The Hague, 23/10/2024
EDOC#1327390 v4
C3-12 – Europol Innovation Lab

ODIN
(PD)

Research & Innovation Sandbox
(Personal Data Processing Environment)

Use & Management Policy

TABLE OF CONTENTS

1. INTRODUCTION

The Europol Research & Innovation Sandbox is called ODIN (Operational Data for Innovation).

During the interim stage of development of ODIN, there will be two distinct data processing environments:

1. **In the Operations Network, a data processing environment that will be permitted to process personal data (covered by this Use & Management Policy): this is ODIN (PD)**
2. In the R&D Network, a data processing environment not permitted to process personal data: this is ODIN (no-PD) – see EDOC-#1315315.

In the target state, still to be defined, the assumption is that there will be a single data processing environment with the appropriate access control, user-based rights, data segmentation, and full functional separation from other services at Europol in line with the Europol Regulation. This environment will simply be called ODIN.

1.1. Purpose

The purpose of this document is to outline the rules for the appropriate and compliant use of ODIN (PD), the *Research & Innovation Sandbox (R&I Sandbox)—personal data processing environment*.

This document is intended for internal use within Europol, but its policy statements also apply to external Law Enforcement users insofar as they make use of ODIN (PD), via specific terms and conditions for all users of this data processing environment.[1]

This Policy is intended to establish acceptable and prohibited uses of ODIN (PD) and to protect Europol and its systems and infrastructure from illegal or harmful actions committed by users of this environment, whether knowingly or unknowingly.

This policy augments the Europol Operations Network Use Policy (EDOC-#739097), specifically as it applies to the 'separate, isolated and protected data processing environment within Europol' in line with Article 33a(2)(d)(i) ER.

This policy document is the sister document of EDOC-#1315315 – ODIN (no-PD) - *Research & Innovation Sandbox—non-personal data environment*.

1.2 Policy Coverage

On the basis of

- the definition in Article 2(v) of the amended Europol Regulation (ER) of 2022[2] ('research and innovation projects')

and on the basis of

- the task defined in Article 4 (1)(v) ER[3]

[redacted]

[2] EDOC-#1237223, see also EDOC-#1263057

[3] "proactively monitor research and innovation activities that are relevant for the achievement of Europol's objectives and contribute to such activities by supporting related activities of Member States and by implementing its own research and innovation activities, including projects for the development, training, testing and validation of algorithms for the development of specific tools for the use by law enforcement authorities, and disseminate the results of the activities to the Member States in accordance with Article 67;"

Europol may process personal data for research and innovation projects (Article 18(2)(e) ER). Such processing may also take place with the aim of creating synergies between EU research and innovation projects under Article 4(1)(w) ER.

The ER, furthermore, specifies the creation of a "separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out research and innovation projects" as laid down in Article 33a(2)(d)(i) ER.

This Use & Management Policy covers only those use cases that explicitly require the use of operational personal data in a separate, isolated and protected data processing environment in Europol.

Note: the process by which projects under Article 33a ER are run is not in the scope of this policy document, but may be found in EDOC-#1160881 – *Support R&I projects processing personal data (Art 33a ER) – Process Description, published on 21/12/2023.*

[redacted]

1.3 Scope

This policy covers the following aspects of the Use and Management ODIN (PD) for R&I projects requiring the use of personal data:

- **Intended use of ODIN (PD)**
- **Access control**
- **Content management, data ownership and responsibilities**
- **Security**
- **Policy Enforcement**

1.2. Owner of the Policy

The owner of this policy is the Europol Innovation Lab.

1.3. Definitions

In the context of this specific policy, the name ODIN (PD) refers only to the data processing environment that is permitted to process personal data.

Term	Definition
ODIN	The generic name for the R&I Sandbox environment at Europol
ODIN (PD)	The specific name of the data processing environment within the R&I Sandbox permitted to process personal data. The data processing environment subject to this policy.
ODIN (no-PD)	The specific name of the data processing environment within the R&I Sandbox not permitted to process personal data.
Expert	A person who is very knowledgeable or skilled in a particular law enforcement related area.
R&I Sandbox	A catch-all term used to highlight the experimental nature of the projects in ODIN. From a technical perspective, it is no different to other such data processing environments at Europol, adhering to the same security controls to ensure the same data integrity and compliance standards. With the involvement of the EDPS, it would become a regulatory sandbox.
Operational personal data	Is defined in Article 3(2) of Regulation 2018/1725, which became applicable to Europol as a result of Article 27a of the ER, as: all

Term	Definition
	personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies. For the purpose of this policy, this content must have been furnished by the data owner with an express permission to permit the use for R&I processing purposes.
Users	Europol users (as defined in more detail at 2.1 below) involved in research & innovation project activities under a particular obligation of discretion or confidentiality.
Europol classified information **and** **Europol classified documents**	Information or documents subject to additional security measures and marked with one of the classification levels RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE / EU CONFIDENTIAL, SECRET UE / EU SECRET or TRÈS SECRET UE / EU TOP SECRET in accordance with Article 42 of the Europol Security Manual.
"Processing of information" **or** **"Processing of data"**	Any operation or set of operations which is performed on operational personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
ICT resources	Any Information & Communication Technology device or solution, such as: ▪ Desktop and Laptop Computers ▪ Mobile office ▪ Telephones ▪ Software applications ▪ Storage solutions, such as SAN or NAS
Uptake	A process whereby the results and outputs of a specific research and innovation project are made available for the operational analysis data processing purpose. Uptake may lead to the results and outputs of R&I projects to be added to the Europol ICT Workplan via the standard annual portfolio processes (and subsequent compliance steps, such as defined in Art. 39 ER). Or it may lead to a tool or solution to be uploaded to the Europol Tool Repository, for use by MS LEA's as part of their uptake (and compliance) processes.

2. POLICY STATEMENTS

2.1. Basic Principles

ODIN (PD) is a data processing environment that allows duly authorised staff of Europol to work on projects related to research and innovation as per Article 2 (v) ER.

The outcomes of these projects may not result in uptake by Europol or EU MS, or the results of these projects may not produce the desired results, due to the uncertain nature of research and innovation.

In accordance with Article 33a ER, ODIN (PD) may process operational personal data.

ODIN (PD) is accessible only to authorised users. [redacted]

[redacted]

In accordance with Article 33a (d)(ii) ER, and once the appropriate technical security measures are in place in the target state, specially authorised staff of the competent authorities of the Member States and Union agencies may access the ODIN (PD) data processing environment.

[redacted]

As specified in the ER (Article 33a(2)(d)(i) ER, each R&I project must have its own "separate, isolated and protected data processing environment" distinct from all other projects. Remote access from non-Europol devices or from non-Europol networks is not foreseen.

All standard Europol security requirements remain in place. Auditing will be performed at the server level in line with the auditing policies governing the Operations Network as captured in the Solution Blueprint developed by the ICT Architecture team.[4]

2.2. Intended Use

ODIN (PD) is a tool that forms part of a multi-stage cycle of activities known as the **Innovation Pipeline**.

The cycle has 4 stages:

1. **Stage 0: Opportunity Scanning** – by means of various inflow channels, potential projects are identified, either through the European Clearing Board for Innovation (EuCB), the EU Innovation Hub for Internal Security, the operational needs of the Analysis Projects at Europol, or any number of mechanisms that identify future business needs.
2. **Stage 1: Validation & Pre-Selection** – this stage intends to qualify proposed opportunities or business needs identified in Stage 0 in order to maintain a list of such projects and initiatives that are suitable and feasible for inclusion in ODIN R&I Sandbox. By means of a set of prioritisation criteria, such projects are queued until they can be executed in Stage 2.[5]
3. **Stage 2: Selection & Operational Prototyping with personal data in accordance with Article 33a ER** – work that will be performed in ODIN (PD), for which this document is the Use & Management Policy. This will include development, training, testing and validation of algorithms including operational personal data, and may include the development of additional security controls, performance or security testing, and similar compliance activities.
4. **Stage 3: Uptake** – making the solution available for operational analysis use at either Europol or the Member States/Schengen-associated countries. This can happen either through inclusion in future ICT Work Plans for implementation at Europol or through the upload of the solution to the Europol Tool Repository (or both). Any Uptake at Europol is subject to standard practices, such as DPIA/Prior Notification under Art. 39, adherence to security standards, or potential security accreditation.

[4] See EDOC-#1326716 Solution Blueprint R&I Opsnet
[5] EDOC-#-#1331956 Validation & Pre-Selection of potential R&D projects – Process Description

In this context, projects in ODIN (PD) may lead to projects being abandoned, as the feasibility of the technology cannot be validated, the risk incurred be deemed unacceptable, impacts on fundamental rights be perceived, or performance to the desired level not be achieved. Failure to result in a future production system must not be regarded as a failure of the project itself, for all insight is valuable.

Looking at the specific activities in **Stage 2 of the Innovation Pipeline**, the following policy statements apply:

- Dedicated Administrators have the right to set up a specific data processing space for each R&I project in ODIN (PD) and make available the project assets (see point below). Note: these administrators must be Europol staff and duly authorised to handle operational personal data.
- Dedicated Administrators will load the relevant software code, models and tools, supporting libraries, and any relevant dataset(s) into the specific data processing space for each R&I project in ODIN (PD). Note that under Article 33a ER, the express consent of the data provider is required to use a dataset including operational personal data for R&I purposes (see also process description EDOC-#1160881).
- Validating, benchmarking, prototyping, further developing, enhancing, or otherwise improving tools and models with datasets including operational personal data are permitted uses of ODIN (PD).
- Users have the right to use the software applications or source code, to copy, modify, adapt and otherwise manipulate the modified software applications or source code within the specific data processing space for the project to which they are allocated.
- Users may not sell the software code or any parts thereof or allow any third party to do so. Neither software nor any other product (e.g. manuals) can be commercialised or used by non-law enforcement officers under any circumstances, including if adapted or reverse-engineered.
- Software applications or source code created, updated and otherwise modified in ODIN (PD) is done under the responsibility of the individual user of each specific R&I project.
- Users are liable for the quality and content of their software application or source code. It must not contain any code or intellectual property belonging to a third party unless such third party has provided their explicit written consent to this or the licence of the code allows for it. Europol accepts no liability for a failure of a user to observe this strict user requirement.
- All users allocated to an R&I project have the same access to the contents of the project and it is the responsibility of the Innovation Project Lead to ensure only authorised users are given access to each specific R&I project.
- Inclusion of code in a specific data processing space for an R&I project does not transfer ownership of said code. Users cannot therefore purport to sub-licence or assign code uploaded by other users. In relation to users' own original coding, no future ownership or licensing can take place that would put other users in breach of intellectual property rights in respect of code previously shared in ODIN (PD).
- Users must comply with all applicable laws, rules, regulations, and other provisions by any governmental authority relating to the use of the code or software part. Any liability for breach of national law is the user's responsibility and Europol holds no responsibility in the event of such breach of national legal provisions.
- Users may not introduce malicious software applications or source code, such as malware or viruses, or links to such software applications or source code.

2.3. Creation of a Project

A new R&I Project in ODIN (PD) will be created once one of a number of criteria are identified as being applicable:

1. The output of the project intends to deliver a tangible result. Note that a negative result may also constitute a legitimate outcome of a research & innovation project.
2. The project is relevant to law enforcement.

3. The project does not at face value present unacceptable risks or breach fundamental rights.

A project must be administered by:

- One or more Innovation Project Leads[6] who are staff members working either in the Europol Innovation Lab or the Europol unit that sponsors the project.

Non-Europol staff (e.g. academia, consultants, MS representatives) may not access ODIN (PD) and cannot manage any such R&I projects at Europol. In the event that the R&I project builds upon expertise provided by an external partner (e.g. an academic researcher or a consultant), Europol staff will perform the work and make available the (potentially redacted) results to the external expert. An Innovation Project Lead assumes overall responsibility for each project.

Innovation Project Leads are responsible for:

- Ensuring only authorised Europol project members having access to the respective data space in the data processing environment,
- Providing to the project members the relevant computing and storage assets (in liaison with the Dedicated Administrators),
- Being aware of and communicating the rules of ODIN (PD),
- Checking that the provisions of this Policy are made binding towards users,
- Identifying and verifying any higher risk elements such as code contributions from third parties, open source terms compliance and basic checks on participating legal entities,
- Checking that access rights are terminated when the situation so requires,
- Responding to any regulatory questions (with the help of project experts), and for
- Ensuring that all project personal data is deleted after the project concludes, in accordance with Article 33a(2)(d)(v) ER and that the relevant logs are kept in accordance with Article 33a(2)(e) ER and all current Europol data retention rules.[7]

2.4. Access Control

2.4.1. Introduction

[6] The Innovation Project Lead does not have to be a formal project manager or hold a project management role in their organisational unit. The Innovation Project Lead is the go-to Europol staff contact for their specific research and innovation project.

[7] Note: any R&I project outputs that are made available for Uptake must still go through their own compliance cycles (e.g. Art. 39 ER) as part of the respective Uptake processes.

2.4.2. Categories of users

[redacted]

2.4.3. Conditions for granting access

[redacted]

[redacted]

2.4.4. Acceptance of a new user

[redacted]

2.4.5. Reviewing and terminating user access

[redacted]

2.4.6. Identification and authentication

[redacted]

[redacted]

[redacted]

2.4.7. Password composition and use

[redacted]

2.5. Content management, Data Ownership and Responsibilities

Europol manages ODIN (PD). Information made available therein is therefore subject to Europol's legal framework and the processing of this data must be within Europol's strategic objectives.

2.5.1. Project Data

Each R&I project processing operational personal data may only do so with the express consent of the data provider, who must make it clear that the data may be used for R&I purposes.[9]

Each R&I project will have its specific objectives. Each project shall have a dedicated data space. Upon completion of each project, the personal data relevant to that project must be deleted alongside the project-specific data space. An exception would be made for a project for which data is needed for regulatory reasons, for example to demonstrate AI accuracy.

For those projects where data processing has enriched or expanded the base dataset, the Innovation Project Lead and the Europol Innovation Lab will determine if the new dataset shall replace the original one, if they shall exist in parallel, or if some other form of data storage is appropriate.

Data originating from external sources (for example, commercially acquired synthetic data) shall be subject to all of Europol's standard data security principles, such as AV and malware scanning, at the time of import.

2.5.2. Personal data

ODIN (PD) may store operational personal data in line with the provisions of Article 33a ER and the Europol Operations Network Policy.

2.5.3. Classification level of the information

No classified information may be processed in the ODIN (PD) data processing environment.

2.5.4. Copyright and other Intellectual Property Rights (IPR)

At the start of each R&I project consideration will be given to the need for granting of intellectual property rights. These could come from a variety of sources and in varying formats (e.g. software, datasets, algorithms). A tool may be developed by Europol or a Member State authority and the purpose of the project may be to train such tool using the dataset of another participant or donor (with informed written consent). Alternatively a tool may be the result of an EU funded project involving multiple participants including commercial companies. Appropriate permissions for each use case are needed. These must be granted for the benefit of all participants explicitly (including more than simply Europol staff e.g. SNEs). They need to cover the R&I project actions e.g. modify/establish accuracy/benchmark/ refine/rebalance etc.

[9] See EDOC-#1160881 Support R&I projects processing personal data (Art. 33a ER)_(pr.v.1)

If the project is likely to result in the generation of IPR, it needs to be considered upfront what rights are granted to the results both during and after the end of the project - and to which entities. These considerations are familiar from consortium agreements entered into in the context of EU funded projects. Care must be taken to ensure due diligence as regards rights for tools from private parties (e.g. to investigated embedded open source elements for compatibility with the R&I project) to ensure at least the good faith potential of an enduring benefit for Europol and our law enforcement stakeholders (notwithstanding the "right to fail" referred to at 2.2 above).

Collaboration with commercial entities to modify their intellectual property is not a currently foreseen scenario. However, should a commercial entity make their IP available (for example by providing for free an open-source, cut-down "LE" version of their commercial product), then such modifications should be agreed up-front, for example in a specific contract or by the commercial entity allowing for such modifications in their End User License Agreement (EULA).

Note that such collaboration may not result in Europol "endorsing" either the commercial entity or their product(s).

2.5.5. Unauthorised content

The following types of content are considered inappropriate. The list below is by no means exhaustive, but attempts to provide examples of unacceptable content:

- Unauthorised copies of copyrighted material
- Proprietary material included without consent or without adhering to terms
- Hyperlinks to inappropriate content on other websites (including commercial sales sites)
- Malware or hyperlinks to malware: Users are requested to take all necessary actions to prevent (unwanted) virus or malicious content being uploaded into the ODIN R&I Sandbox. If the R&I project specifically involves malware, all precautions will be taken to ensure no contamination is possible with other data spaces.
- User's credentials to authenticate on other websites or web services.
- Offensive or explicit content or hyperlinks to such content on other web services.

2.5.6. Content management and responsibilities

Data content management within each R&I project's data space is the responsibility of the Innovation Project Lead for that specific R&I project.

2.5.7. Auditing

The auditing is implemented on the underlying infrastructure [redacted] The relevant logging is specified in the Solution Blueprint developed by ICT Architecture, EDOC-#1326716 Solution Blueprint R&I Opsnet.

2.5.8. Common minimum standards for the protection of information

In order to ensure a common minimum standard of protection to information, all users of ODIN (PD) are expected to comply with the following general security measures as defined in the Europol Operations Network Use Policy (EDOC-#739097):

- All workstations and devices used to access ODIN (PD) shall:
    - be secured from unauthorised entry through the use of appropriate technical identification and authentication mechanisms;
    - provide protection from malicious software through the use of regularly updated anti-virus and anti-spyware software;
    - have its operating system regularly updated and patched;
    - have installed a firewall solution to detect and prevent network attacks and maintain system integrity.

- Users will connect to the solution via their corporate devices in accordance with the Europol Operations Network Use Policy (EDOC-#739097).

3. Security

[redacted]

3.1. Unacceptable use

[redacted]

3.2. Breaches of Security

[redacted]

[redacted]

4. POLICY ENFORCEMENT

The responsibility for general supervision of the application of this policy lies with the Europol Innovation Lab.

However, the nature of this policy necessitates every user of ODIN (PD) in the Europol Operations Network assists in its enforcement through the continuous dissemination and promotion of secure ICT use practices. Europol staff with a management role has, in addition, the responsibility of promoting and enforcing the provisions of this policy to the staff under their supervision.

The Europol Data Protection Function may carry out regular audits of ODIN (PD) to ensure compliance with applicable data protection rules. Findings and suggested corrective measures will be shared with the Head of the Europol Innovation Lab and the concerned Innovation Project Lead(s).

Measures to be implemented for security of processing as well as Security Rules outlining accounting and auditing requirements are outlined in the Decision on the mandatory content and retention period of IT-Security Audit Log files[12].

ODIN (PD) is a collaborative environment, which by definition encourages registered users to collaborate on common objectives. User account activation is on condition of user acceptance of the Terms and Conditions of use, which are derived from this Use and Management Policy.

5. REVIEW OF THE POLICY

This policy will be reviewed when there is an organisational or legal change that affects the policy, or when the interim technical state is superseded by the target state solution.

6. ENTRY INTO FORCE

This policy shall be published in the Europol Vademecum and shall enter into force the day after its publication.

Done at The Hague on xx/xx/2024

Signed by

Catherine De Bolle

Executive Director

[12] Decision on the mandatory content and retention period of IT-Security Audit Log files (EDOC#862442).

ANNEX A – REFERENCES

EDOC#	Title
1237223	Amended Europol Regulation
1263057	Europol Regulation – consolidated version
1160881	Support R&I projects processing personal data (Art 33a ER) – Process Description
865874	Europol Security Rules
862442	Decision on the mandatory content and retention period of IT-Security Audit Log files.
739097	Europol Operations Network Use Policy