MunichInnovationLabs

OSINT CHRONICLE

Vierteljährliche Paper-Reihe zur Einführung
in die Welt der offenen Quellen

OSINT CHRONICLE

Vierteljährliche Paper-Reihe zur Einführung in die Welt der offenen Quellen

Die vierteilige Paper-Reihe zu Open Source Intelligence (OSINT) gewährt jedes Quartal Einblicke in die tiefgründige Welt dieser Intelligence-Disziplin. Den Auftakt macht das erste Paper am 08.04.2024, danach erscheint am Montag jedes Quartals ein weiteres Paper. Die Paper sind dabei so konzipiert, dass sie verschiedene Facetten von OSINT beleuchten, um die Leserschaft fundiert in die Materie einzuführen. Die einzelnen Paper behandeln dabei unterschiedliche Schwerpunkte.

Das erste Paper widmet sich den Grundpfeilern von OSINT, angefangen bei der Historie, über die Definitionen bis hin zu den grundlegenden Konzepten.

Im zweiten Teil liegt der Fokus auf den notwendigen Fähigkeiten und Fertigkeiten sowie ganzheitlichen Schulungsansätzen, um in der Disziplin zu bestehen. Der dritte Teil deckt die rechtlichen Rahmenbedingungen und ethischen Fragestellungen der Thematik auf. Dabei wird ein einzigartiger Einblick in die Herausforderungen und Ungewissheiten dieser Disziplin gewährt. Das finale vierte Paper taucht in den gegenwärtigen technologischen Status quo von OSINT ein, präsentiert die neuesten Trends und analysiert die Diskrepanzen zwischen Theorie und Praxis.

Datum	Paper Thema
08.04.2024	Historische Herleitung und Definition von OSINT
01.07.2024	Ganzheitliche Schulung/Schulungsansätze
02.09.2024	Rechtliche und ethische Herausforderungen/Ungewissheiten
07.01.2025	Technologischer Status Quo

Verfolgen Sie die Serie für tiefgreifende Einblicke in die Intelligence-Disziplin OSINT.

Eine Kooperation der Unternehmen ESG Elektroniksystem- und Logistik-GmbH,
Munich Innovation Labs GmbH und PREVENCY GmbH

OSINT:

Rechtskonforme, ethische Entwicklung & Implementierung

Abstract

Open Source Intelligence (OSINT) hat sich zu einem essentiellen Instrument für Organisationen im Bereich der inneren und äußeren Sicherheit entwickelt. Dieser Beitrag adressiert die kritische Notwendigkeit einer rechtskonformen und ethischen Implementierung von OSINT-Lösungen. Er behandelt rechtliche und ethische Rahmenbedingungen, Privacy-by-Design-Strategien, zukunftssichere Konfigurationen, Best Practices für Implementierung und Nutzung sowie praktische Leitlinien für OSINT-Projekte.

Kernempfehlungen umfassen die Implementierung robuster Privacy-by-Design-Prinzipien, die Entwicklung flexibler Architekturen für Cloud- und On-Premise-Bereitstellungen, die Integration von KI-Technologien unter Berücksichtigung rechtlicher und ethischer Aspekte, die Etablierung umfassender Compliance-Prozesse und die kontinuierliche Anpassung an sich entwickelnde OSINT-Quellen und rechtliche Anforderungen.

Dieses Dokument dient als technischer Leitfaden für OSINT-Anwender und IT-Verantwortliche, insbesondere im Bereich der inneren und äußeren Sicherheit. Es ergänzt die juristische Beratung aus technischer Sicht; für spezifische Rechtsfragen wird die Konsultation qualifizierter Rechtsexperten empfohlen.

1. Einleitung

OSINT ermöglicht die systematische Akquisition, Analyse und Verwertung öffentlich zugänglicher Informationen aus diversen Quellen. Die Anwendung erstreckt sich über alle Phasen des Intelligence Cycles, wobe idie Methoden und Instrumente der Informationsgewinnung und -analyse maßgeblich durch den kontinuierlichen technologischen Fortschritt beeinflusst werden [1]. Daher ist eine umfassende Ausbildung der OSINT-Anwender, die das theoretische Fundament und praktische Kompetenzen gleichermaßen vermittelt, unerlässlich [2].

Um schließlich die OSINT-Potenziale voll auszuschöpfen, ist eine rechtskonforme Implementierung zwingend erforderlich. Die technischen Systeme zur Datenakquise und -auswertung müssen einer Vielzahl juristischer Vorgaben entsprechen und ethischen Maßstäben genügen. Fortschritte, insbesondere im Bereich KI, ermöglichen OSINT Auswertungen effizienter durchzuführen. Daher rücken Debatten über deren transparente und rechtmäßige Nutzung in den Vordergrund.

2. Rechtliche und ethische Rahmenbedingungen für OSINT-Lösungen

Bei der Nutzung von OSINT-Systemen sind diverse Rechtsgebiete zu berücksichtigen, darunter Datenschutzrecht (DSGVO, BDSG) [3, 4], Telekommunikations- und Medienrecht (TKG, DDG) [5, 6], sowie einsatzspezifische Regelungen und Sicherheitsgesetze. Für die nicht-polizeiliche Gefahrenabwehr sind das Zivilschutz- und Katastrophenhilfegesetz (ZSKG) sowie landesspezifische Katastrophenschutzgesetze maßgeblich [7]. Im Bereich der inneren Sicherheit gelten Polizeigesetze der Länder, das Bundeskriminalamtgesetz (BKAG) [8] und Verfassungsschutzgesetze [9]. Für die äußere Sicherheit ist insbesondere das BND-Gesetz (BNDG) [10] relevant sowie Artikel 87a des Grundgesetzes, welcher den Kernauftrag der Bundeswehr festlegt [11]. Zudem müssen Regelungen bezüglich des Einsatzes von Künstlicher Intelligenz beachtet werden, insbesondere die kommende KI-Verordnung zum EU AI Act [12]. Die KI-Verordnung zum EU AI Act wird in nationales Recht umgesetzt werden und wird den Einsatz von KI auch in OSINT-Systemen mit besonderen Regelungen hinsichtlich Anwendungen in der inneren und äußeren Sicherheit regeln.

Ethische Grundsätze bei der OSINT-Nutzung umfassen die Verhältnismäßigkeit der Datenerhebung und -nutzung, Transparenz und Rechenschaftspflicht, Schutz der Privatsphäre und persönlichen Freiheit, Fairness und Nicht-Diskriminierung sowie Datensicherheit und ver-

Abb. 2: Ethische und rechtliche Aspekte für OSINT Lösungen, Quelle: Eigene Darstellung.

antwortungsvoller Informationsumgang.
Je nach Anwendungskontext gelten unterschiedliche rechtliche Rahmenbedingungen. Beispielsweise Datenschutz in Notfall- und Krisensituationen, die Grenzen präventiver Datenerhebung, die Verwendung von OSINT-Erkenntnissen in Gerichtsverfahren und völkerrechtliche Bestimmungen bei internationalen Einsätzen.

3. Privacy-by-Design in OSINT-Systemen

Privacy-by-Design (PbD) integriert Datenschutz proaktiv in die Gestaltung und den Betrieb von IT-Systemen und Organisationsprozessen. Für OSINT-Systeme ist PbD besonders relevant, da es die Verarbeitung großer Mengen öffentlich zugänglicher Daten mit dem Schutz personenbezogener Informationen in Einklang bringt.

Implementierungsstrategien umfassen die zweckgebundene Datenerhebung und -verarbeitung, die Implementierung von Datenfiltern für sensitive Informationen, die Trennung von Datenhaltung und Verarbeitung sowie die automatische Löschung nach Zweckerfüllung. Zudem sollten Anonymisierungstechniken und reversible Pseudonymisierung für die notwendige Rückverfolgbarkeit eingesetzt werden.

Zugriffskontrolle und Verschlüsselung spielen eine zentrale Rolle. Rollenbasierte Zugriffskontrolle, Ende-zu-Ende-Verschlüsselung und regelbasierte granulare Zugriffskontrolle sind entscheidende Komponenten.

Beispiele für Privacy-by-Design-Funktionen

1. Automatische Erkennung und Maskierung personenbezogener Daten
2. Speicherdauer mit regelbasierter Löschung
3. Audit-Logs für alle Datenzugriffe und

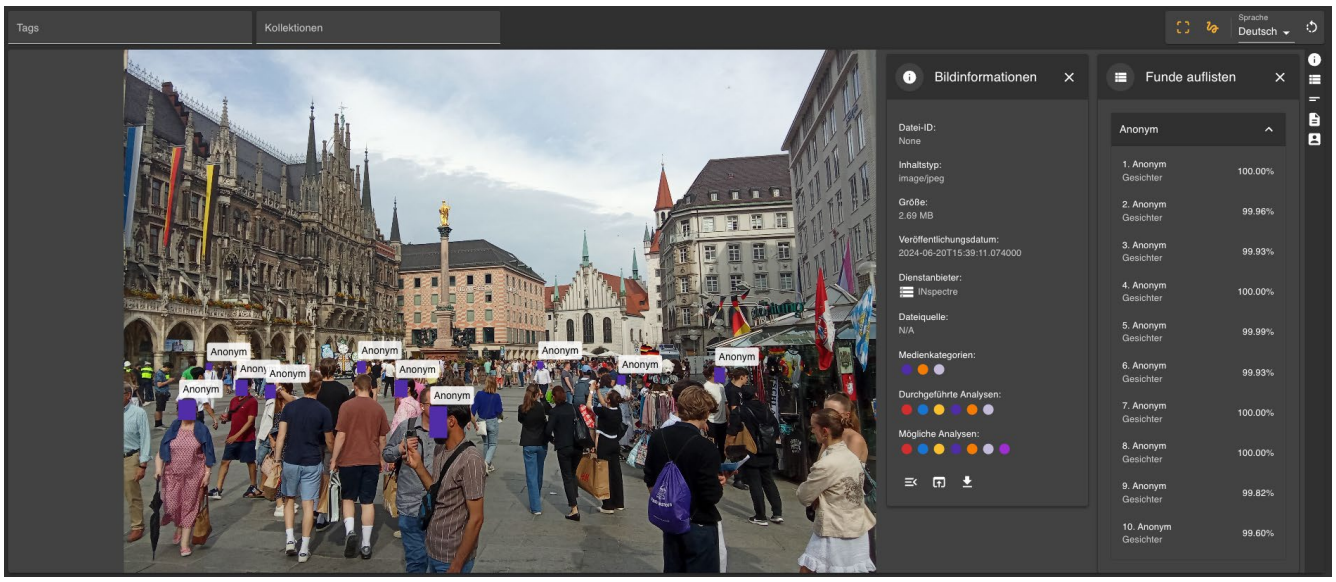


Abb. 3: Beispiel einer technischen Umsetzung zur Entfernung personenbezogener Informationen in der OSINT-Plattform INspectre, Quelle: Eigene Darstellung.

-verarbeitungen
4. Datenschutz-Folgenabschätzung für OSINT-Systeme bis hin zur Funktionsebene
5. Mandantenfähige Architektur zur Trennung von Daten

Die Implementierung von PbD in OSINT-Systeme erfordert einen ganzheitlichen Ansatz, der technische Maßnahmen mit organisatorischen Prozessen verbindet.

4. Zukunftssichere Konfiguration von OSINT-Systemen

Eine zukunftssichere Gestaltung von OSINT-Systemen erfordert eine flexible Architektur, KI-Integration und robuste Sicherheitsmechanismen, unter Berücksichtigung von On-Premise-Bereitstellungen.

Die Systemarchitektur sollte auf Microservices basieren, um eine einfache Integration und Aktualisierung zu ermöglichen. On-Premise-Bereitstellungen erfordern spezifische Deployment-Strategien für isolierte Umgebungen und die Unterstützung sowie Integration von Legacy-Systemen.

Bei der Integration von KI-Modellen müssen externe, Open-Source- und eigenentwickelte Modelle hinsichtlich Leistung, Sicherheit und On-Premise-Kompatibilität evaluiert werden. Ein robustes Testframework zur Überprüfung der KI-Modelle in On-Premise-Umgebungen ist essentiell, ebenso wie ein kontinuierliches Monitoring der Modellleistung und Überprüfung auf Bias.

Sicherheits- und Compliance-Mechanismen umfassen detaillierte Protokollierung aller Systemaktivitäten, automatisierte Compliance-Checks und die Implementierung starker Verschlüsselungsmechanismen. Regelmäßige Schulungen der Mitarbeiter in Datenschutz und Informationssicherheit mit Fokus auf On-Premise-Spezifika sind unerlässlich.

5. Best Practices für die Implementierung und Nutzung von OSINT-Systemen

Um der sich ständig wandelnden OSINT-Datenquellen gerecht zu werden, sollten Organisationen flexible Prozesse zur schnellen Integration neuer Quellen etablieren, Technologien zur Akquise und Auswertung regelmäßig aktualisieren und automatisierte Systeme zur Überwachung und Bewertung von Quellenveränderungen implementieren. Diese Maßnahmen ermöglichen eine kontinuierliche Anpassung an neue Informationsquellen und verbessern die Qualität der gewonnenen Daten.

Ein strukturierter, in das OSINT-System integrierter Genehmigungsprozess ist ebenfalls von herausragender Bedeutung. Dies umfasst die Implementierung von Workflow-Management für OSINT-Aktivitäten, die Konfiguration von Zugriffsrechten basierend auf Fallnummern oder Projektkennungen und die automatische Freischaltung bestimmter Analysefunktionen oder Datenakquisen nach Genehmigung. Ein solcher Prozess stellt sicher, dass nur autorisierte Personen Zugriff auf sensible Daten haben und die Analyseprozesse effizient und kontrolliert ablaufen.

Des Weiteren ist die Zusammenführung von Datenschutz-Folgenabschätzung und Compliance-Überwachung entscheidend. Dies beinhaltet die Integration von Datenschutz-Checks in OSINT-Workflows, die Implementierung automatisierter Compliance-Monitoring-Tools und die regelmäßige Überprüfung und Aktualisierung der Datenschutz- und Compliance-Maßnahmen. Dies gewährleistet, dass die OSINT-Aktivitäten im Einklang mit den geltenden Datenschutzbestimmungen und Compliance-Richtlinien durchgeführt werden.

Umfassende Schulungsprogramme, flexible Prozesse, strukturierte Genehmigungsabläufe und die Integration von Datenschutz- und Compliance-Maßnahmen sind also entscheidend für die effektive Nutzung von OSINT. Durch die Implementierung dieser Elemente können Organisationen ihre OSINT-Aktivitäten optimieren und gleichzeitig rechtlichen und ethischen Anforderungen gerecht werden.

6. Fazit und Checkliste

Die rechtskonforme und ethische Implementierung von OSINT-Lösungen erfordert eine ganzheitliche Herangehensweise. Kernaspekte umfassen eine flexible und zukunftssichere Systemarchitektur, die Integration von

KI-Technologien unter Berücksichtigung rechtlicher und ethischer Aspekte, robuste Sicherheits- und Compliance-Mechanismen, umfassende Schulungsprogramme und kontinuierliche Anpassung an sich verändernde OSINT-Quellen und rechtliche Rahmenbedingungen.

Handreichung: Leitfragen für rechtskonforme Entwicklung und Einführung von OSINT

1. Zweck und Umfang: Wie definieren Sie den spezifischen Einsatzbereich, d.h. Einsatzzweck und Nutzergruppe und die Ziele Ihres OSINT-Systems unter Berücksichtigung rechtlicher und ethischer Grenzen?

2. Rechtliche Grundlagen: Welche technischen und organisatorischen Maßnahmen ergreifen Sie, um die Einhaltung relevanter Gesetze (z.B. DSGVO, bereichsspezifische Vorschriften) bei der Datenerfassung und -verarbeitung sicherzustellen?

3. Datenschutz und Sicherheit: Wie gewährleisten Sie den Schutz und die Sicherheit der gesammelten Daten von der Erfassung bis zur Löschung?

4. Risikobasierter Ansatz: Entwicklung spezifischer Gegenmaßnahmen für jedes identifizierte Risiko.

5. Nutzerverwaltung und Zugriffsrechte: Welche Strategie verfolgen Sie bei der Gestaltung von Nutzerrollen, Zugriffsrechten und Genehmigungsprozessen für OSINT-Aktivitäten?

6. Schulung und Bewusstseinsbildung: Wie stellen Sie sicher, dass alle Nutzer die rechtlichen, ethischen und praktischen Aspekte der OSINT-Nutzung verstehen und anwenden?

7. Kontinuierliche Überprüfung und Anpassung: Welche Prozesse etablieren Sie zur regelmäßigen Überprüfung und Anpassung Ihrer OSINT-Praktiken an sich ändernde rechtliche, technologische und organisatorische Anforderungen?

Hinweis: Dieser Leitfaden dient als Orientierungshilfe. Für eine rechtliche Bewertung sind Rechtsexperten und Datenschutzbeauftragte zu konsultieren.

7. Glossar

OSINT (Open Source Intelligence): Informationsgewinnung aus öffentlich zugänglichen Quellen.

Privacy-by-Design (PbD): Konzept, bei dem der Datenschutz von Anfang an in die Gestaltung von Systemen und Prozessen integriert wird.

DSGVO (Datenschutz-Grundverordnung): EU-Verordnung zum Schutz personenbezogener Daten.

Pseudonymisierung: Verarbeitung personenbezogener Daten so, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer Person zugeordnet werden können.

Anonymisierung: Prozess, bei dem personenbezogene Daten derart verändert werden, dass sie nicht mehr einer spezifischen Person zugeordnet werden können.

API (Application Programming Interface): Programmierschnittstelle, die die Kommunikation zwischen verschiedenen Softwarekomponenten ermöglicht.

Microservices: Architekturstil, bei dem Anwendungen als Sammlung kleiner, unabhängiger Dienste entwickelt werden.

Containerisierung: Technologie zur Isolierung von Anwendungen in standardisierten Einheiten (Containern) für einfache Bereitstellung und Skalierung.

Audit-Trail: Chronologische Aufzeichnung aller relevanten Aktivitäten in einem System zur Nachvollziehbarkeit und Überprüfung.

Compliance: Einhaltung von Gesetzen, Richtlinien und ethischen Standards.

On-Premise: Bereitstellung und Betrieb von Software und Hardware in den eigenen Räumlichkeiten eines Unternehmens, im Gegensatz zu Cloud-basierten Lösungen.

8. Interview mit Robert Pelzer, TU Berlin, Zentrum für Technik und Gesellschaft: Ethische Aspekte von OSINT in Behörden

Interviewer: Herr Pelzer, basierend auf Ihrer Forschung: Welche ethischen Grundsätze sollten OSINT-Anwender in Behörden bei ihrer täglichen Arbeit besonders beachten?
Robert Pelzer: Werden im Zuge von OSINT-Recherchen Informationen über Personen oder Gruppen gesammelt, wird in Freiheitsrechte der Betroffenen eingegriffen. Entscheidend ist daher, dass OSINT-Anwender:innen in Behörden die Verhältnismäßigkeit ihrer Maßnahmen im Blick behalten, d.h. v.a. die Eingriffstiefe der geplanten Auswertungen mit dem erwarteten Nutzen abzuwägen Ein ethischer Leitfaden kann hier als wichtige Ergänzung zu den rechtlichen Rahmenbedingungen dienen. Besonders wichtig sind zudem Prinzipien wie Transparenz, Rechenschaftspflicht und der Schutz der Privatsphäre von insbesondere Unbeteiligten.

Interviewer: Wie können Nutzer die Vorteile von KI in OSINT-Systemen nutzen und gleichzeitig ethische Risiken minimieren?
Robert Pelzer: Die Integration von KI in OSINT-Systeme bietet enorme Potenziale, birgt aber auch Risiken. Um diese zu minimieren, wäre die Implementierung von „Compliance und Ethik"-Modulen direkt in die OSINT-Systeme denkbar. Diese könnten beispielsweise Abfragen beinhalten, die Nutzer:innen für die Eingriffstiefe ihrer Aktionen sensibilisieren.

Interviewer: Können Sie ein Fallbeispiel aus Ihrer Forschung schildern, das Behördenmitarbeiter für ethische Dilemmata bei der OSINT-Nutzung sensibilisieren könnte?
Robert Pelzer: Ein Beispiel für ethische Herausforderungen bildet die Auswertung von großen Datenmengen mithilfe von KI-gestützten Analysetools, die relevante Inhalte vorselektieren, so dass Auswertende sich auf diese Inhalte fokussieren können. Kein KI-Modell kann jedoch alle relevanten Inhalte finden. Wann, d.h. bei welchen Auswertungen, ist man bereit eine höhere Fehlerquote, z.B. eine Sensitivität von nur 80%, in Kauf zu nehmen, um die Effizienz von Massendatenauswertungen zu erhöhen. In welchen Fällen ist eine viel höhere Sensitivität erforderlich? Das sind ethische und rechtliche Fragen, die in der Praxis im Dialog mit der Gesellschaft verhandelt werden sollten.

Interviewer: Welche praktikablen Methoden empfehlen Sie Behörden, um ethische Standards in ihre OSINT-Prozesse zu integrieren, ohne die Effizienz zu beeinträchtigen?
Robert Pelzer: Neben Schulungen und Leitlinien sehe ich großes Potenzial in der Erforschung technischer Lösungen. Zum Beispiel könnten Tools implementiert werden, die Anwender:innen darin unterstützen, die Eingriffstiefe von OSINT-Aktivitäten zu bewerten. Dies würde die Einhaltung ethischer Standards erleichtern, ohne die Effizienz zu beeinträchtigen, aber auch ein ethisch kontrolliertes Vorgehen dokumentieren und die Anwender:innen dadurch in ihrer Compliance absichern.

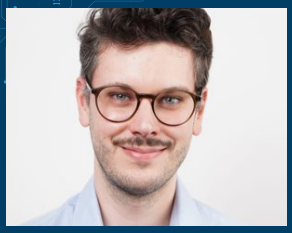
Interviewer: Welche ethischen Herausforderungen sehen Sie auf OSINT-Anwender in Behörden zukommen, und wie können sie sich darauf vorbereiten?
Robert Pelzer: Die rasante technologische Entwicklung im OSINT-Bereich stellt uns vor ständig neue ethische Herausforderungen. Ein Beispiel ist die zunehmende Verfügbarkeit von Gesichtserkennungstechnologien. Um darauf vorbereitet zu sein, müssen Behörden ihre ethischen Richtlinien regelmäßig überprüfen und anpassen. Zudem ist es wichtig, den Diskurs mit Expert:innen aus Ethik, Recht und Technologie zu suchen und zu pflegen. Abschließend möchte ich betonen, dass die Integration von Ethik in OSINT-Systeme ein komplexes und dynamisches Forschungsfeld ist. Die Herausforderung besteht darin, praktikable Lösungen zu entwickeln, die sowohl den praktischen Anforderungen der Auswertenden, als auch den rechtlichen und ethischen Standards gerecht werden. Im Rahmen des vom BMBF im Rahmen der zivilen Sicherheitsforschung geförderten Projektes INTEGER wurden ethische und rechtliche Gestaltungsanforderungen für Softwareplattformen zur Unterstützung polizeilicher Internetauswertungen entwickelt. Diese wurden im Projekt KISTRA mit Blick auf den Einsatz von KI-Modellen ergänzt. Im nächsten Schritt ginge es darum, entsprechende „Compliance und Ethik"-Module technisch zu implementieren und mit Anwender:innen zu testen.

Das vierte Paper zeigt den gegenwärtigen technologischen Status quo von OSINT auf, präsentiert die neuesten Trends und analysiert die Diskrepanzen zwischen Theorie und Praxis. Erscheinungsdatum: 07.01.2025.

Ansprechpartner

Dr. Stefan Taing
Autor
Managing Director
✉ st@munich-innovation.com

MunichInnovationLabs



Yannick Kuplewatzki
Autor
Wissenschaftlicher Mitarbeiter
✉ yk@munich-innovation.com

MunichInnovationLabs

Timo Keim
Leiter Public Security Academy
✉ Timo.Keim@esg.de

ESG
A HENSOLDT COMPANY

Robert Pelzer
Interview Partner
TU Berlin

Technische Universität Berlin

8. Quellen

[1] Kayser, F.: OSINT auf den Spuren. Die Evolution von Open Source Intelligence. Fürstenfeldbruck, Germany, 2024.

[2] Klewer, S.: OSINT lehren und lernen: Ganzheitliche Ansätze für eine effektive und zukunftssichere Ausbildung. Fürstenfeldbruck, Germany, 2024.

[3] European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Available at: http://data.europa.eu/eli/reg/2016/679/oj. Accessed August 19, 2024.

[4] Bundesministerium der Justiz: Bundesdatenschutz-

gesetz (BDSG). Available at: https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf. Accessed August 19, 2024.
[5] Bundesministerium der Justiz: Telekommunikationsgesetz (TKG). Available at: https://www.gesetze-im-internet.de/tkg_2021/TKG.pdf. Accessed August 19, 2024.
[6] Bundesministerium der Justiz: Digitale-Dienste-Gesetz (DDG). Available at: https://www.gesetze-im-internet.de/ddg/DDG.pdf. Accessed August 19, 2024.
[7] Bundesministerium der Justiz: Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz - ZSKG). Available at: https://www.gesetze-im-internet.de/zsg/ZSKG.pdf. Accessed August 19, 2024.
[8] Bundesministerium der Justiz: Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG). Available at: https://www.gesetze-im-internet.de/bkag_2018/BKAG.pdf. Accessed August 19, 2024.
[9] Bundesministerium der Justiz: Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG). Available at: https://www.gesetze-im-internet.de/bverfschg/BVerfSchG.pdf. Accessed August 19, 2024.
[10] Bundesministerium der Justiz: Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG). Available at: https://www.gesetze-im-internet.de/bndg/BNDG.pdf. Accessed August 19, 2024.
[11] Bundesministerium der Justiz: Grundgesetz für die Bundesrepublik Deutschland, Art 87a. Available at: https://www.gesetze-im-internet.de/gg/art_87a.html. Accessed August 19, 2024.
[12] European Union: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION. Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206. Accessed August 19, 2024.