≋ EUROPOL

Policy

Development and Use of Machine Learning Tools for the Purpose of Supporting Operational Analysis at Europol

PUBLIC
Document made partially accessible to the public on

1 5 OKT. 2024

Table of contents

1. Introduction

The development and use of machine learning tools is considered as a form of application of Artificial Intelligence (AI) entailing a number of risks to the fundamental rights and freedoms of individuals.

Fundamental rights, enshrined in the Charter of Fundamental Rights of the European Union (hereinafter, 'the Charter'), constitute the core values of the European Union. These rights must be respected whenever the EU institutions and bodies design and implement new policies or adopt any new legislative measure. Other fundamental rights norms also play an important role in the EU legal order, in particular the European Convention for the Protection of Human Rights and Freedoms (ECHR).

Mindful of the sensitivity of the use of AI systems by law enforcement agencies, these tools must be designed, built and trained in a manner which fully respects European data protection and human rights standards and follow the ethical guidelines for trustworthy AI. They must implement data privacy-by and security-by design principles and be trained on representative data sets collected and use algorithms in line with European standards and safeguards, and be subject to European oversight.

1.1. Background

Criminal investigations and criminal intelligence operations increasingly include the collection and processing of large and complex datasets by law enforcement authorities.

Some Member States might not have the necessary IT tools, expertise and resources to analyse large and complex datasets, as part of a criminal investigation, and therefore might turn to Europol for support.

Pooling of expertise and capabilities at Union level, when dealing with complex investigations should be generally encouraged and supported subject to checks and balances with regard to personal data processing by the agency. The analysis of large and complex datasets raises a number of challenges to the protection of personal data, related, inter alia, to purpose limitation, data minimisation, data quality, storage limitation and transparency.

High common standards, increased transparency, as well as technological sovereignty and strategic autonomy of the EU in the area of internal security are of key importance in the fight against serious crime and terrorism. The alternative - Europol and the national law enforcement authorities relying on tools and products developed by external vendors, very often situated outside the EU - clearly poses much higher risks, also with regard to the fundamental rights to privacy and data protection. Taking into account that development of new technologies very often involves extensive processing of personal data, e.g. for training of algorithms, the key challenge is how to ensure the strict necessity and proportionality of such processing. Article 4(1)(a)

It also builds on the EDPS opinion on the proposal for amendment of the Europol Regulation published by the Supervisor on 08/03/21 inter alia stating that that there is no inherent and irreconcilable conflict between security and fundamental rights, including the right to data protection. (EDOC#1161141). Furthermore, an EDPS toolkit for the assessment of the necessity of measures that limit the fundamental right to the protection of personal data[1] as well as EDPS

---

[1] Assessing the necessity measures that limit the fundamental right to the protection of personal data: A toolkit, European Data Protection Supervisor (11 April 2017).

guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data have been applied.[2]

1.2. Purpose and Scope

The policy on the development and use of machine learning tools for the purpose of operational analysis serves the purpose of data governance i.e. the management of the entire data lifecycle. Adequate controls and auditing mechanisms are fundamental to ensure that the output produced by an AI system meets the required standards, not just in terms of the primary purpose the system was designed for, but also in relation to wider aspects such as data biases and/or biased algorithms.

It enables the development and use of such tools to effectively and efficiently process large amounts of data received in the fulfilment of Europol's mandate while safeguarding fundamental rights and notably the right to the protection of personal data.

In view of the evolving security threats and exploitation of the digital transformation and new technologies by criminals, the objective of the policy is to support the effective response at EU level, by providing the law enforcement authorities with the necessary tools to counter such threats. Machine learning elements such as natural language processing, data clustering and other functionalities will assist in focusing on the right subset of data.

Examples of the machine learning models are:

Article 4(1)(a)
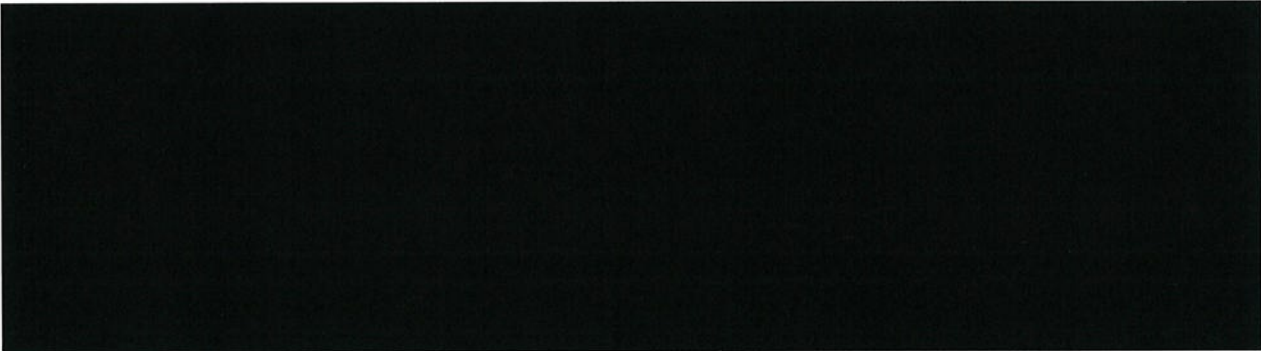
This policy addresses the development and use of machine learning models for the purpose of supporting the operational analysis of datasets provided by Member States and cooperation partners including in the context of specific Joint Investigation Teams (JITs). Article 4(1)(a)

The use of such models in the operational analysis phase ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ falls within the scope of Article 18(2)(c) ER. Regarding the question whether the processing of the operational data included in the datasets for the training, testing and validation of the pre-trained machine learning models can rely on the same legal basis the following should be considered:

Article 2(c) ER defines operational analysis in a broad manner as encompassing all methods and techniques by which information is collected, stored, processed and assessed with the aim of supporting criminal investigations. According to Article 7 of the Integrated Data Management Concept ('IDMC') Guidelines the purpose of operational analysis is to support criminal investigations and criminal intelligence operations through all methods and techniques by which information is collected, stored, processed and assessed.

For the purpose of operational analysis personal data is used specifically to determine operational action against (a group of) individuals in relation to one or more criminal offences, which may include the seizure of goods, the arrest of suspects and the deployment of investigative techniques to collect evidence.

---

[2] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, European Data Protection Supervisor (19 December 2019).

Article 4(1)(a)

███

███

███

Given that the further development, training, testing and validation of machine learning models is a preparatory task to ensure that a given tool (a machine learning model) is suitable for supporting the operational analysis in a given context and for the datasets on which it was trained, Article 18(2)(c) ER is considered as a suitable legal basis.[3]

This policy does not cover predictive policing or automated decision making. Also the development and use of machine learning models beyond the scope of Article 18(2)(c), e.g. in the context of more forward looking research and innovation projects is not covered by this policy.[4]

1.3. References

The following documents shall be read in conjunction with this policy:

. Europol Regulation (ER)

Article 4(1)(a)

. ███████████████████████████████████

. ███████████████████████████████

. ██████████████████████████████

1.4. Owner of the Policy

The policy is owned by the Deputy Executive Director Capabilities of Europol, who shall ensure the update of the policy at regular intervals.

2. Authorised Users

2.1. Policy Statement

The following categories of persons may be permitted to process personal data in the context of the development and use of machine learning tools for the purpose of operational analysis:

. ███████████████████████████████████████

. ███████████████████████████████████████

Article 4(1)(a)

---

[3] Also see chapter 3.4.1 of EDPS Opinion on a prior consultation by Europol regarding thedevelopment and use of machine learning models for operational analysis (Case 2021-0130) (EDOC#1158401).

[4] See in this regard chapter 3.4 of EDPS opinion on the proposal for amendment of the Europol Regulation published by the Supervisor on 08/03/21 (EDOC#1161141).

Data Protection Function and Security (for auditing purposes);

Article 4(1)(a)

Authorisations shall be terminated in case of a severe security breach. Authorisations shall be reviewed whenever a person is assigned to a different post.

2.2. Commentary

Access to personal data in the context of the development and use of machine learning tools for the purpose of operational analysis will be granted after the following conditions have been met:

- The user has a need to process personal data by reason of his/her duties;

- The user has been provided with appropriate training on the development and use of machine learning tools for the purpose of operational analysis;

- The user possesses a sufficient level of security clearance;

- The user has received and accepted this policy. In case of doubt or dispute, the end responsibility for granting access to personal data in the context of the development and use of machine learning tools for the purpose of operational analysis lies with the Europol Security Coordinator. The Security Coordinator has the right to terminate access of any user at any time for security reasons.

3.   Necessity and Proportionality

3.1. Policy Statement

Any use and development of machine learning tools for the purpose of operational analysis shall be necessary and proportionate.

3.2. Commentary

Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal[5].

Proportionality in a broad sense encompasses both the necessity and the appropriateness of a measure, that is, the extent to which there is a logical link between the measure and the (legitimate) objective pursued. Furthermore, for a measure to meet the principle of proportionality as enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to

---

[5] The EDPS checklist for assessing necessity consists of four consecutive steps. Each step corresponds to a set of questions which will facilitate the assessment of necessity.

- **Step 1** is preliminary; it requires **a detailed factual description** of the measure proposed and its purpose, prior to any assessment.

- **Step 2** will help identify whether the proposed measure represents **a limitation** on the rights to the protection of personal data or respect for private life (also called right to privacy), and possibly also with other rights.

- **Step 3** considers the **objective of the measure** against which the necessity of a measure should be assessed;

- **Step 4** provides **guidance on the specific aspects to address** when performing the necessity test, in particular that the measure should be **effective** and **the least intrusive.**

If the assessment of any of the elements detailed in Steps #2 to #4 leads to the conclusion that a measure might not comply with the requirement of necessity, then the measure should either not be proposed, or should be reconsidered in line with the results of the analysis.

Also see pages 6 ff. of EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, European Data Protection Supervisor (19 December 2019).

the exercise of the fundamental rights. This latter element describes proportionality in a narrow sense and constitutes the proportionality test[6]. It should be clearly distinguished from necessity.

Article 4(1)(a)

Compliance with the Europol Regulation also includes compliance with the fundamental data protection principles described in Article 28 ER. The principles of necessity and proportionality are of particular interest when developing machine learning models. In more detail, the development of machine learning models needs to be driven by the proven ability of the model to fulfil a specific and legitimate purpose and not by the availability of the technology.[7]

In assessing necessity, Europol should demonstrate the need for the processing of personal data in order to achieve the purpose, particularly when the data involves structured information related to special categories of personal data (Art. 30.2 ER), different categories of data subjects (Art. 30.1 ER), or for other reasons qualifies as particularly sensitive. This need should be documented including in how far the processing effectively addresses it and why the same purpose cannot reasonably be achieved with other less invasive means.[8] In assessing proportionality, Europol should demonstrate that their purposes could not be accomplished in another reasonable way.

Article 4(1)(a)

These factors, including potential biases in the algorithms and inaccuracy in the datasets could have detrimental effects to data subjects. Hence, in order to further comply with proportionality, Europol should weigh the interest in using AI against the risks it may pose to the rights and freedoms of individuals.[10]

---

[6] The EDPS checklist for assessing proportionality consists of four consecutive steps. Each step corresponds to a set of questions which will facilitate the assessment of proportionality.

- **Step 1**: assess **the importance ('legitimacy') of the objective** (identified under step 3 of the Necessity Toolkit) and **whether and to what extent** the proposed measure would meet this objective and addresses the issue identified in the problem definition ("**genuinely** meets") [this would be 'the advantage/benefit'].

- **Step 2**: assess **the scope, the extent and the intensity** of the interference (identified under step 2 of the Necessity Toolkit) in terms of **impact** on the fundamental rights to privacy and data protection [this would be 'the disadvantage/cost'].

- **Step 3**: proceed to the **fair balance (*advantage/disadvantage; benefit/cost*) evaluation** of the measure.

- **Step 4**: **take a decision ('go/no go') on the measure**. If the result is 'no go', taking into account all factors which determined the evaluation as disproportionate, identify and introduce (if possible) safeguards which could make the measure proportionate.

[7] Information Commissioner's Office, Guidance on AI and data protection, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/

[8] EDPS Opinion on a prior consultation by Europol regarding the development and use of machine learning models for operational analysis (Case 2021-0130), p. 12.

[10] Guidance in AI and Data Protection (ICO), https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-artificial-intelligence-and-data-protection/, accessed on 19/05/21.

4.   Data Minimisation

4.1. Policy Statement

Any use and development of machine learning tools for the purpose of operational analysis shall respect the data minimisation principle.

4.2. Commentary

Another assessment that should be carried out concerns compliance with the data minimisation principle laid down in Article 28(1)(c) of the Europol Regulation. Europol should thus demonstrate that the personal data it processes is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

When working with structured data, one data minimisation technique to be considered is pseudonymisation, i.e. the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation is specifically mentioned as a possible measure to ensure respect for the principle of data minimisation in derogations for scientific and historical research , see Art. 89 GDPR. The following GDPR recitals further specify the concept of pseudonymisation:

.   Pseudonymous data is still personal data - it is not anonymous. (Rec. 26).
    Pseudonymisation is a data risk reduction measure (Rec. 28).
.   Technical and organisational measures must ensure that the additional information necessary for re-identification is kept separately within the same controller and that the authorised persons are indicated (Rec. 29)
.   Personal data should be pseudonymised as soon as possible (Art. 89 and 25, Rec. 78).

The application of pseudonymisation can reduce the privacy risks to the data subjects concerned, and thus help the data controller to demonstrate compliance. For instance, the identity (or identifying details) of data subjects in an operational data set would ultimately be needed for the operational analysis. However, in some cases and with simple models, not all personal details would necessarily be required for the preceding training of the machine learning algorithm.
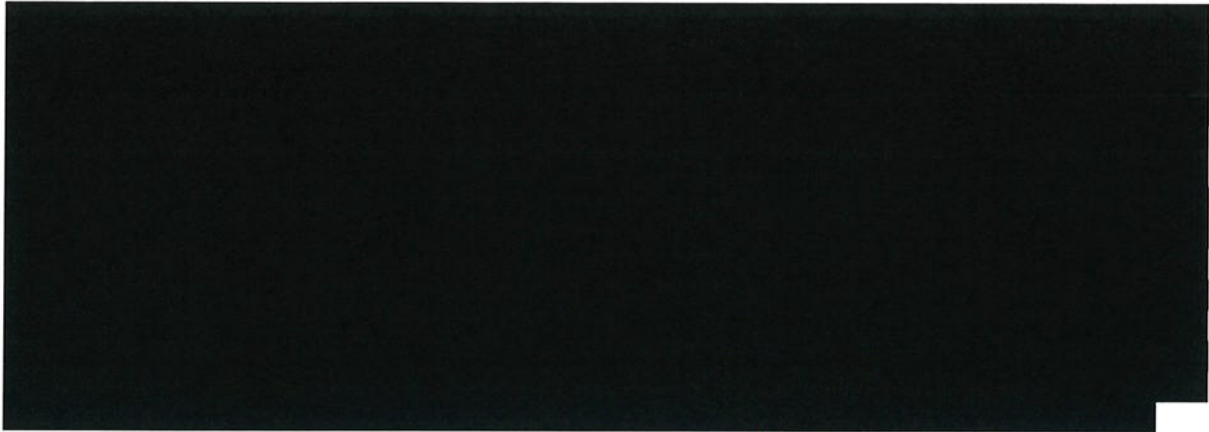
Article 4(1)(a)

Article 4(1)(a)

5. Data Bias

5.1. Policy Statement

Europol shall implement appropriate measures in order to prevent forms of data bias that could have detriment effects on individuals, in particular, if the processing operation involves the processing of special categories of personal data and/or different categories of data subjects as defined in Article 30(1) and (2) ER.

Europol shall verify that the training data used do not reflect discrimination and, should this be the case, replace it with a different set of data whenever possible. Any identified data bias that could produce detriment effects on data subjects needs to be removed or limited in the data used to further train the relevant models. Whenever it is not possible to minimize the bias on the data or the models to an acceptable level, or even to measure it, it should be decided whether the models are still fit for use, including a caveat.

Europol shall ensure regular monitoring of the models regarding biases and their readjustment or retraining.

5.2. Commentary

If machine learning models learn from data, where the training data is unbalanced or reflects discrimination, they may produce outputs which have discriminatory effects on people based on their particular characteristics. The documentation should elaborate how Europol would avoid transferring possible biases included in their own data, whether pre-trained models are going to be used 'as is', whether their accuracy rates are valid for different categories of data subjects, e.g. for different ethnicities or different ages, whenever possible.

The EDPS has acknowledged the use of pre-trained models that were not exclusively trained on law enforcement data as an important element that addresses risks related to bias within law enforcement information[11].

6. Data Accuracy

6.1. Policy Statement

Europol shall implement appropriate measures in order to ensure a high level of data accuracy. In particular, Europol shall ensure that the training data and validation data is statistically sound. For pre-trained models, it needs to be analysed and determined if the input data of the pre-trained models will accurately reflect the operational data ultimately used. Where this is not

---

[11] See European Data Protection Supervisor (EDPS) opinion dated 05/03/21 on a prior consultation by Europol regarding the development and use of machine learning models for operational analysis (Case 2021-0130) (EDOC#1158401), page 14.

possible, transfer-learning and fine-tuning techniques shall be deployed in order to adapt the models respectively.

The validation of data and test data shall be performed keeping in mind the data minimisation principle and the need to have representative data sets.

The output data shall regularly be reviewed in order to detect and correct errors without undue delay to prevent further propagation in Europol's systems.

6.2. Commentary

It is crucial to ensure that the training data reflects the data that ultimately will be processed by the model. This is due to the fact that if the training data does not statistically reflect the operational data, the model will suffer from sample bias (sometimes called selection bias).

Accuracy requirements can differ depending on the underlying business case. An example would be a machine learning model with the aim to find images depicting torture in very large datasets. Those images might be very rare so that the machine learning accuracy rate might be comparatively low. However, even such a low accuracy might be very much appreciated by the operational business.

Even though that not all entries in the training data will be accurate, errors in the output data need to receive the necessary attention since errors in the model's output, whatever their source, if left unchecked, might be detected very late in the operational processes, which will lead to a rapidly increasing number of propagation errors which ultimately will lead to poor data quality.

7.   Human Intervention

7.1. Policy Statement

Any output produced by the development and use of machine learning tools shall undergo human validation before being included into any operational analysis or other reports in the fulfilment of Europol's mandate.

In case the automated results produced by machine learning tools are assessed as false positive or false negative, the human intervention shall provide feedback for the retraining of the machine learning models. This feedback shall be recorded by Europol.

7.2. Commentary

Article 30(4) of the Europol Regulation does not allow for decisions of competent authorities that produce adverse legal effects for the data subjects to be based solely on automated processing of sensitive data.

The processing of personal data in the context of the development and use of machine learning tools at Europol involves systematic human intervention, evaluation and validation by Europol expert staff of the Operations Directorate on the relevance of the output. Human validation is an inherent step of the process. It verifies that the assessment of the source information corresponds to the search result, so as to ensure that the output of the system is faultless.

Therefore, no automatic decision-making will take place based on the results of using the tools, and every result delivered by the machine learning toolbox will be verified by the operational experts.

Human intervention is also guaranteed before the use of the machine learning models when training, testing and validating them. Once the machine learning models have been selected and adapted by the members of the Capabilities Department, their results are manually reviewed by selected members of the Operations Directorate who provide qualitative feedback and manual annotations that can be used for further fine tuning the models to achieve better performance.

8. Data Retention

8.1. Policy Statement

Personal data shall only be processed as long as it is necessary for the development and use of machine learning tools for the purpose of operational analysis.

8.2. Commentary

The machine learning model training sets of data containing all the manually annotated data items will be kept only as long as it is necessary for modifying and improving the algorithm. In this respect, the retention of the training data sets shall be justified and adequately recorded by Europol and reviewed before expiration of three years. After expiration, training data should be archived until prosecution has been completed, as a court may require legal access to or information about the training data to determine the validity of the analytical approach in court proceedings.

Also the retention of personal data in the context of operational analysis will be implemented in accordance with all rules further implementing Article 31 ER.

9. Data Security

9.1. Policy Statement

Europol shall take all the necessary and appropriate technical and organisational security measures to protect personal data against accidental or unlawful destructions, accidental loss or unauthorized disclosure, alteration and access or any other form of unauthorized processing.

This includes but is not limited to conducting a security risk assessment for the machine learning environment and the tools as well as the boundaries/interfaces of the machine learning models to ensure confidentiality, availability and integrity of the processing of personal data in the context of the development and use of machine learning models for the purpose of operational analysis.

Europol shall ensure that all software components of the tools and systems are at their latest security patch, periodic access list reviews are implemented, logs are regularly reviewed as necessary.
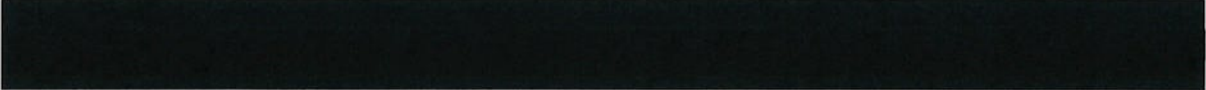
9.2. Commentary

Article 32 of the Europol Regulation requires Europol to take all the necessary and appropriate technical and organisational security measures to protect personal data against accidental or unlawful destructions, accidental loss or unauthorized disclosure, alteration and access or any other form of unauthorized processing. Article 4(1)(a)

The machine learning environment at Europol requires "accountability on security", meaning that a security framework is applied and that rules on data management, data governance and risk management are clearly defined. Europol is aware that the use of various new tools and frameworks, the involvement of new people (stakeholder groups) and the development of new systems or combinations of systems requires a thorough analysis of the data flows and of the security risks.

Article 4(1)(a)

Article 4(1)(a)

The use of new technologies in Europol's technical environment are deployed with measures that ensure the prevention and early detection of any personal data breach. Europol ensures that in case of a personal data breach the EDPS as well as the competent authorities of the Member States concerned as well as the provider of the personal data are notified according to Article 34 of the Europol Regulation. A security incident response plan will be immediately activated in case of a security incident in the machine learning environment.

Europol ensures that all stakeholders have a complete understanding of security and privacy. Data protection by design and by default, data classification, data protection techniques, secure methods of authentication, privacy principles, are elements that are and have to continuously be well defined in the organization.

Europol shall ensure that all stakeholders have, based on their function and role, the appropriate training and knowledge of security and privacy.

Article 4(1)(a)

A thorough monitoring and security hygiene of the machine learning toolbox environment will be ensured.

10. Auditing

10.1. Policy statement

Any access to personal data in the context of the development and use of machine learning tools for the purpose of operational analysis shall be traceable and logged for auditing purposes.

It is the responsibility of the Capabilities Department to ensure that the development and use of machine learning tools for the purpose of operational analysis are set up to comply with this requirement.

The log files shall be stored in a protected environment accessible only to officials specifically nominated for this purpose in their role as Security and Data Protection Function staff.

All actions performed by auditors shall be logged in order to allow 'auditing the auditors'.

10.2. Commentary

In order to comply with the data protection and information assurance regime at Europol all processing operations upon personal data in the context of the development and use of machine learning tools for the purpose of operational analysis must be logged.

Whenever technically possible, the log files must be sent to the Unified Auditing Solution (UAS) enabling auditors to establish which data have been used for training, validation and operational

analysis. The UAS should also be capable of tracing the propagation of data coming from the machine learning models in the operational databases.

In cases in which log files cannot be sent to the UAS, the log files must be kept locally and must be made accessible for auditing purposes.

Article 4(1)(a)

11. Unacceptable Use

The following activities shall constitute an unacceptable use of machine learning tools. The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unauthorised development and use of machine learning tools:

- Any violation of the principles related to the development and use of machine learning tools as specified in this policy.
- Support of information collection outside of Europol's mandate.
- Deliberately introducing data bias.
- Any development or use of machine learning tools with the aim to produce discriminatory effects on people.
- Any development or use of machine learning tools for personal purposes.

12. Review of the Policy

This policy shall be reviewed every time there is an organisational or legal change that affects this policy, or earlier if requested by one of the parties involved in the process.

13. 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 11/06/21

Signed by

Article 4(1)(b)