

OSINT CHRONICLE



Quarterly paper series introducing
the world of open sources

OSINT CHRONICLE





Quarterly paper series introducing
the world of open sources



The four-part series of papers on Open Source Intelligence (OSINT) provides a quarterly insight into the profound world of this intelligence gathering discipline. The series starts on April 8, 2024 and continues on the first Monday of each subsequent quarter. The papers are designed to shed light on different facets of OSINT in order to provide readers with an in-depth understanding of the subject matter. Each paper will therefore focus on a different key area.

The first paper will be dedicated to the basic pillars of OSINT, starting with the history, definitions and funda-

mental concepts. The second paper will focus on the necessary skills and abilities as well as holistic training approaches to excel in the discipline. The third part will cover the legal framework and ethical issues surrounding the subject. It will provide a unique insight into the challenges and uncertainties of this discipline. The final fourth paper will conclude by exploring the current technological status quo of OSINT, presenting the latest trends and analyzing the discrepancies between theory and practice.

Date		Paper-topic
08.04.2024		Historical derivation and definition of OSINT
01.07.2024		Holistic training/training approaches
02.09.2024		Legal and ethical challenges/uncertainties
07.01.2025		Technological status quo

Follow the series for in-depth insights into the intelligence discipline OSINT.

A cooperation of the companies ESG Elektroniksystem- und Logistik-GmbH,
Munich Innovation Labs GmbH and PREVENY GmbH

OSINT:

Legal and Ethical Development & Implementation

Abstract

Open Source Intelligence (OSINT) has evolved into an essential tool for organizations involved in internal and external security. This paper addresses the critical need for a legally compliant and ethical implementation of OSINT solutions. It covers legal and ethical frameworks, privacy-by-design strategies, future-proof configurations, best practices for implementation and use, and practical guidelines for OSINT projects.

Key recommendations include the implementation of robust privacy-by-design principles, the development of flexible architectures for cloud and on-premise deployments, the integration of AI technologies with consideration for legal and ethical aspects, the establishment of comprehensive compliance processes, and continuous adaptation to evolving OSINT sources and legal requirements.

This document serves as a technical guide for OSINT users and IT managers, particularly in the field of internal and external security. It complements legal advice from a technical perspective; for specific legal questions, consulting qualified legal experts is recommended.

1. Introduction

OSINT enables the systematic acquisition, analysis, and utilization of publicly accessible information from various sources. Its application spans all phases of the intelligence cycle, with the methods and tools for information gathering and analysis being significantly influenced by continuous technological advancements [1]. Therefore, comprehensive training of OSINT users, which imparts both theoretical knowledge and practical skills, is essential [2].

In order to fully exploit OSINT's potential, legal compliance in its implementation is mandatory. The technical systems for data acquisition and analysis must

comply with a multitude of legal requirements and meet ethical standards. Advances, particularly in AI, allow OSINT evaluations to be conducted more efficiently. Consequently, debates about their transparent and lawful use are gaining prominence.

2. Legal and Ethical Frameworks for OSINT Solutions

The use of OSINT systems requires consideration of various legal domains, including data protection law (GDPR, BDSG) [3, 4], telecommunications and media law (TKG, DDG) [5, 6], as well as specific regulations and security laws. For non-police emergency management, the Civil Protection and Disaster Relief Act (ZSKG) and state-specific disaster protection laws are decisive [7]. In the area of internal security, state police laws, the Federal Criminal Police Office Act (BKAG) [8], and intelligence service laws apply [9]. For external security, the BND Act (BNDG) [10] and Article 87a of the Basic Law, which defines the core mandate of the Bundeswehr, are particularly relevant [11]. Additionally, regulations regarding the use of Artificial Intelligence must be observed, especially the upcoming AI Regulation under the EU AI Act [12]. The AI Regulation under the EU AI Act will be transposed into national law and will include specific rules for the use of AI in OSINT systems concerning applications in internal and external security.

Ethical principles in the use of OSINT include the proportionality of data collection and use, transparency and accountability, privacy and personal freedom protection, fairness and non-discrimination, as well as data security and responsible information handling.

Depending on the application context, different legal frameworks apply, such as data protection in emergency and crisis situations, the limits of preventive data collection, the use of OSINT findings in court proceedings, and international legal provisions for international missions.

- Legal framework
- Ethical principles

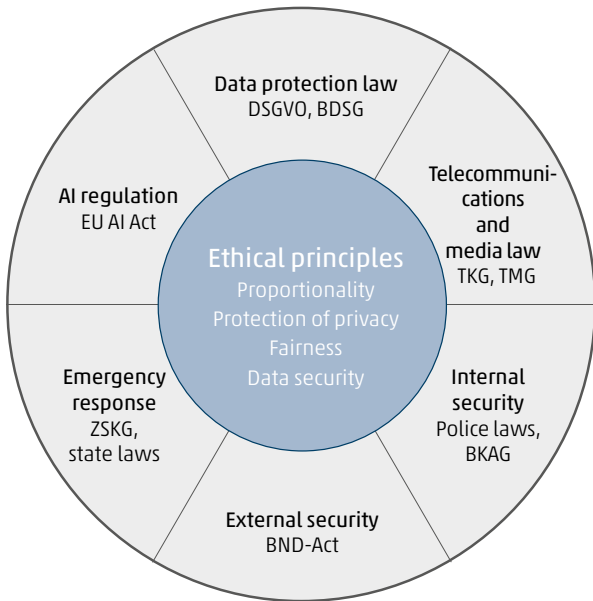


Fig. 2: Ethical and legal aspects of OSINT solutions, Source: Own illustration.

3. Privacy-by-Design in OSINT-Systems

Privacy-by-Design (PbD) proactively integrates data protection into the design and operation of IT systems and organizational processes. PbD is particularly relevant for OSINT systems, as it aligns the processing

of large amounts of publicly accessible data with the protection of personal information.

Implementation strategies include purpose-specific data collection and processing, the implementation of data filters for sensitive information, the separation of data storage and processing, and automatic deletion after purpose fulfillment. Additionally, anonymization techniques and reversible pseudonymization should be employed for necessary traceability.

Access control and encryption play a key role. Role-based access control, end-to-end encryption, and rule-based granular access control are critical components.

Examples of Privacy-by-Design functions:

1. Automatic detection and masking of personal data
2. Storage duration with rule-based deletion
3. Audit logs for all data access and processing
4. Data protection impact assessment for OSINT systems down to the function level
5. Multi-tenant architecture to separate data

The implementation of PbD in OSINT systems requires a holistic approach that combines technical measures with organizational processes.

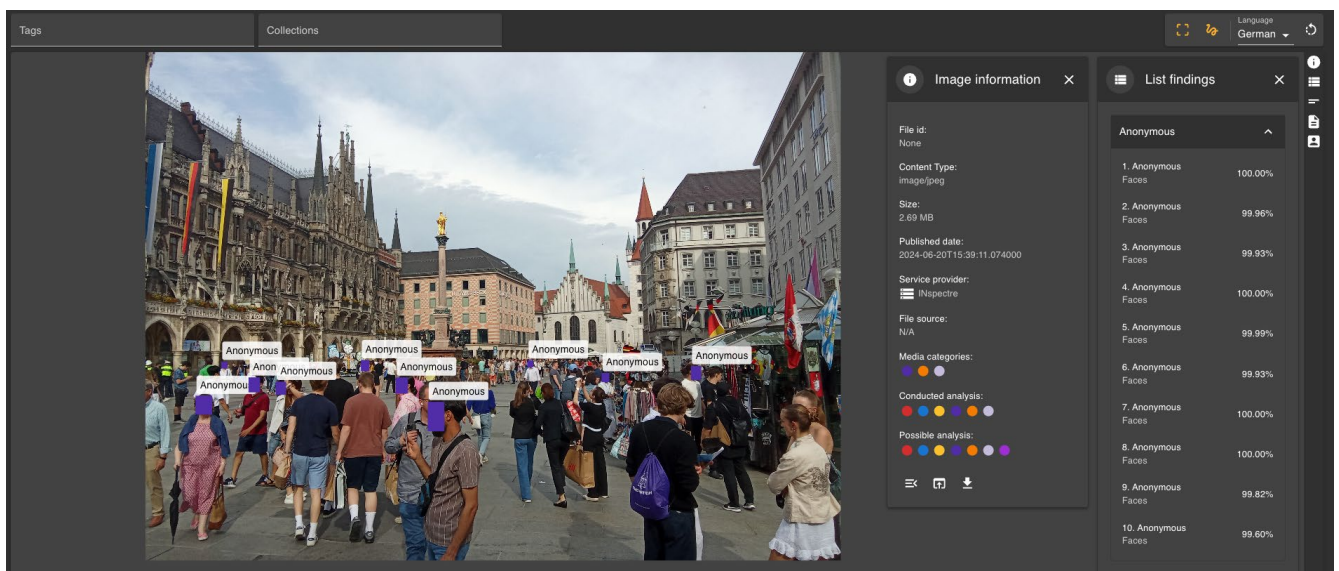


Fig. 3: Example of technical implementation to remove personal information in the OSINT platform INspectre, Source: Own illustration.

4. Future-Proof Configuration of OSINT Systems

Future-proof design of OSINT systems requires flexible architecture, AI integration, and robust security mechanisms, considering on-premise deployments. The system architecture should be based on microservices to enable easy integration and updates. On-premise deployments require specific deployment strategies for isolated environments and support for and integration with legacy systems.

When integrating AI models, external, open-source, and self-developed models must be evaluated regarding performance, security, and on-premise compatibility. A robust test framework to verify AI models in on-premise environments is essential, as is continuous monitoring of model performance and checking for bias.

Security and compliance mechanisms include detailed logging of all system activities, automated compliance checks, and the implementation of strong encryption mechanisms. Regular training of employees in data protection and information security, with a focus on on-premise specifics, is essential.

5. Best Practices for the Implementation and Use of OSINT Systems

To keep pace with constantly evolving OSINT data sources, organizations should establish flexible processes for the rapid integration of new sources, regularly update technologies for acquisition and evaluation, and implement automated systems for monitoring and assessing changes in sources. These measures enable continuous adaptation to new information sources and improve the quality of the data obtained.

A structured, integrated approval process within the OSINT system is also of paramount importance. This includes implementing workflow management for OSINT activities, configuring access rights based on case numbers or project identifiers, and automatically enabling certain analysis functions or data acquisitions upon approval. Such a process ensures that only authorized personnel have access to sensitive data and

that the analysis processes run efficiently and under control.

Furthermore, combining data protection impact assessment and compliance monitoring is crucial. This includes integrating data protection checks into OSINT workflows, implementing automated compliance monitoring tools, and regularly reviewing and updating data protection and compliance measures. This ensures that OSINT activities are conducted in accordance with applicable data protection regulations and compliance guidelines.

Comprehensive training programs, flexible processes, structured approval procedures, and the integration of data protection and compliance measures are therefore crucial for the effective use of OSINT. By implementing these elements, organizations can optimize their OSINT activities while meeting legal and ethical requirements.

6. Conclusion and Checklist

The legally compliant and ethical implementation of OSINT solutions requires a holistic approach. Key aspects include flexible and future-proof system architecture, the integration of AI technologies considering legal and ethical aspects, robust security and compliance mechanisms, comprehensive training programs, and continuous adaptation to evolving OSINT sources and legal frameworks.

Guideline: Key Questions for the Legally Compliant Development and Introduction of OSINT

- 1. Purpose and Scope:** How do you define the specific area of application, i.e., purpose and user group, and the goals of your OSINT system considering legal and ethical boundaries?
- 2. Legal Basis:** What technical and organizational measures do you take to ensure compliance with relevant laws (e.g., GDPR, sector-specific regulations) in data collection and processing?

3. Data Protection and Security: How do you ensure the protection and security of collected data from collection to deletion?

4. Risk-Based Approach: Develop specific countermeasures for each identified risk.

5. User Management and Access Rights: What strategy do you pursue in designing user roles, access rights, and approval processes for OSINT activities?

6. Training and Awareness: How do you ensure that all users understand and apply the legal, ethical, and practical aspects of OSINT use?

7. Continuous Review and Adaptation: What processes do you establish to regularly review and adapt your OSINT practices to changing legal, technological, and organizational requirements?

Note: This guide serves as an orientation. For a legal evaluation, legal experts and data protection officers should be consulted.

7. Glossary

OSINT (Open Source Intelligence): Information gathering from publicly accessible sources.

Privacy-by-Design (PbD): A concept where data protection is integrated into the design of systems and processes from the outset.

GDPR (General Data Protection Regulation): EU regulation for the protection of personal data.

Pseudonymization: Processing personal data so that it can no longer be attributed to a specific person without additional information.

Anonymization: Process by which personal data is altered so that it can no longer be attributed to a specific person.

API (Application Programming Interface): Interface that enables communication between different software components.

Microservices: Architectural style in which applications are developed as a collection of small, independent services.

Containerization: Technology for isolating applications in standardized units (containers) for easy deployment and scaling.

Audit Trail: Chronological record of all relevant activities in a system for traceability and review.

Compliance: Adherence to laws, guidelines, and ethical standards.

On-Premise: Deployment and operation of software and hardware on a company's premises, as opposed to cloud-based solutions.

8. Interview with Robert Pelzer, TU Berlin, Center for Technology and Society: Ethical Aspects of OSINT in Government Agencies

Interviewer: Mr. Pelzer, based on your research, what ethical principles should OSINT practitioners in government agencies particularly observe in their daily work?

Robert Pelzer: When conducting OSINT investigations, gathering information about individuals or groups can infringe on the affected parties' rights. Therefore, it is crucial that OSINT practitioners in government agencies consider the proportionality of their actions, meaning they should weigh the depth of the planned analyses against the expected benefits. An ethical guideline can serve as an important supplement to the legal framework. Principles such as transparency, accountability, and the protection of privacy, especially for uninvolved parties, are particularly important.

Interviewer: How can users leverage the advantages of AI in OSINT systems while minimizing ethical risks?

Robert Pelzer: The integration of AI into OSINT systems offers enormous potential but also carries risks. To minimize these, it would be conceivable to implement "compliance and ethics" modules directly into the OSINT systems. These could include queries that raise user

awareness about the level of intrusion their actions entail.
Interviewer: Can you describe a case study from your research that could make government employees aware of ethical dilemmas in OSINT usage?

Robert Pelzer: An example of ethical challenges is the analysis of large data sets using AI-based analysis tools that pre-select relevant content, allowing analysts to focus on these contents. However, no AI model can identify all relevant content. When, that is, in which evaluations, are you willing to accept a higher error rate, such as a sensitivity of only 80%, in order to increase the efficiency of mass data analysis? In which cases is a much higher sensitivity required? These are ethical and legal questions that should be negotiated in practice through dialogue with society.

Interviewer: What practical methods do you recommend for government agencies to integrate ethical standards into their OSINT processes without compromising efficiency?

Robert Pelzer: Besides training and guidelines, I see great potential in exploring technical solutions. For example, tools could be implemented that assist users in evaluating the level of intrusion involved in their OSINT activities. This would facilitate the adherence to ethical standards without compromising efficiency while also documenting ethically controlled actions and thereby protecting users in their compliance.

Interviewer: What ethical challenges do you foresee for OSINT practitioners in government agencies, and how can they prepare for them?

Robert Pelzer: The rapid technological advancements in the OSINT field present us with constantly new ethical challenges. An example is the increasing availability of facial recognition technologies. To be prepared for this, government agencies must regularly review and adapt their ethical guidelines. It is also important to engage in and maintain discourse with experts in ethics, law, and technology.

In conclusion, I would like to emphasize that integrating ethics into OSINT systems is a complex and dynamic research field. The challenge lies in developing practical solutions which meet both the practical requirements of the analysts and the needs of government agencies, while also adhering to legal and ethical standards. As part of the INTEGER project, funded by the BMBF within the framework of civil security research, ethical and legal design requirements for software platforms to

support police internet analysis were developed. These were further supplemented in the KISTRA project with regard to the use of AI models. The next step would be to technically implement the corresponding 'Compliance and Ethics' modules and test them with users.

The fourth paper presents the current technological status quo of OSINT, outlines the latest trends and analyzes the discrepancies between theory and practice. Publication date: 07.01.2025.

Contacts



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



Yannick Kuplewatzki
Author
Postgraduate researcher
✉ yk@munich-innovation.com



Timo Keim
Head of Public Security Academy
✉ Timo.Keim@esg.de



Robert Pelzer
Interview Partner
TU Berlin



8. References

[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: Bundesdatenschutzgesetz (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.