Rechten und Pflichten) eine vergleichbare Systematik von bereichspezifischen Ausnahmen und darüber hinaus gehender Gestaltungsmöglichkeit des nationalen Gesetzgebers auf.

Darüber hinaus wird in großen Teilen der Literatur von einer Anwendbarkeit der DSGVO auch auf den Bereich der «öffentlichen Sicherheit», einschließlich des Katastrophenschutzes, ausgegangen.[15] In jedem Fall erscheint es angebracht, fallweise zu differenzieren, ob es sich um Verarbeitungstätigkeiten handelt, welche gänzlich aus dem Anwendungsbereich des Unionsrecht fallen, oder um solche, die zwar diese Bereiche berühren, jedoch

---

6 Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt: a) die nationale Sicherheit; b) die Landesverteidigung; c) die öffentliche Sicherheit; […].

7 Siehe Art. 23 Abs. 1 lit. a – c DSGVO.

8 Knyrim, Datenschutz-Grundverordnung: Praxishandbuch (2016) 363; Feiler/Forgó in Feiler/Forgó, EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkommentar (2017) Art. 23 Rz 4; wohl auch: Gola in Gola, Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar$^2$ (2018) Art. 23 Rz 6; aA: Bäcker in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG: Kommentar$^2$ (2018) Art. 23 Rz 15, 17.

9 Art. 23 Abs. 1 lit. c DSGVO.

10 Vgl. Erw. 73 DSGVO.

11 Etwa Peuker in Sydow, Europäische Datenschutzgrundverordnung: Handkommentar$^2$ (2018) Art. 23 Rz 9.

12 EuGH 21. Dezember 2016, C203/15 und C698/15 («Tele2 Sverige»).

13 EuGH 21. Dezember 2016, C203/15 und C698/15 («Tele2 Sverige») Rz. 72.

14 Entsprechende Ausnahmebestimmung; vgl. EuGH 21. Dezember 2016, C203/15 und C698/15(«Tele2 Sverige») Rz 69; EuGH 02. Oktober 2018, C207/16 («Ministerio Fiscal») Rz 32.

15 Siehe Gola in Gola, Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar$^2$ (2018) Art. 23 Rz. 7; Bäcker in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG: Kommentar$^2$ (2018) Art. 23 Rz. 19; aA: Peuker in Sydow, Europäische Datenschutzgrundverordnung: Handkommentar$^2$ (2018) Art. 23 Rz. 9, 22 sowie Haidinger in Knyrim, DatKomm Praxiskommentar zum Datenschutzrecht – DSGVO und DSG (2018) Art. 23 Rz. 15.

nicht gänzlich außerhalb des Regimes der Datenschutz-Grundverordnung stehen, sondern lediglich dem nationalen Gesetzgeber aufgrund dieses Umstandes einen größeren Regelungsspielraum einräumen.[16] Von einer gänzlichen Ausnahme vom Anwendungsbereich der DSGVO auf den Katastrophenschutz kann in Hinblick auf die Judikatur des EuGH jedenfalls nicht ausgegangen werden.

Um die mit einer solchen fallweisen Abwägung verbundene Rechtsunsicherheit zu vermeiden, sieht die nationale Bestimmung des § 4 Abs. 1 DSG die **generelle Anwendbarkeit der Bestimmungen der DSGVO** vor, sofern nicht die spezifischen Umsetzungsbestimmungen der Datenschutzrichtlinie Polizei-Justiz zur Anwendung gelangen. Mit dieser Bestimmung wurde durch den nationalen Gesetzgeber daher dahingehend Rechtssicherheit geschaffen, als die oben erörterte Frage der Anwendbarkeit der DSGVO auf Staatsfunktionen nicht im Einzelfall zu prüfen ist, sondern die Bestimmungen der DSGVO grundsätzlich anzuwenden sind.[17]

### 3.2. § 10 (österreichisches) Datenschutzgesetz

Eine weitreichende datenschutzrechtliche Erlaubnis zur Verarbeitung personenbezogener Daten im Rahmen des Katastrophenschutzes stellt § 10 DSG dar, der im Wesentlichen die bisher in § 48a DSG 2000[18] geregelte Verwendung von personenbezogenen Daten im Katastrophenfall fortführen soll.[19] Für das Projekt INTERPRETER waren die Zulässigkeitstatbestände der ersten beiden Absätze des § 10 DSG besonders bedeutsam:

§ 10 (1) Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen sind im Katastrophenfall ermächtigt, personenbezogene Daten gemeinsam zu verarbeiten, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist.

(2) Wer rechtmäßig über personenbezogene Daten verfügt, darf diese an Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen übermitteln, sofern diese die personenbezogenen Daten zur Bewältigung der Katastrophe für die in Abs. 1 genannten Zwecke benötigen. […]

§ 10 Abs. 1 DSG ermächtigt zunächst **Verantwortliche des öffentlichen Bereichs** und **Hilfsorganisationen** zur Verarbeitung von personenbezogenen Daten im Katastrophenfall im Rahmen taxativ aufgezählter Zwecke und kann als gesetzliche Grundlage einer Aufgabe im öffentlichen Interesse nach Art. 6 Abs. 1 lit. e DSGVO erfasst werden. Als Verantwortliche des öffentlichen Bereichs werden gemäß § 26 Abs. 1 DSG sowohl Verantwortliche, welche in Formen des öffentlichen Rechts eingerichtet sind, als auch Verantwortliche des Privatrechts, soweit sie in Vollziehung der Gesetze tätig sind, verstanden. Darüber hinaus sind auch Hilfsorganisationen zu der in § 10 Abs. 1 DSG vorgesehenen gemeinsamen Verarbeitung personenbezogener Daten berechtigt. Der Begriff der Hilfsorganisation wird in den Erläuterungen der Regierungsvorlage als «eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann» definiert.[20] Aufgrund des funktionalen Ansatzes des § 26 Abs. 1 DSG sind hier die jeweiligen gesetzlichen bzw. statutarischen[21] Aufgaben zu beachten, im Rahmen derer die genannten Verantwortlichen handeln.

---

16 Für eine diesbezügliche Differenzierung abhängig von den nationalen Bestimmungen über die Zuständigkeit: Bäcker in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG: Kommentar[2] (2018) Art. 23 Rz. 13; [wohl nur hinsichtlich Art. 23 Abs. 1 lit. d DSGVO:] Feiler/Forgó, EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkommentar (2017) Art. 23 Rz. 6.

17 Vgl. Kunnert in Bresich et al, DSG, Datenschutzgesetz: Kommentar (2018) § 4 Rz. 3.

18 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000)StF: BGBl. I Nr. 165/1999 idF BGBl. I Nr. 83/2013

19 ME BlgNR 322/ME XXV. GP – Ministerialentwurf – Erläuterungen 13; 1664 der Beilagen XXV. GP – Regierungsvorlage – Erläuterungen 13.

20 Ibidem.

21 Ibidem.

Das Vorliegen einer «**Katastrophe**» ist jenes zentrale Moment, welches die Anwendbarkeit des speziellen Erlaubnistatbestandes des § 10 DSG bedingt. Weder im Gesetz, noch in den Materialien zum Datenschutzanpassungsgesetz 2018[22] findet sich eine Definition. Nach den Gesetzesmaterialien zu § 48a DSG wird zunächst auf den allgemeinen «Sprachgebrauch» verwiesen, jedoch in Folge dargelegt, dass von einer Katastrophe jedenfalls dann auszugehen sei, wenn durch ein Naturereignis oder ein sonstiges Ereignis dem Umfange nach eine außergewöhnliche Schädigung von Menschen oder Sachen eingetreten ist oder unmittelbar bevorsteht.[23] Auch wenn das Vorliegen einer Katastrophe nach § 10 DSG daher unabhängig von einer allfälligen Feststellung einer solchen nach den landesgesetzlichen Katastrophenschutzgesetzen[24] zu prüfen ist, wird regelmäßig von einer Überschneidung der unterschiedlichen Katastrophenbegriffe auszugehen sein, wobei das Vorliegen einer Katastrophe nach den landesgesetzlichen Bestimmungen im Regelfall auch die Anwendbarkeit des § 10 DSG zur Folge hat. Die Feststellung einer Katastrophe durch die landesgesetzlich vorgesehene Katastrophenschutzbehörde hat jedoch auf die Anwendbarkeit des § 10 DSG keine Auswirkung.

Liegt nun ein Ereignis mit entsprechendem Gefahrenpotential vor, so berechtigt § 10 DSG die genannten Verantwortlichen zu einer gemeinsamen Verarbeitung für die Erfüllung bestimmter Aufgaben. Diese Aufgaben sind die Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, die Auffindung und Identifizierung von Abgängigen und Verstorbenen und die Information von Angehörigen. Eine Verarbeitung ist nur zulässig, soweit sie zur Erfüllung dieser Aufgaben notwendig ist und § 10 Abs. 6 DSG hält diesbezüglich nochmals fest, dass die zu Zwecken der Bewältigung des Katastrophenfalles verarbeiteten personenbezogenen Daten unverzüglich zu löschen sind, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.[25]

Die gemäß § 10 DSG erlaubten Datenverarbeitungsvorgänge reichen sehr weit. Dies hat seine Grundlage in der Entstehungsgeschichte der Norm. In Reaktion auf die vorangegangene Tsunami-Katastrophe, sollten die Kompetenzen der Behörden, insbesondere in Hinblick auf die Weitergabe von personenbezogenen Daten an Angehörige, klargestellt werden.[26] Die Erläuterungen der Regierungsvorlage zu § 48a DSG führen dazu folgendes aus:

«[…] Die Sonderbestimmung des § 48a soll primär eine gesetzliche Grundlage für die Verwendung **sensibler Daten** im Katastrophenfall schaffen, wobei in der Praxis regelmäßig Datenanwendungen bestehen, die sowohl nicht-sensible als auch sensible Daten enthalten. Eine exakte Trennung dieser Datenarten ist in vielen Fällen nicht möglich. […]»[27]

Von einer Anwendbarkeit der Bestimmung auf sensible Daten des (alten) § 48a DSG 2000 geht auch Jahnel aus.[28] Für die Verarbeitung im Katastrophenfall wäre eine eigene Bestimmung nicht notwendig gewesen.[29] Dies ist im Ergebnis auch in geltender Rechtslage anzunehmen. Die Intention des Gesetzgebers war die Überführung der Grundsätze der bereits bestehenden Regelung des § 48a DSG und ihre Anpassung an die neuen Erfordernisse der DSGVO. Letztere Anpassung zeigt sich in § 10 Abs. 1 DSG jedoch lediglich in sprachlicher, nicht jedoch in inhaltlicher Hinsicht. So entfällt die konkrete Erlaubnis der Nutzung eines Informationsverbundsystems, wobei § 10 DSG nunmehr jedoch eine «gemeinsame» Verarbeitung zulässt, was begrifflich

22 Ibidem.

23 IA zu § 48a DSG, 515/A BlgNR 22. GP.

24 Etwa § 4 Gesetz vom 16. März 1999 über die Abwehr und Bekämpfung von Katastrophen (Steiermärkisches Katastrophenschutzgesetz) Stammfassung: LGBl. Nr. 62/1999.

25 Vgl. hiezu Art. 5 Abs. 1 (Zweckbindung) i.V.m. Art. 17 Abs. 1 lit. a DSGVO (Löschung bei Zweckerreichung).

26 Dohr et al, Kommentar Datenschutzrecht[2] (2017) § 48a DSG.

27 AB zu § 48a DSG, 821 BlgNR 22. GP.

28 Jahnel, Handbuch Datenschutzrecht (2010) 229.

29 Ibidem.

sogar über die Nutzung eines Informationsverbundsystems in der Diktion des ehemaligen § 4 Z 13 DSG[30] hinausgeht. Auch der im Rahmen der INTERPRETER-Architektur durchgeführte Informationsaustausch zur Erstellung eines gemeinsamen Lagebildes unterfällt der gemeinsamen Verarbeitung nach § 10 DSG.

Hervorzuheben ist auch der Umstand, dass in § 10 DSG keine Einschränkung auf bestimmte Verarbeitungsvorgänge vorgenommen wird. Nach der Vorgängerbestimmung des § 48a DSG 2000 waren Auftraggeber des öffentlichen Bereichs und Hilfsorganisationen ermächtigt, Daten zu «verwenden», wobei diese «Verwendung» gemäß § 4 Z 8 DSG 2000 als jede Art der Handhabung von Daten, also sowohl als Verarbeiten als auch als Übermitteln von Daten, definiert war. Der Gesetzgeber ging davon aus, dass auch das «Ermitteln» von Daten davon umfasst sein sollte.[31] Die Ersetzung der «Verwendung» durch die «Verarbeitung» führt diesbezüglich zu keinem anderen Ergebnis, da auch Art. 4 Z 2 DSGVO unter anderem sowohl ein Erheben, Erfassen und eine Speicherung, als auch eine Übermittlung umfasst, wodurch sich inhaltlich im Vergleich zur «Verwendung» durch die Geltung der DSGVO keine Änderung ergibt. Aufgrund der engen Zweckbindung des § 10 DSG erscheint diese weitreichende Erlaubnis auch in Hinblick auf Art. 9 Abs. 2 lit. c und g DSGVO zulässig.

Bemerkenswert ist noch, dass § 10 DSG keine Einschränkung dahingehend trifft, auf wen sich die Daten, welche gemeinsam verarbeitet werden, beziehen. So muss der Betroffene iSd Art. 4 Z 1 DSGVO nicht zwingend auch der Nutznießer des Verarbeitungsvorganges sein. Demnach ist auch die Verarbeitung von personenbezogenen Daten von Beistehenden, Einsatzkräften oder sonstigen Personen umfasst, sofern dies zur Hilfeleistung für durch eine Katastrophe unmittelbar betroffene Personen notwendig ist.

Im Ergebnis erlaubt § 10 DSG als nationale gesetzliche Bestimmung eine Datenverarbeitung für den Katastrophenschutz im Rahmen einer engen Zweckbindung, jedoch ohne Beschränkungen hinsichtlich der Verarbeitungsvorgänge oder Datenkategorien und erlaubt daher den dadurch befugten Verantwortlichen (Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen) auch eine umfassende Nutzung einer Systemarchitektur, wie sie im Rahmen des Projektes INTERPRETER realisiert wurde.

### 3.3. Bevölkerungsinformationssystem

Wird nun die Bevölkerung in die Lagebild-Erstellung eingebunden, kann diese hinsichtlich der Verarbeitung personenbezogener Daten grundsätzlich nicht auf die Ermächtigung des § 10 Abs. 1 DSG i.V.m. Art. 6 Abs. 1 lit. e DSGVO zurückgreifen. Verarbeitungstätigkeiten von freiwilligen Helfern und Nutzern der App, welche sich an der Lagebilderstellung beteiligen möchten, jedoch keiner öffentlichen Einrichtung oder Hilfsorganisation die im Katastrophenschutz tätig wird zugerechnet werden können, sind schließlich von § 10 DSG nicht umfasst.

Bei der Nutzung der INTERPRETER-App sollte, um die datenschutzrechtliche Prüfung zu erleichtern, zwischen den einzelnen Verarbeitungsschritten unterschieden werden. Grob kann dies in folgender Dreiteilung geschehen:

1. Der Nutzer der App generiert personenbezogene Daten;
2. Upload durch den Nutzer über die Applikation;
3. (Folge-)Verarbeitungen im Datenhub.

Schritt 1. und 2. erfolgen grundsätzlich in der Verantwortlichkeit des jeweiligen Nutzers. Auch unter Berücksichtigung der aktuellen Judikatur des EuGH zur datenschutzrechtlichen Rollenverteilung weiterhin anzunehmen sein, dass es sich dabei um eine separate bzw. alleinige Verantwortlichkeit des Nutzers handelt, da die bloße Bereitstellung einer Infrastruktur bzw. der Möglichkeit zur Kontaktaufnahme nicht die erforderli-

[30] «Informationsverbundsystem»: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden. (§ 4 Z 13 DSG).

[31] AB zu §48a DSG 821 BlgNR 22. GP 4.

che Verbindung der verarbeitenden Personen zur Folge hat, wie sie der EuGH in den Rechtssachen C-210/16 («Wirtschaftsakademie Schleswig-Holstein») und C-25/17 («Jehovan todistajat») weiterhin für gemeinsame Verarbeitung voraussetzt. So mag zwar selbst der Betreiber einer Fanpage für u. a. für das Setzen von Cookies durch Facebook (gemeinsam mit Facebook) verantwortlich sein, ebenso wie die Gemeinschaft der Zeugen Jehovas für die Verarbeitungsvorgänge, welche von ihren «Verkündern» gesetzt werden, jedoch hatte in diesen Konstellationen[32] die streitgegenständliche Partei stets noch einen gewissen Einfluss auf die Verarbeitungstätigkeit, welcher über die bloße Ermöglichung/Ermunterung zur Datenverarbeitung hinausging.[33] Nur unter diesen Voraussetzungen, wurde eine (gemeinsame) Festlegung der Zwecke und Mittel angenommen.

Selbst wenn man hinsichtlich einer allfälligen gemeinsamen Verantwortlichkeit zu einem anderen Ergebnis kommen sollte, bedürfte es einer Rechtsgrundlage für die Verarbeitungstätigkeiten des Nutzers, welche (s.o.) außerhalb von § 10 Abs. 1 DSG zu suchen wäre. Eine alleinige Verantwortlichkeit des Betreibers des Datenhubs für die Verarbeitungsvorgänge des Nutzers kann ausgeschlossen werden.

Die Verarbeitung personenbezogener Daten durch den Nutzer könnte etwa auf die Erforderlichkeit zur Wahrung lebenswichtiger oder berechtigter Interessen des Betroffenen oder einer anderen natürlichen Person nach Art. 6 Abs. 1 lit. c und f DSGVO sowie auf § 10 Abs. 2 DSG i.V.m. Art. 6 Abs. 1 lit. e DSGVO gestützt werden. Auf die zusätzlichen Anforderungen bei der Verarbeitung von sensiblen Daten und Bildaufnahmen sei hier lediglich hingewiesen.

### 3.4. Privacy-by-Design & ein Ausblick

Die entwickelte technische Lösung lässt sich derzeit sehr leicht in den datenschutzrechtlichen Rahmen einfügen. Aufbauend auf den Proof-of-Concept bieten sich noch Möglichkeiten für weitere Maßnahmen, um – nach dem Grundsatz Privacy-by-Design – die Rechte der betroffenen Personen zusätzlich zu schützen. Neben der Beschränkung der Nutzung der Applikation auf geschulte und in das Katastrophenschutzmanagement eingebundene Personen, wie dies etwa bereits im Rahmen der Katastrophenschutzübung Murau 2018 erfolgte[34], können auch technische Vorkehrungen getroffen werden.

Dazu empfiehlt sich ein Vorgehen nach den von der ENISA[35] empfohlenen Strategien MINIMISE, HIDE, SEPERATE, AGGREGATE, INFORM, CONTROL, ENFORCE und DEMONSTRATE.[36] Da der Fokus in Art. 25 DSGVO insbesondere auf der Datenminimierung liegt, sollten insbesondere jene personenbezogenen Daten, die für den Zweck inadäquat, unerheblich, oder entbehrlich sind vermieden werden.[37] Damit rückt auch der Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO in den Vordergrund. Demnach ist eine Erhebung von Daten ohne festgelegten eindeutigen und legitimen Zweck nicht gestattet.[38] Auch die Speicherzeitbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO, welche die Zweckbindung um ein zeitliches Element ergänzt, ist hier zu beachten. Nach diesem Grundsatz dürfen Daten zu einem bestimmten Zweck nur solange gespei-

---

32 In EuGH 5. Juni 2018, C-210/16 («Wirtschaftsakademie Schleswig-Holstein») etwa das Setzen der Parameter für die Analyse durch Facebook sowie die Statistik, welche von Facebook dem Fanpage-Betreiber zur Verfügung gestellt wird; in EuGH 5. Juni 2018, C-25/17 («Jehovan todistajat») die Ermunterung zu und der Organisation der Verkündungstätigkeit durch die Gemeinschaft auf Grundlage der gesammelten Informationen.

33 Festlegung der Parameter für die Auswertung der durch Facebook verarbeiteten Daten durch den Fanpagebetreiber bzw. Organisation der Verkündigungstätigkeit durch die Zeugen Jehovas.

34 Dabei wurde im Rahmen einer Katastrophenschutzübung unter der Leitung und Organisation der Landeswarnzentrale Steiermark die INTERPRETER-Systemarchitektur genutzt, einschließlich des Bevölkerungsinformationssystems bzw. der Ereignis-Melde-Applikation (EMA). Der Test der EMA wurde von Mitgliedern der steiermärkischen Berg- und Naturwacht im simulierten Einsatz durchgeführt.

35 The European Union Agency for Network and Information Security.

36 ENISA, Privacy and Data Protection by Design (2014) 19ff (zuletzt aufgerufen am 21.12.2018 unter: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design).

37 Reimer in Sydow, Europäische Datenschutzgrundverordnung: Handkommentar$^2$ (2018) Art 5 Rz 29.

38 Reimer in Sydow, Europäische Datenschutzgrundverordnung: Handkommentar$^2$ (2018) Art 15 Rz 18.

chert werden, solange sie für ebenjenen Zweck benötigt werden.[39] Da es bei den dargestellten Grundsätzen keine allgemein gültige Lösung gibt, muss die technische Umsetzung unter Berücksichtigung des jeweiligen Systems erfolgen.[40]

Derzeit werden die Empfänger von Meldungen im System durch den jeweiligen Bearbeiter ausgewählt. Hier wurde im Rahmen des Projektes bereits angedacht, diese Auswahl zukünftig durch die Nutzung von eingebauten Filtern zu ergänzen. Ziel ist es, diesfalls die Daten automatisch allen Organisationen mitzuteilen, welche diese Informationen für eine effiziente Erfüllung ihrer gesetzlichen Aufgaben benötigen, dabei allerdings die ausgetauschten Informationen abhängig vom Empfänger und der Rolle im Katastrophenmanagement auf den erforderlichen Umfang und die erforderliche Detaildichte zu beschränken, da die verschiedenen Akteure unterschiedliche Informationen benötigen. So werden von den Akteuren im Regelfall nur die wesentlichen, für die Erstellung eines Lagebildes erforderlichen Informationen benötigt, während bei einem Rettungseinsatz die Einsatzkräfte auch Informationen hinsichtlich der betroffenen Personen zu Verletzungsgrad oä. benötigen.

Die angedachte Kategorisierung hat sich dabei jedoch nicht an den im Datenschutzrecht gebräuchlichen Kategorien («personenbezogen», «besondere Kategorien personenbezogener Daten») zu orientieren, sondern aufbauend auf gewissen Grundinformationen für das Lagebild (Schadlage [Autounfall, Gebäudeeinsturz, Murenabgang, etc.], Ort und Status der Schadstelle) jeweils weitere Detailstufen zu unterschiedlichen Merkmalen (etwa Anzahl involvierter Personen, deren Status [verletzt, eingeschlossen]; Verletzungsbild) zu beinhalten, welche nur mit der entsprechenden Autorisierung eingesehen werden können.

Ein solches System aus vorangehender Kategorisierung und automatisierter Filterung bedarf jedoch einer Möglichkeit zur Reaktion auf unvorhergesehene Situationen und Änderungen in der Rolle der beteiligten Akteure. Daher sollte die Zugriffskontrolle entsprechend dynamisch gestaltet sein und entsprechende Anpassungen auf schnelle und einfache Art gestatten.

## 4. Fazit

Die Entwicklung neuer Technologien und deren Einbeziehung in Bereichen wie dem Katastrophenmanagement sind mit zahlreichen Rechtsfragen verknüpft, von denen in diesem Beitrag nur ein kleiner Ausschnitt dargestellt werden konnte. Zusammenfassend sind die europäischen Vorgaben im Datenschutzrecht auch im Katastrophenmanagement grundsätzlich zu beachten, wenngleich dem nationalen Gesetzgeber ein weiterer Regelungsspielraum offensteht. Der österreichische Gesetzgeber führt in § 10 DSG die Sonderbestimmung zur Datenverarbeitung im Katastrophenfall des § 48a DSG(alt) fort und ermöglicht damit trotz Anwendbarkeit der Bestimmungen der DSGVO eine weitgehende Nutzung der dem Projekt INTERPRETER zugrunde liegendem Systemarchitektur. Darüber hinaus kann der Austausch von Informationen im Rahmen der Amtshilfe und unter Berücksichtigung der gesetzlichen Befugnisse der jeweiligen Akteure über das System erfolgen. In weiterer Folge sind insbesondere noch Maßnahmen des Datenschutzes durch Technikgestaltung anzustellen bzw. weiterzuführen und in der praktischen Anwendung zu testen.

## 5. Danksagung

Das Projekt INTERPRETER wird im Rahmen des Sicherheitsforschungs-Förderungsprogrammes KIRAS über die Österreichische Forschungsförderungsgesellschaft vom Bundesministerium Digitalisierung und Wirtschaftsstandort sowie dem Bundesministerium für Verkehr, Innovation und Technologie finanziert.

[39] Frenzel in Paal/Pauly, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz[2] (Beck'sche Kompakt-Kommentare 2018) Art 5 Rz 43.

[40] Vgl. Hötzendorfer in Knyrim, Datenschutz-Grundverordnung: Praxishandbuch (2016) 148.

## 6. Literatur

Bresich, Ronald/Dopplinger, Lorenz/Dörnhofer, Stefanie/Kunnert, Gerhard/Riedl, Eckhard, DSG, Datenschutzgesetz: Kommentar, Linde, Wien 2018

Dohr, Walter/Weiss, Ernst M. /Pollirer, Hans-Jürgen /Knyrim, Rainer, Kommentar Datenschutzrecht[2], Manz, Wien 2017

Feiler, Lukas/Forgó, Nikolaus, EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkommentar, Verlag Österreich, Wien 2017

Gola, Peter, Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar[2], C.H. Beck, München 2018

Jahnel, Dietmar, Handbuch Datenschutzrecht, Jan Sramek Verlag, Wien 2010

Knyrim, Rainer, Datenschutz-Grundverordnung: Praxishandbuch, MANZ, Wien 2016

Knyrim, Rainer, DatKomm Praxiskommentar zum Datenschutzrecht – DSGVO und DSG (2018)

Kühling, Jürgen/Buchner, Benedikt, Datenschutz-Grundverordnung/BDSG: Kommentar[2], C.H. Beck, München 2018

Paal, Boris P. /Pauly, Daniel A., Datenschutz-Grundverordnung, Bundesdatenschutzgesetz[2], C.H. Beck, München 2018

Sydow, Gernot, Europäische Datenschutzgrundverordnung: Handkommentar[2], Nomos, Baden-Baden 2018