ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Durchführung der ersten Datenschutz-Vorsorge

Ein Planspiel

Von Alina Boll und Ines Geissler

Impressum

Kontakt
Nationales Forschungszentrum für angewandte
Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Inhalt

1. Einleitung

Insbesondere im Bereich der wissenschaftlichen Forschung[1] ist eine Verarbeitung personenbezogener Daten nicht immer das primäre Ziel einer Forschungsaktivität, kann aber im Vorfeld nicht immer vorhergesehen und/oder geplant werden. Da das aktuelle Datenschutzsystem der europäischen Union (weitestgehend) unvorhersehbare und unplanbare Verarbeitungen personenbezogener Daten nicht vorsieht, besteht für Forschende eine erhebliche Rechtsunsicherheit in Bezug auf derartige Datenverarbeitungen.[2] Daher herrscht insbesondere in der Forschung ein dringender Bedarf, das bestehende Datenschutzrechtssystem der europäischen Union durch ein neues Instrument zu erweitern, welches unvorhersehbare und unplanbare Datenverarbeitungen rechtskonform ermöglicht.

Ein solches Instrument wurde von Wissenschaftlerinnen des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE vorgeschlagen und „Datenschutz-Vorsorge" (kurz: „DS-V") genannt. Durch die DS-V sollen (weitestgehend) unvorhersehbare und unplanbare Verarbeitungen personenbezogener Daten einen rechtlichen „Mantel" erhalten, indem Verantwortliche dazu verpflichtet werden, Annahmen zu der ggf. bevorstehenden Verarbeitung zu treffen, die Aufschluss darüber geben, ob diese wahrscheinlich personenbezogene Daten enthalten und/oder mit einem hohen Risiko für die Rechte und Freiheiten betroffener Personen verbunden sein wird. Für hinreichend wahrscheinliche und/oder voraussichtlich besonders risikobehaftete Datenverarbeitungen soll der Verantwortliche sodann verpflichtet sein, datenschutzrechtliche Kernaspekte angemessen umzusetzen, bevor es zu der personenbezogenen Datenverarbeitung kommt. Insofern sollen durch die DS-V bei personenbezogenen Datenverarbeitungen, die als wahrscheinlich eingestuft werden oder (in Einzelfällen) mit einem hohen Risiko für die betroffenen Personen verbunden wären, die Pflichten der DSGVO bereits in den Bereich der Verarbeitung nicht-personenbezogener Daten vorverlagert werden – also Datenschutzanforderungen schon umgesetzt werden, wenn noch nicht sicher feststeht, ob diese überhaupt erfolgen wird. Hierdurch soll für eine datenschutzkonforme Verarbeitung personenbezogener Daten gesorgt werden, falls es zu einer solchen kommen sollte.[3] Die DS-V beinhaltet die folgenden sechs Schritte:

1. Die umfassende Beschreibung der geplanten Verarbeitungstätigkeit (hier: Forschungsaktivität), inkl. der hinreichend wahrscheinlichen Verarbeitungen personenbezogener Daten und Verarbeitungsumständen.
2. Die Identifizierung einschlägiger Rechtsgrundlagen für diese ggf. erfolgenden Verarbeitungen personenbezogener Daten.
3. Die Bewertung des Bestehens von Informationspflichten im Rahmen der ggf. erfolgenden Verarbeitungen personenbezogener Daten und ggf. die Umsetzungsvorbereitung.
4. Die Identifizierung geeigneter technischer und organisatorischer Maßnahmen für die ggf. erfolgenden Verarbeitungen personenbezogener Daten sowie deren Umsetzung.
5. Die fortlaufende Betreuung des Datenschutzes im Wirkbetrieb der Verarbeitungstätigkeit (hier: Forschungsaktivität).
6. Die Dokumentation aller vorgenannten Schritte.

Im Rahmen der Konzeption und Ausgestaltung der DS-V wurde auch ein konkreter Vorschlag zur Ergänzung der DSGVO um das Instrument der DS-V erarbeitet.[4] Eine solche Ergänzung ist wünschenswert, um die Rechtssicherheit im Bereich unvorhersehbarer und unplanbarer Verarbeitungen personenbezogener Daten zu erhöhen.

2. Erste Umsetzung einer Datenschutz-Vorsorge im Rahmen eines Planspiels

Basierend auf der erfolgten Konzeption und Ausgestaltung sowie dem Ergänzungsvorschlag der DSGVO hat die Autorin *Boll* in den vergangenen Monaten im Rahmen eines Planspiels die erste exemplarische Umsetzung einer DS-V vorgenommen. Die vorliegende Ausarbeitung skizziert zunächst die Durchführung dieser exemplarischen Umsetzung einer DS-V und stellt darauffolgend Auszüge aus der Dokumentation dieser zur Verfügung, um wichtige Anhaltspunkte zur Umsetzung einer DS-V zu geben.

---

[1] Hierbei ist speziell die Cybersicherheitsforschung Auslöser der Problemidentifikation gewesen, der den Vorschlag der Datenschutz-Vorsorge motiviert hat, vgl.: *Boll/Selzer/Spiecker,* Tagesspiegel 2023.
[2] *Boll/Selzer/Spiecker,* Tagesspiegel 2023. Weiter ausgeführt in: *Selzer/Spiecker/Boll,* DuD 2023, 785 ff.; *Boll/Stummer/Selzer*, DuD 2024, 172 ff.; *Boll/Stummer*, DuD 2024, 118 ff.
[3] *Boll/Stummer*, DuD 2024, S. 118.
[4] *Boll,* DuD 2023, S. 785 ff.; *Boll/Selzer,* DuD 2024, S. 44 ff.; *Boll/Stummer*, DuD 2024, S. 118 ff.; *Boll/Stummer/Selzer*, DuD 2024, S. 172 ff.; *Boll/Stummer/Selzer,* Positionspapier zur zweiten DSGVO-Evaluation 2024; *Boll,* DuD 2024, S.383 ff.

2.1 Fallbeispiel

Der praktischen Umsetzung der DS-V im Rahmen des Planspiels lag folgendes Fallbeispiel zugrunde:

Die Cybersicherheitsforschende C arbeitet für eine Cybersicherheitsforschungseinrichtung F und befasst sich im Rahmen eines Forschungsprojektes mit neuen Cyberangriffsmethoden. Ziel des Projektes ist es, neue Cyberangriffsmethoden und ggf. Gegenmaßnahmen schnellstmöglich zu identifizieren und einen durch die neue Cyberangriffsmethode entstandenen Schaden einzuschätzen. Insbesondere für letztgenannten Schritt ist C auf Darknet-Recherchen angewiesen.

Während ihrer Forschungsarbeit entdeckt C eine neue Cyberangriffsmethode. Um die neue Cyberangriffsmethode wissenschaftlich zu untersuchen, die dahinterliegenden Angriffsmuster besser zu verstehen und den durch die neue Cyberangriffsmethode entstandenen Schaden einschätzen zu können, möchte C eine Darknet-Recherche durchführen. Durch diese möchte sie insbesondere auch herausfinden, ob im Darknet bereits Angebote existieren, mit Hilfe der neuen Cyberangriffsmethode gestohlene Daten zu kaufen.

Durch Vorerfahrungen aus ähnlichen Forschungsprojekten ist C bewusst, dass Darknet-Recherchen in Bezug auf personenbezogene Daten unberechenbar sind. C kann nicht ausschließen, im Rahmen ihrer Darknet-Recherche gestohlene Daten aufzufinden, ohne dass dies für sie vor dem Datenzugriff ersichtlich wäre. C weiß nicht, ob darunter auch personenbezogene Daten sein werden. Falls dem so wäre, kann sie ebenso wenig einschätzen, welche, wie viele und welche Kategorien von personenbezogenen Daten sie bei ihrer Suche einsehen könnte.

C kann lediglich aufgrund der Vorerfahrungen einschätzen, dass bei der Darknet-Recherche eine gewisse Wahrscheinlichkeit besteht, dass sie bei ihrer Suche auf personenbezogene Daten treffen wird. In ähnlichen Projekten der F wurden jedoch noch nie besondere Kategorien personenbezogener Daten gefunden. C möchte nun die datenschutzkonforme Umsetzung des Forschungsvorhabens im Rahmen einer DS-V vorbereiten und wendet sich hierzu an ihre Vorgesetzte, die Verfahrenseignerin V.

2.2 Zeitrahmen

Die Umsetzung der ersten DS-V im Rahmen eines Planspiels erfolgte vom 11.3.24 bis zum 22.4.24. Die Dokumentation des Planspiels erfolgte mit dessen Beginn ab dem 11.3.24 und dauerte nach Ende des Planspiels noch bis zum 13.5.24 an.

2.3 Beteiligte

An dem Planspiel waren beteiligt:

- die Verfahrenseignerin der Forschungsaktivität (**V**),
- die Cybersicherheitsforschungseinrichtung als Verantwortliche, vertreten durch eine delegierte Person (**F**),
- die Cybersicherheitsforschende (**C**),
- die Datenschutzbeauftragte der F (**D**),
- der Informationssicherheitsbeauftragter der F (**I**),[5]
- der Auftragsverarbeiter (**A**) und
- 3 potenziell betroffene Personen.

[5] Die Einbeziehung dieser Rolle findet im DSGVO-Vorschlag zur DS-V keine Erwähnung, sie erfolgte jedoch zur Unterstützung der Umsetzung von TOMs entsprechend der gängigen Praxis.

2.4 Durchführungsstationen

Die DS-V wurde anhand der sechs skizzierten Schritte durchgeführt. Die Umsetzung der DS-V – inkl. Simulation der Wirkbetrieb-Datenerhebung – erfolgte vorwiegend durch die Autorin *Boll* der vorliegenden Ausarbeitung, die im Planspiel die Rolle der V einnahm. Die weiteren Rollen wurden im Rahmen von Gesprächen, Workshops und E-Mail-Abstimmungen wie folgt eingebunden:

- Insgesamt wurden im Rahmen des Planspiels sieben Gesprächstermine und Workshops durchgeführt,
  - davon vier zwischen V, F und D (zur Planung der Schritte 1 bis 6),
  - einer zwischen der D und I (zur Freigabe der identifizierten, seitens F zu treffenden technischen und organisatorischen Maßnahmen) und
  - einer zwischen D und drei potenziell betroffenen Personen (zur Information und Einholen von Standpunkten über die geplante Forschungsaktivität, den datenschutzrechtlichen Rahmen sowie die im Rahmen der DS-V getroffenen Maßnahmen).
  - einer zwischen V und D (zur Betreuung im Wirkbetrieb).
- Zusätzlich erfolgte zwischen V, F und der D im Anschluss an jeden Umsetzungsschritt mind. ein Austausch per E-Mail, um Zwischenstände der Dokumentationen auszutauschen. Ebenfalls fand ein E-Mail-Wechsel zwischen V und dem eingesetzten A zu den von ihm eingesetzten technischen und organisatorischen Maßnahmen statt. Diese sowie die bei F umzusetzenden Maßnahmen waren ebenfalls Gegenstand eines E-Mail-Wechsels zwischen V und I.

2.5 Gewonnene Erkenntnisse zum Aufwand

Um Anhaltspunkte dafür zu geben, mit wie viel Aufwand die Durchführung einer DS-V verbunden ist, werden nachfolgend die Aufwände der einzelnen Rollen in Stunden angegeben:

- V hatte im Rahmen der Umsetzung der DS-V den meisten Aufwand, nämlich 46,25 Stunden.
- F hatte einen Aufwand von 4,50 Stunden für die Teilnahme an Besprechungen.
- D hatte einen Aufwand von 19,00 Stunden für die Teilnahme an Besprechungen sowie für die inhaltliche Beratung und Kommentierung per E-Mail.
- I hatte 2,5 Stunden Aufwand für die Teilnahme an einer Besprechung sowie für die inhaltliche Beratung und Kommentierung per E-Mail.
- A hatte einen Aufwand von 1 Stunde für die Überprüfung des Auftragsverarbeitungsvertrags und der Erstellung seiner TOMs
- Die drei einbezogenen betroffenen Personen hatten einen Aufwand von je 1,5 Stunden zur Teilnahme an einem Workshop.

Insgesamt betrug der Aufwand zur Durchführung der DS-V somit 77,75 Stunden. Zu berücksichtigen ist hierbei, dass die DS-V unter der Annahme durchgeführt wurde, dass bei der F – außerhalb des Verarbeitungskontextes, für den die DS-V durchgeführt wird – bereits Prozesse zur Umsetzung von Betroffenenrechten etabliert wurden, technische und organisatorische Maßnahmen implementiert wurden, Löschkonzepte sowie Mitarbeiteranweisungen zur Umsetzung des Datenschutzrechts bestehen. Der Aufwand der DS-V-Umsetzung wird daher stark vom Umsetzungsstand datenschutzrechtlicher Anforderungen beim Verantwortlichen abhängen.

3. Dokumentation

Jede Verarbeitung personenbezogener Daten in Organisationen hat gemäß den datenschutzrechtlichen Vorgaben zu erfolgen. Organisationen müssen diese Konformität im Rahmen ihrer Rechenschaftspflicht nachweisen. Die Einführung des neu vorgeschlagenen Instruments der DS-V würde Möglichkeiten eröffnen, um Verarbeitungen personenbezogener Daten rechtssicherer zu gestalten, die vor Verarbeitungsbeginn weder sicher vorhersehbar noch planbar sind. Die folgende Dokumentation zu dem Planspiel soll einerseits ein besseres Verständnis für die Notwendigkeit und den Nutzen dieses Instruments ermöglichen sowie andererseits dazu beitragen, wichtige Hilfestellungen bei der Umsetzung einer möglicherweise zukünftig gewünschten oder erforderlichen eigenen DS-V zu geben.

Schritt 1	
Beschreibung des Forschungszwecks	**Benennung des Zwecks:** Die geplante Forschungsaktivität im Darknet dient dem wissenschaftlichen Zweck der Beibehaltung und potenziellen Widerherstellung der Cybersicherheit sowie dem Schutz der Gesellschaft, u.a. in Bezug auf den Schutz vor Angriffen Kritischer Infrastrukturen und der unberechtigten Verarbeitung personenbezogener Daten und damit einhergehender Eingriffe in die Rechte und Freiheiten betroffener Personen.
	Übergeordnetes Ziel der Zweckerreichung: Ziel der Recherche im Darknet ist es, Informationen über neue Cyberangriffsmethoden zu erlangen. Durch diese Informationen sollen neue Cyberangriffsmethoden schnellstmöglich identifiziert werden können. Ebenso sollen hierdurch ggf. schnellstmöglich geeignete Gegenmaßnahmen identifiziert werden, um einen Cyberangriff mittels einer neuen Cyberangriffsmethode erfolgreich abwenden zu können. Durch die Recherche im Darknet soll darüber hinaus ggf. der durch die neue Cyberangriffsmethode entstandene Schaden im Zeitraum zwischen erstmaligem Identifizieren der Angriffsmethode und Identifizieren der Gegenmaßnahmen eingeschätzt werden.
Beschreibung der Forschungsnotwendigkeit	**Feststellung der Notwendigkeit:** Die wissenschaftliche Notwendigkeit der Recherche im Darknet liegt in der kontinuierlichen Weiterentwicklung der Cybersicherheit, der proaktiven Bekämpfung von Cyberbedrohungen sowie der Einschätzung von Schäden und dem damit verbundenen Schutz der Rechte und Freiheiten betroffener Personen.
	Begründung der Notwendigkeit: Die Erreichung des Forschungsziels ist von entscheidender Bedeutung, da eine erfolgreiche Identifizierung neuer Angriffsmethoden und die Entwicklung entsprechender Abwehrmaßnahmen dazu beitragen, die Integrität und Vertraulichkeit schützenswerter Daten (zu denen auch personenbezogene Daten zählen können) aufrecht zu erhalten. Die Schadensbewertung trägt dazu bei, das Ausmaß des Schadens zu erkennen und betroffenen Personen gegebenenfalls angemessene Reaktionsmöglichkeiten zu bieten. Falls das Ziel der Forschung nicht erreicht werden würde, könnten erhebliche Gefahren und Risiken für die Gesellschaft eintreten. Die schnelle Identifikation neuer Angriffsmethoden und die Entwicklung von Gegenmaßnahmen sind notwendig, um Angriffe auf IT-Infrastrukturen, Systeme und Anwendungen sowie die darin verarbeiteten Daten einzudämmen oder zu verhindern. Die Schadensidentifikation hilft dabei, das Ausmaß und die Art der Schäden zu erkennen, sodass betroffene Personen und Organisationen angemessen reagieren können. Dies schützt die Gesellschaft vor Identitäts- und Datendiebstählen sowie vor Angriffen auf Kritische Infrastrukturen.
	Diskussion milderer Mittel: Mildere Mittel, die den Forschungszweck in gleicher zufriedenstellender Weise erreichen könnten, stehen vorliegend nicht zur Verfügung. Es stehen insbesondere keine Mittel zur Verfügung, im Rahmen derer eine personenbezogene Datenverarbeitung ausgeschlossen oder planbar wäre. Informationen über neuartige Cyberangriffsmethoden oder gestohlene Daten sind i.d.R. nicht im öffentlich zugänglichen Clear Web frei verfügbar. Diese Informationen werden im Darknet preisgegeben, da es sich hierbei um Informationen handelt, denen zumeist Straftaten zugrunde liegen, sodass die Herausgeber dieser Informationen unentdeckt bleiben wollen. Daher ist eine Recherche im Darknet unerlässlich, um den wissenschaftlichen Zweck zu erreichen. Die Kennzeichnung potenzieller Daten als personenbezogen liegt hierbei nicht in den Händen der Forschenden, sondern in den Händen der straftatverübenden Personen, die wiederum – z.T. aus Versehen, z.T. aber auch bewusst – vor dem Datenzugriff nicht erkennbar machen, auf welche Daten zugegriffen wird.
Beschreibung der Forschungsaktivität	**Beschreibung des Vorgehens:** Um Zugang zum Darknet zu erhalten, nutzt C den Tor-Browser, der ihr den Eintritt in Darknet-Märkte und -Foren ermöglicht. Die C beginnt zunächst damit, sich im Darknet über neue Angriffsmethoden zu informieren und nutzt bei ihrer Suche verschiedene Darknet-Suchmaschinen, um Informationen über den neuen Cyberangriff zu erhalten. Dabei sucht sie gezielt nach Hinweisen, Taktiken, Techniken und Tools, die von Angreifern genutzt werden könnten, um Informationen zu erhalten, die auf neue Cyberangriffsmethoden hindeuten. Die Suche beschränkt sich auf Schlagwörter, die mit der (initial identifizierten) neuen Angriffsmethode im Zusammenhang stehen. Falls direkte Informationen über die neue Cyberangriffsmethode die Nutzung der Suchmaschinen nicht verfügbar sind, beteiligt sie sich an Diskussionen in Foren, stellt Fragen und tauscht sich mit anderen Mitgliedern der Darknet-Community aus, um Einblicke und ggf. hilfreiche Informationen über neue Cyberangriffsmethoden zu erhalten. Darüber hinaus überwacht sie Darknet-Foren und Blogs, die regelmäßig neue Informationen über Angriffsmethoden und Schwachstellen veröffentlichen.
	Beschreibung der geplanten Sicherheitsmaßnahmen/des Vorgehens zur Erhöhung der Cybersicherheit: Nach Identifizierung einer neuen Angriffsmethode versucht C – basierend auf den recherchierten Informationen – Gegenmaßnahmen abzuleiten. Zusätzlich prüft die C, ob im Darknet bereits Angebote existieren, einen Cyberangriff basierend auf der neuen Angriffsmethode gegen Bezahlung durchzuführen oder gestohlene Daten gegen Bezahlung zu veräußern. Bei der Suche nach Verkaufsangeboten über gestohlene Daten beschränkt sich C auf Angebote, die einen konkreten Hinweis darauf enthalten, dass sie mit dem stattgefundenen Cyberangriff in Verbindung gestanden haben.
	Geplante Dauer der Forschungsaktivität: Für die Forschungsaktivität ist zunächst ein zeitlicher Rahmen von drei Monaten vorgesehen.

Beschreibung der wahrscheinlichen Datenverarbeitung	**Wahrscheinliche Verarbeitung personenbezogener Daten:** Aus den Erfahrungen früherer Recherchen der F im Darknet kann gefolgert werden, dass die Wahrscheinlichkeit besteht, dass im Rahmen von Darknet-Recherchen Daten aufgerufen werden könnten, die aus früheren Angriffen auf Unternehmen stammen. Bei den Daten könnte es sich demnach wahrscheinlich um Kundenstammdaten oder Log-In-Daten und somit um personenbezogene Daten handeln: - Kundenstammdaten: Namen, Geburtsdaten und andere demografische Informationen von Kunden eines Unternehmens. - Log-In-Daten: Benutzernamen, Passwörter, PIN-Codes und andere Zugangsdaten, die für den Zugriff auf Online-Konten oder Systeme verwendet werden. Aufgrund der Vorerfahrungen der F kann außerdem die Annahme getroffen werden, dass es sich bei den betroffenen Personen um Kunden oder Arbeitnehmer von einem Unternehmen handelt, das in der Vergangenheit von einem Cyberangriff betroffen war. Dass dabei eine große Anzahl betroffener Personen und eine große Datenmenge involviert sind, ist nicht auszuschließen.
	Verarbeitung besonderer Datenkategorien und Daten über Straftaten: Aufgrund der technisch und inhaltlich eng gefassten Recherche, die sich ausschließlich auf indikatorspezifische Schlagwörter zum aktuellen Cyberangriff (z. B. Schadsoftware-Bezeichnungen, Ports) beschränkt, ist nicht davon auszugehen, dass hierbei (1) besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) oder (2) strafrechtlich relevante Daten (Art. 10 DSGVO) verarbeitet werden.
	Bestehen von Aufbewahrungspflichten: Es bestehen grundsätzlich keine Vorgaben externer Fördergeber, aus denen sich Aufbewahrungspflichten ergeben, die einer Löschung von für die Forschungsaktivität nicht benötigten personenbezogenen Daten (nach Ablauf ggf. bestehender gesetzlicher Fristen) im Wege stünden.
	Meldung an betroffene Personen: Ggf. kann es notwendig sein, die im Darknet gefundenen personenbezogenen Daten zu bereits stattgefundenen Cyberangriffen an die betroffenen Personen und betroffenen Unternehmen zu melden.
Schritt 2	
Identifizierung der Rechtsgrundlage für den Verantwortlichen	**Rechtsgrundlage für die Verarbeitung personenbezogener Daten:** ☐ *Einwilligung – Art. 6 Abs. 1 lit. a DSGVO* ☐ *Vertragsverhältnis – Art. 6 Abs. 1 lit. b DSGVO* ☐ *Gesetz / rechtliche Verpflichtung – Art. 6 Abs. 1 lit. c DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 6 Abs. 1 lit. d DSGVO* ☐ *Wahrung einer öffentlichen Aufgabe – Art. 6 Abs. 1 lit. e DSGVO* ☒ *Bestehen berechtigter Interessen – Art. 6 Abs. 1 lit. f DSGVO* ☐ *Sonstiges*:
	Begründung: <u>Bestehen eines berechtigten Interesses:</u> Sollten personenbezogene Daten verarbeitet werden, dient dies dazu, Erkenntnisse über neue Cyberangriffsmethoden zu generieren und daraus wiederum neue Gegenmaßnahmen zur Widerherstellung und Beibehaltung der Cybersicherheit zu entwickeln. Darüber hinaus werden die personenbezogenen Daten benötigt, um ggf. das Ausmaß des bereits durch eine neuartige Angriffsmethode entstandenen Schadens einschätzen zu können. Das berechtigte Interesse der F liegt folglich in der Weiterentwicklung der Cybersicherheitsforschung und der Abwendung von Gefahren für die Rechte und Freiheiten betroffener Personen. Da eine Verarbeitung der personenbezogenen Daten zu wissenschaftlichen Zwecken erfolgt und im Hinblick auf die in Art. 13 GRCh, Art. 10 EMRK sowie Art. 5 Abs. 3 Satz 1 GG verankerte Forschungsfreiheit als schutzwürdig anzusehen ist,[6] ist ein berechtigtes Interesse der F gegeben. Außerdem dient die Verarbeitung im Kontext von Cyberangriffen nicht nur dem eigenen Interesse der F, sondern hat auch eine gesamtgesellschaftliche Bedeutung, denn die Verhinderung von und der Schutz vor Cyberangriffen tragen zum Schutz der digitalen Infrastruktur und damit zum Schutz einer Vielzahl von Nutzern und Organisationen bei. Die Verarbeitung dient zudem den Interessen betroffener Organisationen und betroffener Personen. Sollten bei der Darknet-Recherche personenbezogene Daten verarbeitet werden, ist zu berücksichtigen, dass diese bereits öffentlich sind und hierdurch die Gefahr des Missbrauchs durch böswillige Dritte besteht. Die Erhebung durch F führt dagegen nicht nur dazu, dass künftige ähnlich gelagerte Fälle verhindert werden, sondern auch dazu, dass die betroffene Person in die Lage versetzt wird, Kenntnis darüber zu erlangen, dass ihre personenbezogenen Daten abgegriffen wurden, sodass sie selbst Gegenmaßnahmen ergreifen kann, insbesondere durch die Änderung ihrer betroffenen Zugangsdaten und ggf. auch auf anderen Plattformen. <u>Erforderlichkeit:</u> Ein milderes Mittel zur Umsetzung der Forschungsziele ist nicht ersichtlich, da Informationen über neue Cyberangriffsmethoden und die dadurch verursachten Schäden nur begrenzt im Clear Web zugänglich sind und diese Informationen regelmäßig nicht ausreichen, um konkrete Angriffsszenarien in Echtumgebungen zu verstehen oder individuelle Schwachstellen gezielt beheben zu können. Eine ausschließlich auf öffentlichen, generischen Informationen beruhende Analyse würde kein präzises Bild des

[6] *Böker*, in: Kipker Cybersecurity, Kap. 15 IT-Sicherheitsforschung, Rn. 13 f.

	tatsächlichen Angriffs liefern und damit auch keine verlässlichen Erkenntnisse für die Entwicklung zielgerichteter Schutzmaßnahmen ermöglichen. Somit ist kein milderes Mittel zur Umsetzung der Forschungsziele und folglich auch kein milderes Mittel einer ggf. erfolgenden personenbezogenen Datenverarbeitung gegeben. Abwägung der Interessen: Das Interesse der F an der Verarbeitung der personenbezogenen Daten müsste das Interesse der betroffenen Personen an einem Ausschluss der Verarbeitung überwiegen. Für ein Überwiegen des Interesses der F spricht zum einen das übergeordnete Ziel der Forschungsaktivität – konkret die Beibehaltung bzw. Wiederherstellung der Cybersicherheit sowie der daraus resultierende Schutz der Gesellschaft und der betroffenen Personen. Zum anderen spricht für ein überwiegendes Interesse an der Verarbeitung zu Forschungszwecken, die von dem Verordnungsgeber bspw. in Art. 5 Abs. 1 lit. b, e, Art. 9 Abs. 2 lit. j, Art. 14 Abs. 5 lit. b DSGVO oder den ErwG 33 DSGVO getroffene Priorisierung der wissenschaftlichen Forschung.[7] Ebenso ergibt sich aus Art. 3 Abs. 3 EUV und Art. 179 Abs. 1 AEUV, dass die Förderung des wissenschaftlichen Fortschritts und die Schaffung eines europäischen Raumes der Forschung Ziele der Europäischen Union sind. Da Cyberangriffe zunehmend Wirtschaft und Gesellschaft bedrohen, besteht zudem ein hohes öffentliches Interesse daran, neue Angriffsmethoden rasch zu erkennen und wirksame Gegenmaßnahmen sowie Präventionsstrategien zu entwickeln. Die Forschung auf diesem Gebiet genießt grundrechtlichen Schutz (Art. 5 Abs. 3 GG, Art. 13 GRCh), was das Interesse an einer wissenschaftlichen Analyse zusätzlich stärkt. Da sich die Forschungsaktivität auf die Identifizierung des Angriffs und Schadensanalysen konzentriert, werden keine umfassenden Verhaltensprofile der Betroffenen erstellt, sodass der Eingriff in deren Persönlichkeitsrechte in seiner Intensität begrenzt bleibt. Für ein Überwiegen des Interesses der F spricht zudem, dass die personenbezogenen Daten bereits durch böswillige Dritte veröffentlicht wurden. Die Verarbeitung durch F führt dazu, dass die betroffenen Personen Kenntnis über den Datenabgriff erlangen und dadurch in die Lage versetzt werden, selbst Gegenmaßnahmen zu ergreifen. Ergebnis: Unter Berücksichtigung des hohen Gewichts der Cybersicherheitsforschung, der starken gesellschaftlichen Relevanz von IT-Sicherheit und der vergleichsweise geringen Eingriffsintensität für betroffene Personen, überwiegt das Interesse der F an der Verarbeitung der personenbezogenen Daten. Das Interesse der betroffenen Person an einem vollständigen Ausschluss der Verarbeitung überwiegt hier somit nicht.
	Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten ☐ *Ausdrückliche Einwilligung – Art. 9 Abs. 2 lit. a DSGVO* ☐ *Arbeitsrecht, soziale Sicherheit, Sozialschutz – Art. 9 Abs. 2 lit. b DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 9 Abs. 2 lit. c DSGVO* ☐ *Politisch, weltanschaulich, religiös und gewerkschaftlich ausgerichtete Organisationen – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Selbst veröffentlichte Daten – Art. 9 Abs. 2 lit. e DSGVO* ☐ *Rechtsansprüche und Gerichtsverhandlungen – Art. 9 Abs. 2 lit. f DSGVO* ☐ *Erhebliches öffentliches Interesse – Art. 9 Abs. 2 lit. g DSGVO* ☐ *Gesundheits- und Sozialbereich – Art. 9 Abs. 2 lit. h DSGVO* ☐ *Öffentliche Gesundheit – Art. 9 Abs. 2 lit. i DSGVO* ☐ *Archiv-, Forschungs- und statistische Zwecke – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Sonstiges*:
	Begründung: Voraussichtlich werden keine besonderen Kategorien personenbezogener Daten verarbeitet.
Ggf. Identifizierung der Rechtsgrundlage für Datenweitergabe	**Rechtsgrundlage für die Verarbeitung personenbezogener Daten:** ☐ *Einwilligung – Art. 6 Abs. 1 lit. a DSGVO* ☐ *Vertragsverhältnis – Art. 6 Abs. 1 lit. b DSGVO* ☐ *Gesetz / rechtliche Verpflichtung – Art. 6 Abs. 1 lit. c DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 6 Abs. 1 lit. d DSGVO* ☐ *Wahrung einer öffentlichen Aufgabe – Art. 6 Abs. 1 lit. e DSGVO* ☒ *Bestehen berechtigter Interessen – Art. 6 Abs. 1 lit. f DSGVO* ☐ *Sonstiges*:

[7] *Böker,* in: Kipker Cybersecurity, Kap. 15 IT-Sicherheitsforschung, Rn. 13 f.

	Begründung: Bestehen eines berechtigten Interesses: Die F möchte Daten von betroffenen Personen an die übergeordnete, geschädigte Organisation weitergeben, damit diese ihre Kunden und Mitarbeiter als betroffene Personen über den Fund ihrer personenbezogenen Daten informieren kann. Hierbei sind nicht nur berechtigte Interessen des Verantwortlichen von Bedeutung, sondern auch solche betroffener Personen. Betroffenen eines Cybersicherheitsangriffs kann grundsätzlich ein berechtigtes Interesse an der Weitergabe ihrer im Darknet gefundenen personenbezogenen Daten an das übergeordnete Unternehmen unterstellt werden (hier bestehende Annahme: Diese werden dort ohnehin verarbeitet; bei Daten, die diese Voraussetzung nicht erfüllen, muss dieser Umstand separat in die Interessenabwägung einfließen), weil das übergeordnete Unternehmen und ggf. auch die betroffenen Personen selbst auf diese Weise möglichst frühzeitig über den Datenabfluss/die Veröffentlichung im Darknet informiert werden und gezielt Schutzmaßnahmen ergreifen können. Durch die frühzeitige Kenntnis kann das übergeordnete Unternehmen bspw. koordinierte Sicherheitsupdates, Passwortänderungen oder andere Risikominimierungen einleiten und die betroffenen Personen gezielt bei der Abwehr weiterer Schäden unterstützen. Gleichzeitig wird so auch die Erfüllung eventueller rechtlicher Benachrichtigungspflichten (etwa gem. Art. 34 DSGVO) erleichtert, die sich aus einem Datenschutzvorfall ergeben können. Erforderlichkeit: Das übergeordnete Unternehmen kann ggf. bestehende Benachrichtigungspflichten nur nachkommen, wenn es selbst hinreichend über einen möglichen Datenschutzvorfall im Darknet informiert ist und weiß, welche seiner Mitarbeiter/Kunden von dem Vorfall betroffen sind. Ein milderes Mittel könnte darin liegen, das übergeordnete Unternehmen generisch über den Datenfund im Darknet zu informieren, jedoch würde es sich hierbei regelmäßig um kein tatsächlich milderes Mittel handeln, da die betreffenden Daten ggf. frei im Darknet liegen und daher auch von dem übergeordneten Unternehmen dort einsehbar wären. Insofern scheint die (direkte) Datenweitergabe an das übergeordnete Unternehmen mit direkten Vorteilen für die betroffenen Personen verbunden zu sein, schnell als von einem Datenschutzvorfall betroffene Person identifiziert werden zu können, um z.B. konkrete Handlungsempfehlungen an diese geben zu können. Die Weitergabe kann somit im Ergebnis als erforderlich eingestuft werden (hier bestehende Annahme: Siehe „Bestehen eines berechtigten Interesses“). Abwägung der Interessen: Das Interesse der F an der Weitergabe der personenbezogenen Daten müsste das Interesse der betroffenen Personen an einem Ausschluss der Verarbeitung überwiegen. Für ein Überwiegen des Interesses an der Weitergabe spricht zum einen, das Erfüllen von Transparenzpflichten. Zum anderen haben auch betroffene Personen ein Interesse daran, zu erfahren, dass ihre Daten im Darknet gefunden wurden. Da ihre personenbezogene Daten bereits durch einen Cyberangriff veröffentlicht wurden, liegt das Hauptinteresse der betroffenen Personen in der rechtzeitigen Information, um angemessene Schutzmaßnahmen ergreifen zu können. Ohne eine Weitergabe an das übergeordnete Unternehmen würde die betroffene Person möglicherweise gar nicht von der Veröffentlichung ihrer Daten erfahren oder wüsste nicht, ob sie selbst betroffen ist. Ergebnis: Da die betroffenen Personen durch die Weitergabe der Daten an das übergeordnete Unternehmen vor weiteren Schäden geschützt werden sollen und potenzielle Nachteile durch Datenschutzmaßnahmen minimiert werden können, überwiegt das Interesse der F an der Datenweitergabe.
	Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten ☐ *Ausdrückliche Einwilligung – Art. 9 Abs. 2 lit. a DSGVO* ☐ *Arbeitsrecht, soziale Sicherheit, Sozialschutz – Art. 9 Abs. 2 lit. b DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 9 Abs. 2 lit. c DSGVO* ☐ *Politisch, weltanschaulich, religiös und gewerkschaftlich ausgerichtete Organisationen – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Selbst veröffentlichte Daten – Art. 9 Abs. 2 lit. e DSGVO* ☐ *Rechtsansprüche und Gerichtsverhandlungen – Art. 9 Abs. 2 lit. f DSGVO* ☐ *Erhebliches öffentliches Interesse – Art. 9 Abs. 2 lit. g DSGVO* ☐ *Gesundheits- und Sozialbereich – Art. 9 Abs. 2 lit. h DSGVO* ☐ *Öffentliche Gesundheit – Art. 9 Abs. 2 lit. i DSGVO* ☐ *Archiv-, Forschungs- und statistische Zwecke – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Sonstiges*:
	Begründung: Voraussichtlich werden keine besonderen Kategorien personenbezogener Daten weitergegeben.

<table>
<tr><td rowspan="3">Ggf. Abschluss von Verträgen über Auftragsverarbeitung/ gemeinsame Verantwortlich-keit/ Drittstaatübermittlung</td><td>Auftragsverarbeitung: Die Daten der Darknet-Recherche werden mittels eines externen Cloud-Speicherdienstes gespeichert. Dabei handelt es sich um den deutschen Cloud-Computing-Anbieter A. Die rechtskonforme Weitergabe stützt sich auf den Auftragsverarbeitungsvertrag[8] – eine zusätzliche Rechtsgrundlage zur Datenweitergabe an den Auftragsverarbeiter ist nicht erforderlich.</td></tr>
<tr><td>Gemeinsame Verantwortlichkeit: Gemeinsame Verantwortlichkeiten bestehen im Rahmen der geplanten Darknet-Recherche nicht.</td></tr>
<tr><td>Drittstaatübermittlung: A verarbeitet die personenbezogenen Daten ausschließlich auf Servern in Deutschland. Somit bedarf es keiner Garantien für Drittstaatübermittlungen.</td></tr>
<tr><td colspan="2">Schritt 3</td></tr>
<tr><td rowspan="3">Identifizierung der Informationspflichten</td><td>Direkterhebung: Im Rahmen der Darknet-Recherche wird es nicht zu einer Direkterhebung von personenbezogenen Daten bei betroffenen Personen kommen. Personenbezogene Daten werden bei einer Darknet-Recherche nicht durch einen direkten Kontakt mit den betroffenen Personen erhoben, diese werden vielmehr bereits veröffentlicht vorgefunden. Die ursprüngliche Offenlegung wird regelmäßig durch unbefugte Dritte, bspw. durch einen Hackerangriff, erfolgen. Die Verarbeitung dieser Daten durch F erfolgt daher nicht durch eine Erhebung bei den betroffenen Personen, sondern durch den Zugriff auf eine fremde Quelle.</td></tr>
<tr><td>Dritterhebung – Kontaktmöglichkeit über Dritte: Aufgrund der Vorerfahrungen ist hinreichend wahrscheinlich, dass sich den im Darknet gefundenen personenbezogenen Daten entnehmen lässt, von welcher Organisation diese Daten ursprünglich stammen. Eine geeignete Maßnahme zur Wahrung der Rechte und Freiheiten betroffener Personen ist in diesem Fall die Informationserteilung über den Datenfund an diese übergeordnete Organisation. Damit verbunden sollte gegenüber der übergeordneten Organisation die Bitte ausgesprochen werden, eine durch F mitgeschickte Information i.S.d. Art 14 Abs. 1 und 2 DSGVO an die durch den Cyberangriff betroffenen Mitarbeiter/Kunden weiterzuleiten. Diese Bitte sollte bereits im Rahmen des Erstkontakts zwischen F und der übergeordneten Organisation erfolgen. Sofern F im Rahmen der weiteren Kommunikation jedoch Teile der aufgefundenen Daten mit der übergeordneten Organisation teilen muss, damit diese ihrerseits geeignete Maßnahmen ergreifen kann, stellt F in ihrer diesem Schritt vorgelagerten Kommunikation mit der übergeordneten Organisation sicher, dass die Erteilung der Information an die betroffenen Personen spätestens zum Zeitpunkt der ersten Offenlegung an die übergeordnete Organisation durch diese erfolgt, Art. 14 Abs. 3 lit. c DSGVO.</td></tr>
<tr><td>Dritterhebung – keine Kontaktmöglichkeit: Aufgrund der Vorerfahrungen ist ebenso hinreichend wahrscheinlich, dass personenbezogene Daten aus dem Darknet erhoben werden, die weder direkte Kontaktinformationen der betroffenen Person enthalten noch erkennen lassen, von welcher Organisation die gestohlenen Daten ursprünglich stammen. Als geeignete Schutzvorkehrung wird hier die Veröffentlichung der nach Art. 14 Abs. 1 und 2 DSGVO gebotenen Informationen abseits des eigentlichen Verarbeitungskontexts vorgenommen. Konkret wird diese Pflicht durch die Bereitstellung einer Datenschutzinformation auf der Webseite der F erfüllt.[9]</td></tr>
<tr><td>Compliance-Management für Informationspflichten</td><td>Einrichtung eines unternehmensinternen Prozesses: Es wurde folgender unternehmensinterner Prozess etabliert, der die fristgerechte Erteilung der Datenschutzinformation (oder in Fällen des Art. 14 Abs. 5 lit. b DSGVO die Umsetzung geeigneter Maßnahmen) an die betroffenen Personen sicherstellt, sofern es im Rahmen der geplanten Darknet-Recherche tatsächlich zur personenbezogenen Datenverarbeitung kommen sollte.

Prozess zur Umsetzung der Informationspflichten
Schritte vor Beginn der Durchführung der Darknet-Recherche:
1. V hat eine Datenschutzinformation für Fälle zu erstellen, in denen eine Kenntnis des übergeordneten Unternehmens vorliegt (Fall A). Ebenfalls hat V eine Datenschutzinformation für Fälle zu erstellen, in denen keine Kenntnis des übergeordneten Unternehmens vorliegt (Fall B).
2. V hat für Fall A ein Anschreiben mit der erforderlichen Datenschutzinformation an übergeordnete Unternehmen vorzuformulieren.
3. Dieses Anschreiben und die Datenschutzinformation hat V von F und D freigeben zu lassen.
4. V hat für Fall B ein Dokument mit der erforderlichen Datenschutzinformation für die Website der F zu erstellen.
5. Das erstellte Dokument und die Datenschutzinformation hat V von F und D freigeben zu lassen.
6. V hat die freigegebene Datenschutzinformation für Fall B auf der Webseite der F zu veröffentlichen. Dies ist zu dokumentieren.

Schritte nach Beginn der Durchführung der Darknet-Recherche:</td></tr>
</table>

[8] Für den Auftragsverarbeitungsvertrag wurde auf das Muster des BfDI zurückgegriffen, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_zur_Auftragsverarbeitung.pdf?blob=publicationFile&v=2, das an den vorgesehenen Stellen ergänzt wurde. Der Vertrag wurde durch den Auftragsverarbeiter A um technische und organisatorische Maßnahmen ergänzt, die typisch für die Bereitstellung von Cloud-Services ist. Der Vertrag und die Maßnahmen werden hier nicht abgedruckt.

[9] *Dix,* in: Simitis/Hornung/Spiecker gen. Döhmann, 1. Aufl. 2019, DSGVO Art. 14 Rn. 26; *Bäcker*, in: Kühling/Buchner, 4. Aufl. 2024, DS-GVO Art. 14 Rn. 62, 63.

7. Nach jeder personenbezogenen Datenerhebung hat V zu überprüfen, ob die Daten mit einem oder mehreren übergeordneten Unternehmen in Verbindung stehen (Fall A).
8. Sofern dies der Fall ist, hat V das freigegebene Anschreiben und die freigegebene Datenschutzinformation innerhalb von zehn Werktagen an das oder die übergeordnete(n) Unternehmen zu senden. Die Kontaktaufnahme und die enthaltene Datenschutzinformation (per E-Mail oder per Kontaktformular auf der Website des Unternehmens) sind durch Aufbewahrung der E-Mail oder durch Erstellen eines Screenshots festzuhalten.

Sofern V, nach entsprechender Freigabe durch F und D, einem Unternehmen einen Auszug der im Darknet aufgefundenen, seine Mitarbeiter oder Kunden betreffenden Daten, übersendet, hat er die Übersendung der Informationen bereits im Vorfeld der Datenweitergabe mit dem übergeordneten Unternehmen abzuklären, damit die Übersendung der Datenschutzinformationen zum Zeitpunkt der Datenweitergabe erfolgt.

Erstellen von Datenschutzinformationen

Direkterhebung: Im Rahmen der Darknet-Recherche wird es nicht zu einer Direkterhebung von personenbezogenen Daten bei betroffenen Personen kommen, sodass eine Datenschutzinformation nach Art. 13 Abs. 1 und Abs. 2 DSGVO nicht zu erstellen ist.

Dritterhebung - Kontaktmöglichkeit über Dritte: Versenden nachfolgenden Anschreibens und Datenschutzinformation an Kontakt:

Anschreiben

Betreff: Dringende Benachrichtigung: Zufälliger Zugriff auf personenbezogene Daten

Sehr geehrte Damen und Herren,

wir, die Cybersicherheitsforschungseinrichtung F, führen derzeit ein Forschungsprojekt durch, welches das Ziel verfolgt, neue Cyberangriffsmethoden zu identifizieren und Gegenmaßnahmen abzuleiten. Hierfür führen wir Recherchen im Darknet durch. Diese Recherchen haben explizit nicht zum Ziel, aus Cybersicherheitsangriffen stammende Datensätzen zu verarbeiten. Dennoch kam es am [Datum] – aufgrund [Begründung] – zu einer solchen Datenverarbeitung durch die F. Konkret wurden [Datenart] Ihrer [Gruppe betroffener Personen] verarbeitet. [Im Falle des Auffindens von Login-Daten: Die F hat die Login-Daten zu keinem Zeitpunkt zum Zugriff auf die zugehörigen Accounts genutzt und wird dies auch zukünftig nicht tun.]

Soweit Ihrerseits keine Rückfragen zu dem Sachverhalt bestehen, die Sie uns bis zum [Datum] mitteilen, werden die Daten bei uns gelöscht, sobald sie keinen gesetzlichen Aufbewahrungspflichten mehr unterliegen. Bitte beachten Sie jedoch, dass die personenbezogenen Daten der betroffenen Personen unserer Kenntnis nach weiterhin im Darknet auffindbar sind.
Wer die personenbezogenen Daten in das Darknet gestellt hat, entzieht sich unserer Kenntnis.
Da uns keine direkte Kontaktmöglichkeit zu den betroffenen Personen vorliegt, möchten wir Sie bitten, die angefügte Datenschutzinformation an Ihre [Gruppe betroffener Personen] weiterzuleiten und uns somit in der Durchführung unserer Pflicht zur Umsetzung geeigneter Maßnahmen i.S.d. Art. 14 Abs. 5 lit. b DSGVO zu unterstützen.

Für weitere Informationen stehen wir Ihnen gerne zur Verfügung. Wir danken Ihnen im Voraus für Ihre Zusammenarbeit.
Mit freundlichen Grüßen
Cybersicherheitsforschungseinrichtung F

Datenschutzinformation gemäß Artikel 14 DSGVO

Sehr geehrte betroffene Person,

gemäß den Bestimmungen der Datenschutz-Grundverordnung (DSGVO) möchten wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch unsere Cybersicherheitsforschungseinrichtung F informieren. Die folgenden Informationen erteilen wir gem. Art. 14 Abs. 5 S. 1 lit. b S. 2 DSGVO, da eine direkte Erteilung der Datenschutzinformationen an Sie als betroffene Person nicht mit einem verhältnismäßigen Aufwand umsetzbar ist.

1. Verantwortliche Stelle

Verantwortliche Stelle für die Verarbeitung Ihrer personenbezogenen Daten ist:
Cybersicherheitsforschungseinrichtung F
[Adresse]
[Kontaktdaten]
[Kontaktdaten der Datenschutzbeauftragten]

2. Zwecke der Datenverarbeitung
Im Rahmen eines Forschungsprojekts führen wir Darknet-Recherchen zur Identifizierung und Analyse von Sicherheitsrisiken, Datenlecks und zur Verbesserung automatisierter Erkennungen neuer Cyberangriffsmethoden und Dienstleistungen durch. Die Datenerhebung erfolgt zum Teil automatisiert. Zweck der Datenerhebung ist die Aufrechterhaltung eines hohen Schutzes technischer Ressourcen sowie der Rechte und Freiheiten von Menschen.
Zudem führen wir Darknet-Recherchen zur Gewinnung von Informationen über gestohlene oder kompromittierte Daten durch. Hierdurch sollen potenzielle Cyberbedrohungen frühzeitig erkannt und ggf. abgewehrt und ggf. durch den Cyberangriff entstandene Schäden erkannt werden.

3. Kategorien von personenbezogenen Daten
Für uns als Cybersicherheitsforschungseinrichtung ist es im Vorfeld der Forschungsaktivitäten nicht immer vorhersehbar und/oder planbar, ob und welche Kategorien personenbezogenen Daten bei der Darknet-Recherche verarbeitet werden. Insbesondere bei Rechercheaktivitäten im Darknet, die die Identifizierung neuer Cyberangriffsmethoden bezwecken, kann es vorkommen, dass Forschende auf Datensätze stoßen, die gestohlene Daten aus früheren Cyberangriffen enthalten. Welche Inhalte diese Datensätze aufweisen ist im Vorfeld nicht vorherzusehen.
Aufgrund von unseren Erfahrungen ist zu erwarten, dass bei den Darknet-Recherchen folgende Kategorien von personenbezogenen Daten verarbeiten:
- Kundenstammdaten: Dazu gehören Namen, Geburtsdaten und andere demografische Informationen von Kunden eines Unternehmens.
- Log-In-Daten: Benutzernamen, Passwörter, PIN-Codes und andere Zugangsdaten, die für den Zugriff auf Online-Konten oder Systeme verwendet werden

4. Rechtsgrundlage der Datenverarbeitung
Die Verarbeitung Ihrer personenbezogenen Daten erfolgt aufgrund unseres berechtigten Interesses an der Durchführung von Cybersicherheitsaktivitäten und der Gewährleistung der Informationssicherheit gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO.

5. Datenempfänger
Empfänger Ihrer personenbezogenen Daten können sein:
- Interne Abteilungen und Mitarbeiter der F, die an der Durchführung von Darknet-Recherchen beteiligt sind.
- Externe Partner oder Behörden, sofern dies zur Erfüllung gesetzlicher Verpflichtungen oder zur Abwehr von Cyberbedrohungen erforderlich ist.
- Auftragsverarbeiter, insbesondere Cloud-Speicherdienste.

6. Übermittlung in Drittländer
Eine Übermittlung Ihrer personenbezogenen Daten an Empfänger in Drittländern findet nicht statt.

7. Speicherdauer
Wir speichern Ihre personenbezogenen Daten nur so lange, wie es für die Durchführung unserer Darknet-Recherchen und die Erfüllung unserer gesetzlichen Verpflichtungen erforderlich ist.

8. Ihre Rechte
Als betroffene Person stehen Ihnen gemäß der DSGVO folgende Rechte zu:
- Recht auf Auskunft über Ihre gespeicherten Daten.
- Recht auf Berichtigung unrichtiger Daten.
- Recht auf Löschung Ihrer Daten.
- Recht auf Einschränkung der Verarbeitung.

- Recht auf Widerspruch gegen die Verarbeitung.
- Recht auf Beschwerde bei einer Aufsichtsbehörde.

9. Kontakt
Für Fragen oder Ausübung Ihrer Rechte in Bezug auf den Datenschutz stehen wir Ihnen gerne zur Verfügung. Sie können uns wie folgt kontaktieren:

[Kontaktdaten für Datenschutzanfragen]

Mit freundlichen Grüßen
Cybersicherheitsforschungseinrichtung F

Dritterhebung - keine Kontaktmöglichkeit über Dritte: Einbetten folgender Texte in die Datenschutzinformation der Webseite der F:

Datenverarbeitung im Rahmen unserer Darknet-Forschung

1. Zwecke der Datenverarbeitung
Im Rahmen einiger unserer Forschungsprojekte führen wir Darknet-Recherchen zur Identifizierung und Analyse von Sicherheitsrisiken, Datenlecks und zur Verbesserung automatisierter Erkennungen neuer Cyberangriffsmethoden und -dienstleistungen durch. Die Datenerhebung erfolgt zum Teil automatisiert. Zweck der Datenerhebung ist die Aufrechterhaltung eines hohen Schutzes technischer Ressourcen sowie der Rechte und Freiheiten von Menschen. Zudem führen wir Darknet-Recherchen zur Gewinnung von Informationen über gestohlene oder kompromittierte Daten durch. Hierdurch sollen potenzielle Cyberbedrohungen frühzeitig erkannt und ggf. abgewehrt und ggf. durch den Cyberangriff entstandene Schäden erkannt werden.

2. Kategorien von personenbezogenen Daten
Es ist für uns als Forschungseinrichtung im Voraus der geplanten Forschungsaktivitäten nicht immer vorhersehbar und/oder planbar, ob und welche Kategorien personenbezogenen Daten bei der Darknet-Recherche verarbeitet werden. Insbesondere bei Recherche Aktivitäten im Darknet, die die Identifizierung neuer Cyberangriffsmethoden und -dienstleistungen bezwecken, kann es vorkommen, dass Forschende im Rahmen dieser Forschungsaktivitäten auf Datensätze stoßen, die gestohlene Daten aus früheren Cyberangriffen enthalten. Welche Inhalte diese Datensätze aufweisen ist für uns im Vorfeld nicht planbar. Aus Erfahrung können wir sagen, dass wir bei der Darknet-Recherche i.d.R. folgende Kategorien von personenbezogenen Daten verarbeiten:
- Kundenstammdaten: Dazu gehören Namen, Geburtsdaten und andere demografische Informationen von Kunden eines Unternehmens.
- Log-In-Daten: Benutzernamen, Passwörter, PIN-Codes und andere Zugangsdaten, die für den Zugriff auf Online-Konten oder Systeme verwendet werden

3. Rechtsgrundlage der Datenverarbeitung
Die Verarbeitung Ihrer personenbezogenen Daten erfolgt aufgrund unseres berechtigten Interesses an der Durchführung von Cybersicherheitsaktivitäten und der Gewährleistung der Informationssicherheit. Die Datenverarbeitung erfolgt somit i.d.R. auf Basis von Art. 6 Abs. 1 S. 1 lit. f DSGVO.

4. Datenempfänger
Empfänger Ihrer personenbezogenen Daten können sein:
- Interne Abteilungen und Mitarbeiter unserer Forschungseinrichtung, die an der Durchführung von Darknet-Recherchen beteiligt sind.
- Externe Partner oder Behörden, sofern dies zur Erfüllung gesetzlicher Verpflichtungen oder zur Abwehr von Cyberbedrohungen erforderlich ist.
- Auftragsverarbeiter, insbesondere Cloud-Speicherdienste.

5. Übermittlung in Drittländer
Eine Übermittlung Ihrer personenbezogenen Daten an Empfänger in Drittländern findet durch uns nicht statt.

6. Speicherdauer

	Wir speichern Ihre personenbezogenen Daten nur so lange, wie es für die Durchführung unserer Darknet-Recherchen und die Erfüllung unserer gesetzlichen Verpflichtungen erforderlich ist.
Schritt 4	
Identifizierung geeigneter technisch und organisatorischer Maßnahmen	**Verarbeitungsspezifische TOMs der Cybersicherheitsforschungseinrichtung F:** **Personen** - Mündliche datenschutzrechtliche Erstbelehrung der an dem Forschungsprojekt beteiligten Mitarbeiter - Regelmäßige mündliche Folgebelehrungen der an dem Forschungsprojekt beteiligten Mitarbeiter - Arbeitsanweisung für die Datenverarbeitung im Rahmen einer Darknet-Recherche **Arbeitsanweisung für die Datenverarbeitung im Rahmen einer Darknet-Recherche bei der Cybersicherheitsforschungseinrichtung F** **1. Speicherort für Daten:** - Die an dem Forschungsprojekt beteiligten Mitarbeiter sind angewiesen, sämtliche im Darknet erhobenen Daten ausschließlich in der externen Cloud des A zu speichern. - Es ist nicht gestattet, Daten aus dem Darknet auf internen Servern der F zu speichern oder auszudrucken. **2. Zwischenspeicherung und Löschung:** - Sofern Daten aus dem Darknet vor der Weitergabe an Auftragsverarbeiter kurzzeitig lokal bei F zwischengespeichert werden müssen, sind diese unverzüglich nach der Weitergabe zu löschen. - Der Arbeitsplatz darf in der Zeit, in welcher die Daten aus dem Darknet lokal zwischengespeichert sind, bis zur Weitergabe an den Auftragsverarbeiter, nicht verlassen werden. **3. Zugriffsberechtigung für die Zwischenspeicherung:** - Die Berechtigung zur lokalen Zwischenspeicherung wird nur Verfahrenseignerin V und dem jeweils die Forschungsarbeiten durchführenden Cybersicherheitsforschenden gewährt. - Alle anderen Mitarbeiter sind nicht befugt, Daten aus dem Darknet lokal zu speichern. Diese Arbeitsanweisung ist verbindlich und gilt für alle Mitarbeiter der Cybersicherheitsforschungseinrichtung F. Es ist sicherzustellen, dass alle Mitarbeiter die Anweisungen gemäß dieser Arbeitsanweisung befolgen. Verstöße gegen diese Arbeitsanweisung können disziplinarische Maßnahmen nach sich ziehen. **Systeme und Daten** - Einsatz von Firewall- und Antivirensoftware. - Einsatz von Benutzererkennung und Passwort. - Technisches Erzwingen der Nutzung sicherer Passwörter einschließlich regelmäßiger Neusetzung. - Einsatz von RFID-Transpondern oder Token für Zutrittsschutz. - Einsatz von Verschlüsselung und VPN. - Implementierung eines Zugangs- und Zugriffsberechtigungskonzepts einschließlich automatisierter Überprüfung und Protokollierung (auch der einzelnen Eingaben). - Implementierung eines Zutrittsberechtigungskonzepts und einer Zutrittskontrolle durch Abschließen der Türen und dem Einsatz von Sicherheitsschlössern. - Ordnungsgemäßes Vernichten alter Datenträger. **Kooperationen** - Prüfung von Auftragsverarbeitungsverträgen und technischer und organisatorischer Maßnahmen.

<table>
<tr><td>Workshop mit potenziell betroffenen Personen</td><td>Durchführung eines Workshops: Zur Identifikation potenzieller Risiken wurde am 08.04.2024 durch die D ein Workshop mit drei potenziell betroffenen Personen durchgeführt. Damit wurde die Mindestanzahl an Teilnehmenden erreicht, die für eine valide Einschätzung der Datenschutzrisiken erforderlich war. In diesem Workshop wurde zunächst die geplante Forschungsaktivität durch die D vorgestellt. Die D erläuterte, welche Schutzmaßnahmen bei der Durchführung der Forschungsaktivität durch F ergriffen werden. Es folgte eine virtuelle, anonyme Abstimmung mit einem Abstimmungstool, sodass niemand durch das Verhalten eines anderen Teilnehmenden beeinflusst wurde. Abgestimmt wurde über die Fragen, (1) ob die Teilnehmenden alles verstanden haben, was passieren soll, (2) ob sie sich und ihre Rechte und Freiheiten durch die Forschungseinrichtung F angemessen geschützt sehen und (3) ob sie Einwände/Bedenken gegen das Vorhaben haben (mit Freitext). Die potenziell betroffenen Personen hatten keine Anmerkungen und äußerten keine Bedenken.</td></tr>
<tr><td rowspan="2">Implementierung der technischen und organisatorischen Maßnahmen</td><td>Anweisung zur Umsetzung der TOMs: Der I wurde am 28.3.24 angewiesen, die verarbeitungsspezifischen technischen und organisatorischen Maßnahmen umzusetzen.</td></tr>
<tr><td>Bestätigung zur Umsetzung der TOMs: Die Umsetzung der technischen und organisatorischen Maßnahmen wurde durch den I am 28.3.24 bestätigt.</td></tr>
<tr><td colspan="2">Schritt 5</td></tr>
<tr><td rowspan="3">Monitoring der konkreten Datenerhebung</td><td>Beginn der Verarbeitung: Die Darknet-Recherche der F startet, wie geplant, am 22.04.2024 um 10:30 Uhr. Die Darknet-Recherche wurde von der Verfahrenseignerin V angestoßen, indem sie die Cybersicherheitsforschende C dazu aufforderte, die Darknet-Recherche durchzuführen.</td></tr>
<tr><td>Verlauf der Verarbeitung: C kontrolliert kontinuierlich jede Datenerhebung, um nachvollziehen, ob, welche und wie viele personenbezogene Daten von welchen betroffenen Personen tatsächlich verarbeitet werden.</td></tr>
<tr><td>Löschen nicht-relevanter Daten: Nach Absprache zwischen V und C wurden die Daten zumindest kurzfristig auf dem externen Cloud-Speicher des A gespeichert. Siehe hierzu die formulierten Löschfristen:

Verwendungszweck
Die Daten werden verwendet, um
- Informationen über neue Cyberangriffsmethoden zu erlangen
- Geeignete Gegenmaßnahmen zu identifizieren
- Schäden einzuschätzen
- betroffene Personen oder Unternehmen zu informieren und
- rechtliche Ansprüche geltend machen und abwehren zu können.

Hinweise zum Fachprozess
Die Erhebung personenbezogener Daten ist nicht der primäre Zweck der Darknet-Recherche. Vielmehr werden sie „versehentlich“ bzw. zufällig erhoben.

Inhalte der Datenart
Die Datenart könnte die folgenden Datenobjekte umfassen:
- Kundenstammdaten: Dazu gehören Namen, Geburtsdaten und andere demografische Informationen von Kunden eines Unternehmens.
- Log-In-Daten: Benutzernamen, Passwörter, PIN-Codes und andere Zugangsdaten, die für den Zugriff auf Online-Konten oder Systeme verwendet werden.

<table>
<tr><th colspan="2">Datenart „Daten aus Darknet-Recherche“ (Auszug aus Löschregel-Katalog)</th></tr>
<tr><td>Verarbeitungsgrundlage</td><td>Art. 6 Abs. 1 lit. f DSGVO</td></tr>
<tr><td>Löschvorgaben</td><td>Die Löschung erfolgt nach den Grundsätzen der Zweckbindung und Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO. Die Daten werden gelöscht, sobald der Zweck der Speicherung entfällt und keine Aufbewahrungspflichten mehr bestehen.</td></tr>
<tr><td>Aufbewahrungspflichten</td><td>§ 195 BGB: 3 Jahre; § 78 Abs. 3, 4 StGB: 3 Jahre</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Löschregel</td><td>Startzeitpunkt: Datenerhebung
Regellöschfrist: 3 Jahre
Vorhaltefrist: 3 Jahre
Vorbedingungen: Die Daten werden für kein laufendes Rechtsverfahren (mehr) benötigt.</td></tr>
<tr><td>Sperrregel</td><td>Startzeitpunkt: Datenerhebung
Sperrfrist: 12 Wochen
Verbleibende Zugriffsberechtigte: Gemäß einer organisationsinternen Anweisung darf auf die Daten nur zugegriffen werden, wenn sie als Beweismittel genutzt werden müssen (oder um sie nach Ablauf der Löschfrist endgültig zu löschen).</td></tr>
<tr><td>Löschung im Einzelfall</td><td>Löschung im Einzelfall wird stattgegeben.</td></tr>
</table>

Verarbeitungsorte und Umsetzung der Sperr- und Löschregel
Die personenbezogenen Daten werden im Wirkbetrieb ausschließlich in der Cloud des Auftragsverarbeiters A verarbeitet. Sofern das Speichern der Daten bei A eine lokale Zwischenabspeicherung bedarf, darf diese nur durch den Verfahrenseignerin V und dem jeweils die Forschungsarbeiten durchführenden Cybersicherheitsforschenden ausgelöst werden. Die Daten auf dem lokalen Zwischenspeicher sind von V und dem jeweils die Forschungsarbeiten durchführenden Cybersicherheitsforschenden umgehend (spätestens 15 Minuten nach der Übertragung zu A, auch im lokalen Papierkorb) zu löschen, sobald die Daten in der Cloud des A gespeichert wurden. Die Daten in der Cloud des A sind je Datenerhebung in einem separaten Ordner „Datensatz-(laufende Nr.)“ zu speichern.
Nach Ablauf der Sperrfrist sind die Daten innerhalb der Cloud des Auftragsverarbeiters A in einen separaten Ordner „Datensatz-[laufende Nummer]-Eingeschränkt verarbeitete Daten – zu löschen am (TT.MM.JJ)“ zu verschieben. „TT.MM.JJ“ beschreibt das Datum, an dem die Vorhaltefrist der Daten abläuft und eine Löschung erfolgen kann. Eine organisationsinterne Anweisung verhindert unberechtigte Zugriffe auf diesen Ordner.
Für die technische Umsetzung der Löschung werden die Vorgaben der DIN 66398 und 66399 erfüllt. Gefolgt auf das Datum „TT.MM.JJ“ (Datum, an dem die Vorhaltefrist abläuft) ist der Ordner durch V und den jeweils die Forschungsarbeiten durchführenden Cybersicherheitsforschenden grundsätzlich innerhalb von drei Werktagen, entsprechend der Angemessenheitsanforderung an die datenschutzrechtlichen Löschpflichten jedoch spätestens innerhalb von einem Jahr, händisch vollständig zu löschen. Das Datum speichern sich V und der jeweils die Forschungsarbeiten durchführenden Cybersicherheitsforschende, verbunden mit einer entsprechenden Terminerinnerung, in ihren virtuellen Kalendern.

Protokollierung der Löschung
V und der jeweils die Forschungsarbeiten durchführende Cybersicherheitsforschende führen innerhalb der Cloud-Umgebung des A eine Excel-Liste, in die sie jeden erhobenen Datensatz mit Erhebungsdatum, vorgesehenem Datum der eingeschränkten Verarbeitung und vorgesehenem Löschdatum eintragen. Die tatsächliche Umsetzung der Einschränkung und Löschung sind ebenfalls jeweils mit Datumsangabe in die Liste einzutragen. Zur leichteren Übersicht werden die erhobenen Datensätze sowohl in der Excel-Liste als auch in den Ordnern zur Speicherung im Wirkbetrieb und zur Speicherung zur eingeschränkten Verarbeitung mit einer laufenden Nummer versehen.</td></tr>
<tr><td>Dokumentation der zufälligen Zugriffe auf personenbezogene Daten</td><td>Beschreibung des Zugriffs: Bei der Darknet-Recherche hat C am 22.04.2024 um 13:00 Uhr eine Datei geöffnet, da sie davon ausging, dass sich hierin Informationen über den bei Unternehmen Z durchgeführten Angriff befinden (Name der Datei: „So-haben-wir-Unternehmen-Z-angegriffen“).
C hat diese Datei aufgrund der konkreten Vermutung geöffnet. Hierbei stellte sie jedoch fest, dass es sich bei den Daten nicht um Informationen über die neue Angriffsmethode handelt, sondern dass sich in der Datei gestohlene personenbezogene Log-In-Dateien der Online-Buchhandlung Q befinden.
Der Vorfall wurde von C um 13:20 Uhr der Verfahrenseignerin V per E-Mail gemeldet. C hat in dieser E-Mail alle konkreten Informationen zu dem Vorfall mitgeteilt. Insbesondere war der E-Mail zu entnehmen, dass der Vorfall um 13:00 Uhr im Rahmen einer Darknet-Recherche eintrat. C teilte ebenso mit, dass es sich bei den Daten, soweit es für sie zunächst erkenntlich war, um eine Beschreibung des Angriffs, der beim Unternehmen Z durchgeführt wurde, handelte, tatsächlich jedoch auf gestohlene Daten der Online-Buchhandlung Q zugegriffen wurde. C teilte darüber hinaus mit, dass sie die Login-Daten der Q zwar erhoben, jedoch nicht benutzt hat, um sich Zugang zu den Systemen der Q zu verschaffen.
Die Daten wurden um 13:20 Uhr durch V auf dem PC der C gesichtet. Dabei wurde festgestellt, dass es sich bei den gefundenen Daten um circa 100.000 Log-In Daten von Mitarbeitern der Q handelt. Besondere Kategorien personenbezogener Daten sind in dem Datensatz nicht enthalten. Außerdem befinden sich keine E-Mail-Adressen oder sonstige Kontaktdaten bei den Log-In-Daten. Eine unmittelbare Erfüllung der Informationspflicht war somit nicht möglich. Q wurde durch V per E-Mail über den Datenfund informiert. V hat das hierfür vorformulierte Anschreiben genutzt. Darüber hinaus hat V die vorformulierte Datenschutzinformation an diese E-Mail beigefügt. V bat Q darum, diese an die betroffenen Personen weiterzuleiten.</td></tr>
</table>

Abgleich mit den in Schritt 1 getroffenen Annahmen	**Abweichungen:** Überschreitungen der tatsächlichen Datenverarbeitung im Hinblick auf die Annahmen aus Schritt 1 der DS-V sind nicht ersichtlich, da in diesen Annahmen bereits das Risiko einkalkuliert wurde, dass möglicherweise Log-in-Daten erhoben werden könnten.
	Anzahl der erhobenen Daten: Überschreitungen hinsichtlich der Anzahl der tatsächlich erhobenen Daten sind im Hinblick auf die Annahmen aus Schritt 1 der DS-V nicht ersichtlich.
	Art der erhobenen Daten: Überschreitungen hinsichtlich der Art der tatsächlich erhobenen Daten sind im Hinblick auf die Annahmen aus Schritt 1 der DS-V nicht ersichtlich.
Dokumentation der unerwarteten Datenverarbeitungen	**Unerwartete Verarbeitungen personenbezogener Daten (sofern im zuvor vorgenommenen Abgleich Abweichungen festgestellt wurden):** -
Überprüfung der Notwendigkeit der Umsetzung weiterer TOMs	**Feststellung eines erhöhten Risikos:** Da die tatsächliche Datenverarbeitung die Annahmen aus Schritt 1 der DS-V nicht überschreitet und kein erhöhtes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, ist die Umsetzung weiterer technischer und organisatorischer Maßnahmen nicht notwendig.
Ggf. Umsetzung von Betroffenenrechten	**Erfüllung von Informationspflichten:** Die Informationspflichten wurden erfüllt. Sollten Anträge betroffener Personen zu ihren Rechten auf u.a. Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten eingehen, werden diese entsprechend den bereits bestehenden Prozessen zur Umsetzung dieser Betroffenenrechte der F umgesetzt.
Schritt 6	
Dokumentation	Die Umsetzung der Dokumentation erfolgte durch das Ausfüllen dieser Tabelle.

4. Fazit

Die praktische Umsetzung der DS-V im Rahmen des durchgeführten Planspiels hat demonstriert, dass dieses neu vorgeschlagene Instrument einen wesentlichen Beitrag zur Lösung datenschutzrechtlicher Herausforderungen in der Forschung leisten kann. Die strukturierte Herangehensweise in sechs definierten Schritten schafft einen verlässlichen Rahmen, der Rechtssicherheit gewährleistet und gleichzeitig den wissenschaftlichen Erkenntnisgewinn ermöglicht.

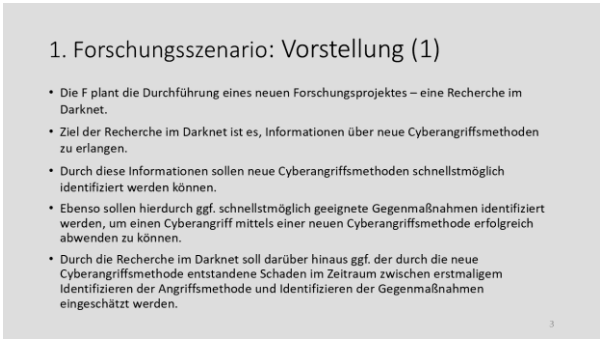
Das Planspiel hat zwei wichtige Verbesserungspotenziale für die DS-V aufgezeigt, die in der bisherigen Konzeption nicht ausreichend berücksichtigt wurden:

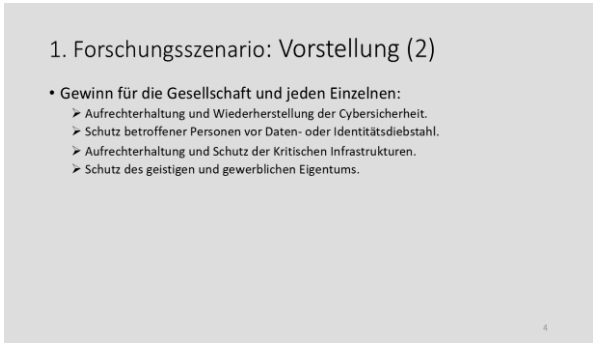
- So wurde deutlich, dass bisher eine konkrete Einbindung betroffener Personen (z.B. in Form eines Workshops) nicht in der Konzipierung der einzelnen Schritte der DS-V berücksichtigt wurde, jedoch ggf. vorgesehen werden sollte, um betroffene Personen in die DS-V einzubeziehen (sofern im Einzelfall angemessen, s.u.).
- Zudem zeigte sich, dass das Compliance-Management für Informationspflichten sinnvollerweise nach der Identifizierung der Informationspflichten und vor dem Erstellen der Datenschutzinformationen erfolgen sollte, was eine Umkehrung der bisherigen Unterschritte 3b (neu: 3c) und 3c (neu: 3b) erfordert.

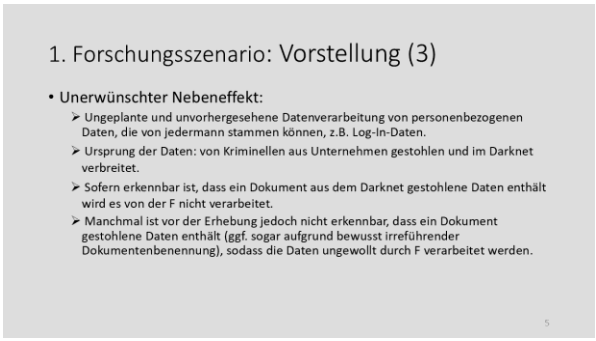
Ob der erforderliche Ressourcenaufwand von 77,75 Stunden als angemessen zu betrachten ist – da dieser bereits zu einem Zeitpunkt zu erbringen wäre, wenn noch nicht einmal feststeht, ob/welche/wie viele personenbezogene Daten überhaupt verarbeitet werden, ist kritisch zu diskutieren. Hierbei sind einerseits der große Mehrwert für die betroffenen Personen und die Rechtssicherheit für die Cybersicherheitsforschenden positiv zu berücksichtigen. Zudem ist der hier identifizierte Durchführungsaufwand insofern zu relativieren, dass der erstmalige Durchführungsaufwand eines Arbeitsschrittes i.d.R. im Vergleich zum Umsetzungsaufwand, sobald dieser Arbeitsschritt Routine geworden ist, überproportional hoch einzustufen ist. Darüber hinaus ist bezüglich des hier beschriebenen Umsetzungsaufwandes relativierend anzumerken, dass eine Forschungseinrichtung den Umsetzungsaufwand der gesamten DS-V i.d.R. nur einmalig umsetzen müsste, weil ähnliche Verarbeitungsvorgänge zusammengefasst in einer DS-V vorbereitet werden könnten (und weil sogar bei nicht-ähnlichen Verarbeitungsvorgängen davon auszugehen ist, dass auf einen Großteil der bereits erstellten Arbeitsanweisungen, Löschfristen usw. zurückgegriffen werden kann). Auch ist eine Einbindung betroffener Personen nur empfohlen, nicht aber verpflichtend, so dass auch in diesem Unterschritt Möglichkeiten zur Reduzierung des Ressourcenaufwandes möglich scheinen, sofern auf die Einbindung betroffener Personen verzichtet werden kann. Unter diesen aufwandseinschränkenden Annahmen und den vorgenannten Vorteilen einer DS-V ist somit die Angemessenheit der DS-V-Durchführung grundsätzlich zu bejahen.

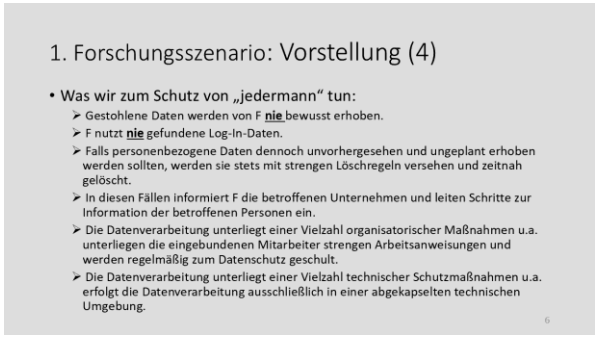
Wäre die DS-V im europäischen Datenschutzrechtssystem verankert, würde sie Forschenden ermöglichen, ihre Arbeit rechtssicher durchzuführen, während gleichzeitig die Rechte und Freiheiten betroffener Personen gewahrt blieben. Die hier vorgestellte Dokumentationsvorlage kann als Orientierungshilfe für Forschungseinrichtungen dienen, die ähnliche datenschutzrechtliche Herausforderungen bewältigen müssen (sofern die DS-V künftig verpflichtender Teil des europäischen Datenschutzrechtssystems würde).

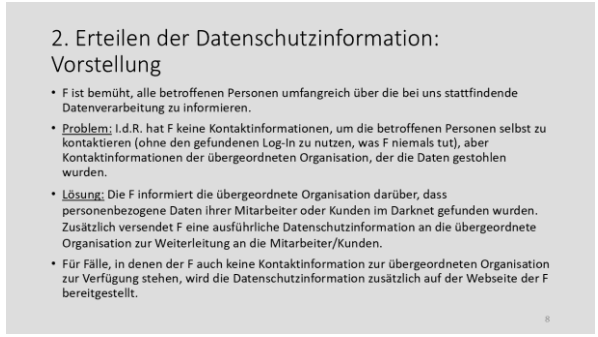
Anhang 1: Folienauszug aus dem Workshop zum Einholen des Standpunkts betroffener Personen











Anhang 2: Dokumentationsvorschlag einer Datenschutz-Vorsorge

Schritt 1	
Beschreibung des Forschungszwecks	Benennung des Zwecks:
	Übergeordnetes Ziel der Zweckerreichung:
Beschreibung der Forschungsnotwendigkeit	Feststellung der Notwendigkeit:
	Begründung der Notwendigkeit:
	Diskussion milderer Mittel:
Beschreibung der Forschungsaktivität	Beschreibung des Vorgehens:
	Beschreibung der geplanten Sicherheitsmaßnahmen/des Vorgehens zur Erhöhung der Cybersicherheit:
	Geplante Dauer der Forschungsaktivität:
Beschreibung der wahrscheinlichen Datenverarbeitung	Wahrscheinliche Verarbeitung personenbezogener Daten:
	Verarbeitung besonderer Datenkategorien und Daten über Straftaten:
	Bestehen von Aufbewahrungspflichten:
	Meldung an betroffene Personen:
	Sonstiges:
Schritt 2	
Identifizierung der Rechtsgrundlage für den Verantwortlichen	Rechtsgrundlage für die Verarbeitung personenbezogener Daten: ☐ *Einwilligung – Art. 6 Abs. 1 lit. a DSGVO* ☐ *Vertragsverhältnis – Art. 6 Abs. 1 lit. b DSGVO* ☐ *Gesetz / rechtliche Verpflichtung – Art. 6 Abs. 1 lit. c DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 6 Abs. 1 lit. d DSGVO* ☐ *Wahrung einer öffentlichen Aufgabe – Art. 6 Abs. 1 lit. e DSGVO* ☐ *Bestehen berechtigter Interessen – Art. 6 Abs. 1 lit. f DSGVO* ☐ *Sonstiges*:
	Begründung:
	Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten ☐ *Ausdrückliche Einwilligung – Art. 9 Abs. 2 lit. a DSGVO* ☐ *Arbeitsrecht, soziale Sicherheit, Sozialschutz – Art. 9 Abs. 2 lit. b DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 9 Abs. 2 lit. c DSGVO* ☐ *Politisch, weltanschaulich, religiös und gewerkschaftlich ausgerichtete Organisationen – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Selbst veröffentlichte Daten – Art. 9 Abs. 2 lit. e DSGVO* ☐ *Rechtsansprüche und Gerichtsverhandlungen – Art. 9 Abs. 2 lit. f DSGVO* ☐ *Erhebliches öffentliches Interesse – Art. 9 Abs. 2 lit. g DSGVO* ☐ *Gesundheits- und Sozialbereich – Art. 9 Abs. 2 lit. h DSGVO* ☐ *Öffentliche Gesundheit – Art. 9 Abs. 2 lit. i DSGVO* ☐ *Archiv-, Forschungs- und statistische Zwecke – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Sonstiges*:
	Begründung:
Ggf. Identifizierung der Rechtsgrundlage für Datenweitergabe	Rechtsgrundlage für die Verarbeitung personenbezogener Daten: ☐ *Einwilligung – Art. 6 Abs. 1 lit. a DSGVO* ☐ *Vertragsverhältnis – Art. 6 Abs. 1 lit. b DSGVO*

	☐ *Gesetz / rechtliche Verpflichtung – Art. 6 Abs. 1 lit. c DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 6 Abs. 1 lit. d DSGVO* ☐ *Wahrung einer öffentlichen Aufgabe – Art. 6 Abs. 1 lit. e DSGVO* ☐ *Bestehen berechtigter Interessen – Art. 6 Abs. 1 lit. f DSGVO* ☐ *Sonstiges*:
	Begründung:
	Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten ☐ *Ausdrückliche Einwilligung – Art. 9 Abs. 2 lit. a DSGVO* ☐ *Arbeitsrecht, soziale Sicherheit, Sozialschutz – Art. 9 Abs. 2 lit. b DSGVO* ☐ *Schutz lebenswichtiger Interessen – Art. 9 Abs. 2 lit. c DSGVO* ☐ *Politisch, weltanschaulich, religiös und gewerkschaftlich ausgerichtete Organisationen – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Selbst veröffentlichte Daten – Art. 9 Abs. 2 lit. e DSGVO* ☐ *Rechtsansprüche und Gerichtsverhandlungen – Art. 9 Abs. 2 lit. f DSGVO* ☐ *Erhebliches öffentliches Interesse – Art. 9 Abs. 2 lit. g DSGVO* ☐ *Gesundheits- und Sozialbereich – Art. 9 Abs. 2 lit. h DSGVO* ☐ *Öffentliche Gesundheit – Art. 9 Abs. 2 lit. i DSGVO* ☐ *Archiv-, Forschungs- und statistische Zwecke – Art. 9 Abs. 2 lit. d DSGVO* ☐ *Sonstiges*:
	Begründung:
Ggf. Abschluss von Verträgen über AV/gem. Verantwortlichkeit/ Drittstaatübermittlung	Auftragsverarbeitung:
	Gemeinsame Verantwortlichkeit:
	Drittstaatübermittlung:
Schritt 3	
Identifizierung der Informationspflichten	Direkterhebung:
	Dritterhebung: - Kontaktmöglichkeit über Dritte: - Keine Kontaktmöglichkeit über Dritte:
Compliance-Management für Informationspflichten	Einrichtung eines unternehmensinternen Prozesses: - Schritte vor Beginn der Verarbeitung: - Schritte nach Beginn der Verarbeitung:
Erstellen von Datenschutzinformationen	Direkterhebung: - Datenschutzinformation gemäß Artikel 13 DSGVO
	Dritterhebung - Kontaktmöglichkeit über Dritte: - Anschreiben - Datenschutzinformation gemäß Artikel 14 DSGVO
	Dritterhebung – keine Kontaktmöglichkeit über Dritte: - Datenschutzinformation gemäß Artikel 14 DSGVO (ggf. nach entsprechender Prüfung: Einbetten auf Webseite der Forschungseinrichtung
Schritt 4	
Identifizierung geeigneter technisch und organisatorischer Maßnahmen	Verarbeitungsspezifische TOMs der Forschungseinrichtung - Personen: - Systeme und Daten:

	- Kooperationen:
Workshop mit potenziell betroffenen Personen	Durchführung eines Workshops:
Implementierung der technischen und organisatorischen Maßnahmen	Anweisung zur Umsetzung der TOMs: Der [Informationssicherheitsbeauftragte] wurde am [Datum einfügen] angewiesen, die verarbeitungsspezifischen technischen und organisatorischen Maßnahmen umzusetzen.
	Bestätigung zur Umsetzung der TOMs: Die Umsetzung der technischen und organisatorischen Maßnahmen wurde durch den [Informationssicherheitsbeauftragten] am [Datum einfügen] bestätigt.
Schritt 5	
Monitoring der konkreten Datenerhebung	Beginn der Verarbeitung: Die [Verarbeitung] startet am [Datum] um [Uhrzeit].
	Verlauf der Verarbeitung:
	Löschen nicht-relevanter Daten: - Feststellung der Speicherung - Platz für Löschregeln/-konzept - Platz zur Protokollierung der Löschung
Dokumentation der zufälligen Zugriffe auf personenbezogene Daten	Beschreibung des Zugriffs:
Abgleich mit den in Schritt 1 getroffenen Annahmen	Abweichungen: - Anzahl der erhobenen Daten: - Art der erhobenen Daten:
Dokumentation der unerwarteten Datenverarbeitungen	Unerwartete Verarbeitungen personenbezogener Daten (sofern im zuvor vorgenommenen Abgleich Abweichungen festgestellt wurden):
Überprüfung der Notwendigkeit der Umsetzung weiterer TOMs	Ergebnis Überprüfung:
Ggf. Umsetzung von Betroffenenrechten	Erfüllung ggf. bestehender, weiterer Informationspflichten:
Schritt 6	
Dokumentation	Die Umsetzung der Dokumentation erfolgte durch das Ausfüllen dieser Tabelle.

Literaturverzeichnis

BfDI: Muster Auftragsverarbeitung, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_zur_Auftragsverarbeitung.pdf?__blob=publicationFile&v=2.

Boll, Alina: Datenschutz-Vorsorge: Schritte 3-6, DuD 2023, S. 383-388.

Boll, Alina; Selzer, Annika: Die Datenschutz-Vorsorge (DS-V), DuD 2024, S. 44-48.

Boll, Alina; Selzer, Annika; Spiecker gen. Döhmann, Indra: Datenschutz in der offensiven Cybersicherheitsforschung, Tagesspiegel 2023: abrufbar unter: https://background.tagesspiegel.de/cybersecurity/datenschutz-in-der-offensiven-cybersicherheitsforschung.

Boll, Alina; Stummer, Sarah: Erste Schritte im Rahmen der Datenschutz-Vorsorge, DuD 2024, S. 118-124.

Boll, Alina; Stummer, Sarah; Selzer, Annika: Datenschutz-Vorsorge, DuD 2024, S. 172-176.

Kipker, Dennis: Cybersecurity, München 2023.

Selzer, Annika; Spiecker gen. Döhmann, Indra; Boll, Alina: Datenschutzvorsorge in der offensiven Cybersicherheitsforschung, DuD 2023, S. 785-790.

Selzer, Annika; Stummer, Sarah; Boll, Alina: Positionspapier zur zweiten DSGVO-Evaluation 2024, abrufbar unter: https://www.athene-center.de/fileadmin/content/PDF/Positionspapier-DSGVO.pdf?_=1708340158.

Simits, Spiros; Hornung, Gerrit; Spiecker gen. Döhmann, Indra: Datenschutzrecht, Nomos, Baden-Baden 2019.