Compliance Report

ECoD Gemeinnützige GmbH, December 2025/January 2026, Dunja Ganser,
Season 2024/2025

(v0.1., review 7 Jan, 20 Jan 2026, DG)

Preliminary Considerations

Adherence to compliance guidelines and internal requirements is a management task and responsibility. The Compliance Officer's task is to support the management, conduct risk analyses, draft a report once a year, conduct in-person meetings with management twice a year, report to and engage with the ECoD Team and act as a point of contact for any compliance-related incidents.

Scope

The report provides key information to all employees, management and stakeholders.
Date(s) of Review: ongoing monitoring throughout the period in question.
Note: Data- and Cyber-Security and Data Protection/Data Privacy are not covered by the Compliance Officer and thus are not included in the report.

Compliance Risk Management

A compliance risk management analysis was conducted and implemented. In this process, compliance-relevant risks were identified and assessed, including their potential impact and likelihood of occurrence. For each task, the relevant compliance matters were assigned to the responsible person or group of persons, and the affected target groups were clearly identified.

Monitoring and Controlling

Monitoring and controlling activities are carried out on an ongoing basis throughout the observation period. From a commercial and operational perspective, appropriate monitoring mechanisms have been introduced and, where necessary and reasonable, supplemented by audit processes and key performance indicator (KPI) reporting.

The ECoD NPO has established a framework based on two pillars:

- Organisational approach: specific compliance responsibilities are embedded in daily work routines.

- Structural approach: internal regulations are regularly reviewed and updated, developments in external laws and regulations are monitored, and external experts are involved where appropriate.

Compliance Assessment

In the area of **data protection**, which does not fall within my direct remit, the current structures and priorities are not fully transparent from a compliance perspective. For future compliance work, increased visibility of key focus areas and ongoing developments in data protection would be beneficial. Given the growing interdependence of data protection, compliance, and artificial intelligence, a strict separation of these domains appears neither practical nor appropriate.

With respect to **copyright**, an increased level of attention is required, particularly in light of the EU AI Act. From a compliance standpoint, a transparent and clearly defined approach within the communications department is advisable. The establishment of a structured overview or database of media assets, classified from a copyright perspective, would support risk mitigation and legal certainty.

The development of the **AI guidelines** is currently being carried out by a designated team. The process reflects a strategic approach and aims to ensure appropriate and coordinated involvement of both institutions in addressing AI-related compliance requirements.

With regard to **compliance-relevant subject matters**, there is demonstrable expertise within both the Institute and the non-profit organisation. While this expertise is available, its use is currently not fully systematic. There is potential to leverage existing knowledge more effectively, in particular for structured training and capacity-building purposes, and to promote more consistent knowledge sharing between both entities. Addressing this would also contribute to reducing parallel structures and clarifying the responsibilities.

All **compliance-relevant documentation**, in particular but not limited to materials related to the European Capital of Democracy, has been reviewed, approved, and published through a coordinated process (throughout summer 2025). This reflects a collaborative approach and provides a consolidated basis for compliance-related communication and governance.

In the area of **events and event management**, a workshop was conducted to identify relevant risk fields. As a result, several priority areas were identified in which measures were considered necessary. The implementation of these measures remains a key factor for mitigating event-related compliance and safety risks.

Recommendations

- **Incident Reporting System:**
  The incident reporting system should be reviewed and updated to ensure clarity, consistency, and effective usability from a compliance perspective. And should also be more user-friendly.

- **Training and Awareness:**
  Regular and structured training and awareness-raising measures should be established for compliance-relevant topics, including copyright, data protection, and the EU AI Act, as well as the communication of the internal AI guidelines.
- **Event Management – Safety and Security and Awareness Guidelines:**
  Event Management should provide the most recent versions of the Safety and Security Guidelines and the Awareness Concept for compliance review and documentation purposes.