eucrim 2024 / 4
European Law Forum: Prevention • Investigation • Prosecution

25th Anniversary of the European Anti-Fraud Office
Le 25e anniversaire de l'Office Européen de Lutte Antifraude
25 Jahre Europäisches Amt für Betrugsbekämpfung

eucrim also serves as a platform for the Associations for European Criminal Law and the Protection of Financial Interests of the EU – a network of academics and practitioners. The aim of this cooperation is to develop a European criminal law which both respects civil liberties and at the same time protects European citizens and the European institutions effectively. More information about the Associations is available at https://eucrim.eu/associations/.

Contents

News

European Union

Council of Europe

Articles

25th Anniversary of the European Anti-Fraud Office

Guest Editorial

Dear Readers of this Jubilee Issue on OLAF,

In 2024, the European Anti-Fraud Office – OLAF – was celebrating its 25th anniversary. This occasion fills me with joy, pride, and gratitude, as the Office has proven to be a great success in the fight against fraud affecting the financial interests of the EU over the last quarter of the century.

OLAF took over operations from the first European anti-fraud entity – UCLAF – in 1999 (UCLAF had been created in 1987 as part of the Secretariat-General of the European Commission). Since then, we have come a long way. While still part of the European Commission, OLAF is fully independent in the conduct of its investigative mandate.

OLAF investigators have uncovered around €16 billion that would otherwise have been lost to irregularities or fraud: for every euro that OLAF's operations cost, we tracked down at least €10 to be recovered to the EU's budget. In total, OLAF has closed over 6000 investigations with recommendations for further action that range from recovering money or improving administrative checks to launching criminal proceedings or initiating disciplinary procedures.

Over the years, OLAF has undergone organisational changes to adapt to new challenges and become more efficient in the fight against fraud. In 2021, the revision of Regulation (EU, Euratom) No 883/2013, the centrepiece of OLAF's legal framework, brought important improvements, e.g., the possibility for OLAF to access bank account information. Close cooperation with the European Public Prosecutor's Office (EPPO), which took up its operations in 2021, was also established. Since then, the EPPO and OLAF work hand in hand to protect EU taxpayer's money. Both bodies ensure that we use all available means, administrative and prosecutorial, to protect the EU budget from fraud.

Regulation 883/2013 is currently being evaluated with a particular focus on OLAF-EPPO cooperation. The results of this evaluation will help OLAF become even more efficient in the future.

By adapting to the changing context in which the Office operates in today's complex, digitalised, and globalised world, we are going to build, not rest, on our work in the last 25 years. Enhanced investigations through data analysis and artificial intelligence will play a key role in addressing this new context, e.g., new digital tools are being deployed in our Anti-Fraud Knowledge Centre. OLAF has also established a large network of international partners and become an important actor in the fight against cross-border fraud. 25 years ago, fraudsters did not have to worry too much about cross-border investigations. This has changed considerably.

Ville Itälä

Environmental crime has also become increasingly relevant across the EU, as fraudsters run relatively low risks for high profits. To counter this growing concern, OLAF participates in coordination cases with the Member States and other key partners such as Interpol, Europol, and Eurojust. So far, OLAF has participated in numerous actions, e.g., against illegal wildlife trade, illegal trade of refrigerant gases, food fraud, and illegal waste shipments. The new Waste Shipment Regulation will reinforce OLAF's mandate in this area.

OLAF's success story over the past 25 years would not have been possible without our partners in the EU institutions and bodies, Member States, international organisations, candidate countries, non-EU countries, financial institutions, and other stakeholders, including the Office's highly committed staff. I would also like to thank all actors in civil society and academia who have taken a keen interest in OLAF, in the EPPO, and in developing the European dimension of criminal law and law enforcement, enriching our work with their insights.

With the valuable support and engagement of all stakeholders, we will relentlessly continue to tackle new challenges and optimise our operations for the benefit of European citizens and enterprises. OLAF's success story is sure to continue.

Ville Itälä
Director-General, European Anti-Fraud Office (OLAF)

News

Actualités / Kurzmeldungen

European Union

Reported by Thomas Wahl (TW), Cornelia Riehle (CR), Dr. Anna Pingen (AP)

Foundations

Rule of Law

Hungary: Rule-of-Law Developments in the Second Half of 2024

This news item continues eucrim's overview of worrying rule-of-law developments in Hungary as far as implications on Union law, in particular the protection of the EU's financial interests, are concerned. It covers the period from 1 July to 31 December 2024. It follows up on the overview in eucrim 1/2024, 5–7 which covered developments in the first half of 2024.

■ 4 July 2024: Civil society members of Monitoring Committees jointly request to convene extraordinary sessions of Monitoring Committees following the Sovereignty Protection Office's (SPO) investigation against Transparency International Hungary Foundation and the investigative news portal atlatszo.hu. The investigations were opened on 25 June 2024 (→eucrim 1/2024, 6–7) on the basis of the "Protection of National Sovereignty Act" of December 2023 (→eucrim 4/2023, 311). The SPO blames the two civil society organisations as "foreign-funded organisations" that "may harm or undermine Hungary's sovereignty", which can result in criminal liability. The civil society members of the Monitoring Committees state that SPO's investigations are unacceptable and an attempt to exert intimidate pressure to all committee members. The Monitoring Committees ensure that Hungary's share of EU funding is spent in accordance with the relevant rules and the approved plans and are therefore an important pillar to protect the EU's financial interests in Hungary.

■ 9 July 2024: A summary of the results of a survey is published in which civil society organisations responded to threats posed by the recently enacted "Protection of National Sovereignty Act" (see above) for civil society organisations in Hungary. The interview partners also assessed how the Act affects their activities, strategies and funding. In conclusion, the replies show that the Act imposes significant burdens on civil society organisations and actively impedes their activities. According to the results of the survey, the chilling effect of the law creates fear and self-regulation, hinders cooperation between organisations, and diverts resources away from the actual activities of the organisations. In these circumstances even EU funding can be perceived as a threat.

■ 23 July 2024: The Deputy State Secretary rejects the request of the civil society members of Monitoring Committees of 4 July to convene an extraordinary session due to the SPO's investigations into the Hungarian branch of Transparency International and news portal atlatszo.hu. It is argued that the letter cannot be considered as a formal request to convene an extraordinary meeting of the Monitoring Committee.

■ 19 September 2024: Following the application no 60778/19, *M.D. and Others v Hungary*, the ECtHR ruled for the seventh time that the Hungarian practice of push-backs of immigrants violated the ECHR. Since 2021, the ECtHR has repeatedly ruled that push-backs to Serbia by Hungarian police, often by force and deception, are, in all cases, a violation of human rights, particularly the prohibition of collective expulsion (Art. 4 of Protocol No. 4 of the ECHR). The case at issue concerned an Afghan family of six who were made to cross the border from Hungary to Serbia against their will and without any formal order. The ECtHR awards the family €9000 in compensation. *Gruša Matevžič*, Senior Legal Officer of the Hungarian Helsinki Committee, which

* Unless stated otherwise, the news items in the following sections cover the period 16 November 2024 – 15 Januar 2025. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

represented the Afghan complainants before the ECtHR, said: "Even though both the Strasbourg Court and the Court of Justice of the European Union condemned this practice of forcible returns, it still continues to this day." In a post on Verfassungblog.de on 7 October 2024, *Dana Schmalz*, Senior Research Fellow at the Max Planck Institute for Comparative Public Law and International Law, commented on the ruling as follows: "The facts of the case reveal a long list of rule-of-law issues. The judgment further clarifies the scope of protection of Article 4 of the Fourth Protocol. At the same time, it shows how the ECtHR – quietly and without much public reaction – is standing up to the complete undermining of legal standards in asylum and migration law" [translation from German into English by the author with the support of DEEPL].

■ 24 September 2024: The Council of Europe Committee of Ministers issues an interim resolution which blames Hungary for not having remedied violations of the prohibition of torture and inhuman or degrading treatment in relation to its law and practice of life sentences. The Committee of Minister scrutinized the *László Magyar* group of cases which partly date back to 2014. It expresses deep regret about the continued absence of information on any developments to comply with ECtHR case law requiring that the applicants' life sentences can be regarded as reducible, so that they are provided with a prospect of release and a possibility of review, both of which must exist from the imposition of the sentence. The interim resolution calls on the Hungarian authorities to submit an updated action plan, including information on all outstanding issues, by 15 March 2025 at the latest.

■ 3 October 2024: The European Commission decides to refer Hungary to the Court of Justice because it considers its national law on the "Protection of National Sovereignty" (see above) to be in breach of EU law. The Commission opened infringements proceedings in this matter against Hungary on 7 February 2024 (→eucrim 1/2024, 5). After having carefully assessed the reply of the Hungarian authorities, the Commission maintains that most of the grievances identified have still not been addressed. The Commission considers that the law infringes several fundamental rights enshrined in the Charter as well as several fundamental freedoms of the internal market, the e-Commerce Directive, the Services Directive, as well as EU Data protection legislation.

■ 12 November 2024: Ahead of the General Affairs Council meeting which plans to deal with the Article 7 procedure against Hungary, the Hungarian Helsinki Committee (HHC) publishes a paper in which selected rule of law and human rights issues are presented that demonstrate Hungary's fundamental disregard for EU values and EU law as well as the diminished level of domestic human rights protection in the country. The HHC also proposes points of inquiry and recommendations. The issues relate to the following: shrinking civic space and the Sovereignty Protection Act; non-execution of European court judgments; the possibility of Hungary's top court to block the binding effect of CJEU judgments; perpetuated states of exception; and lack of an effective domestic human rights protection system.

■ 15 November 2024: The Hungarian Constitutional Court rejects a constitutional complaint brought by Transparency International (TI) Hungary against the "Protection of National Sovereignty" Act (→eucrim 4/2023, 311). The constitutional complaint was supported by 31 other NGOs which participated as amicus curiae. TI argued that the Act allows for a blatantly retaliatory and stigmatising procedure. In particular, the powers of the Sovereignty Protection Office (SPO) to launch procedures against a foreign-funded NGO if the SPO deems that the outcome of an election could be influenced, was considered too broad and unlawful. In rejecting the complaint, the Hungarian Constitutional Court mainly argues that the law did not give the SPO the power to apply any legal consequences, so the sections in question were not connected to the right to the freedom of expression. Moreover, since the reports of the SPO do not constitute either a public authority decision or any other administrative decision, there is no need to provide for a right to appeal against them. While the SPO welcomed the judgment, TI and other NGOs announced that they will have the law reviewed by the ECtHR.

■ 19 November 2024: The General Affairs Council revisits the Article 7 procedure against Hungary for disregarding EU values. However, once more no significant progress is made. It is reported that the Commission provided ministers with an update on the latest developments in Hungary and ministers had an opportunity to provide their comments. Hungary presented its remarks. The Article 7 procedure concerning Hungary was launched by the European Parliament in 2018 due to the erosion of EU values and disregard of EU law by the *Orbán* government. Article 7 TEU allows EU membership rights to be suspended if the European Council decided that a country seriously and persistently breaches the principles on which the EU is founded.

■ 22 November 2024: Representatives of the three highest judicial administration bodies, the Kúria President, the President of the National Office for the Judiciary (NOJ) and the President of the National Judicial Council (NJC), signed an "Agreement" with the Hungarian government, represented by the Ministry of Justice. According to this "Agreement", judicial leaders approved cooperation with the Ministry of Justice in the adoption of undefined overall struc-

tural judicial reforms in exchange for unguaranteed promises regarding a long-overdue salary raise.

■ 27 November 2024: A group of civil society organisations presents a detailed assessment of Hungary's compliance with rule-of-law conditions to access EU funds. The assessment relates to (1) Hungary's commitments under the "conditionality mechanism", (2) the "super milestones" that the country must fulfil in order to receive any payment from the EU's Recovery and Resilience Facility (RRF), and (3) the horizontal enabling condition "Effective application and implementation of the Charter of Fundamental Rights" under the Common Provisions Regulation that would pave the way for EU programme funding (for the mechanisms → article by *I. Jaskolska*, eucrim 4/2023, 337–339). The civil society organisations conclude that the Hungarian government had not taken adequate measures in order to fully address the rule of law and human rights concerns raised, and it had not complied with significant conditions established by EU institutions. The assessment is designed to feed the upcoming re-assessment by the Commission and the Council in the framework of the conditionality mechanism in December 2024.

■ 3 December 2024: Judges and other employees of the judiciary are up in arms against the "Agreement" of 22 November 2024 (see above). The websites of the two major Hungarian judges' associations have published a wealth of protest letters, some of them sharply worded. The number of protests is growing daily. They are directed against both the content of the agreement and the circumstances under which it was signed. Protesters criticise that the Hungarian government put undue pressure on judicial leaders who opted for giving up guarantees of judicial independence in a political bargain that might yield to salary raises.

■ 6 December 2024: Calling the "Agreement" of 22 November 2024 (see above) a "Black Friday at Hungarian Courts", the Hungarian Helsinki Committee analyses the "Agreement", its antecedents, and the unprecedented public protest by Hungarian judges and judicial staff under four angles: (1) how the government exerted financial pressure on the judiciary, pushing it to the brink of inoperability; (2) how this was converted into political pressure on the National Judicial Council; (3) why the concluded "agreement" violates judicial independence and undermines the system of checks and balances; (4) how the undetailed, undefined reforms highlighted in the "agreement" can undermine judicial independence.

■ 11 December 2024: By explaining two cases, the Hungarian Helsinki Committee (HHC) illustrates how pressure is put on judges/judicial staff through administrative means at the *Kúria* – the highest judicial authority in Hungary. The persons concerned have spoken out in defence of the separation of powers, judicial independence, and incompatibility of Hungarian law with EU law. The HHC emphasised that breaches of the freedom of expression of judges have been a long-standing problem in Hungary and the issue is persistent.

■ 16 December 2024: The European Commission decides that it will further block the release of EU funds to Hungary. Using the conditionality mechanism, the Commission declares that it does not accept the specific legislative amendments regarding public interest trusts and entities maintained by them, which were formally notified by Hungary on 2 December 2024. This means that Hungary will lose around €1 billion. Shortcomings in public interest trusts are one area in which the Commission sees a linkage between rule-of-law deficits in Hungary and the protection of the EU's financial interests, so that Regulation 2020/2092 on a general regime of conditionality for the protection of the Union budget applies (→eucrim 3/2020, 174–176). The Commission also clarified that the other Council measure suspending part of cohesion funds also remains in place, as Hungary did not notify any remedy to address the related rule-of-law concerns. Measures to protect the Union budget from breaches of the principles of the rule of law in Hungary were set by the Council in December 2022 (→eucrim 4/2022, 240).

■ 19 December 2024: In the case *M.D.A. and Others v Hungary* (application no. 16217/19), the ECtHR finds that Hungary violated Article 3 (inhuman or degrading treatment) and Article 5 §§1 and 4 (right to liberty and security) ECHR for the treatment and detention of an Afghan family (four children and two adults) in the *Röszke* transit zone located between Hungary and Serbia. The family was held there for four months and Hungarian authorities, *inter alia*, tried to force them to return to Serbia "voluntarily" by withholding food from the parents. The ECtHR particularly rejected Hungary's argument that transit zones are not places of detention. In its reasoning, the ECtHR refers to a similar case decided in March 2021 (*R.R. and Others v Hungary*, application no. 36037/17). The ECtHR also holds that Hungary has to pay the family €10,000 in respect of non-pecuniary damage. (TW)

Poland: Rule-of-Law Developments in the Second Half of 2024

After the previous PiS government had been replaced by the new Polish government under the leadership of Donald Tusk at the end of 2023, the reappraisal and reversal of judicial reforms in Poland that jeopardised the rule of law has started (→previous overview in eucrim 1/2024, 3–5). At the end of May 2024, the Commission also offered its support in further rein-

stating the rule of law in Poland when the Commission decided to close the Article 7 procedure against the country (→eucrim 1/2024, 5).

Above all, the new government needs to establish a legislative framework for addressing the status of "neo-judges" who were appointed by the former PiS government through contested procedures and revert specific mechanism introduced against rule-of-law defenders. The latter mainly includes the Extraordinary Complaint Mechanism, which allowed the Prosecutor General (who is at the same time the Minister of Justice) to lodge an appeal in order to reverse final judgments, and the Disciplinary Chamber and the Chamber of Professional Responsibility of the Supreme Court. Both mechanisms were declared unlawful by the European Courts, thus reforms are also needed to implement CJEU and ECtHR judgements. The latest developments in rolling back the reforms of the justice system by the former PiS government include:

- In mid-November 2024, the Codification Committee of Civil Law published a special resolution in which it called for changes in the Polish Supreme Court. The Committee has been particularly concerned about the leadership of neo-judges in the Supreme Court presiding over most chambers and now constituting a majority within the Court. One possible outcome would be the abolition of the Supreme Court chambers whose illegality has been confirmed by both the CJEU and the ECtHR. According to the Committee, the extraordinary complaint mechanism should also be abolished, because it was misused as a political tool by the former PiS government and constitutes an unjustified exception to the concept of the finality of judgments. Lastly, the Committee advocated the abolition of the Chamber of Professional Responsibility of the Supreme Court – the successor of the former Disciplinary Chamber – since it lacks justification.
- On 21 November 2024, Polish Minister of Justice, *Adam Bodnar*, tabled "10 pillars" for judicial reforms. These reforms are intended to be carried out without legislative amendments and are designed to make the work of the Polish courts more efficient and effective within the next two years. Reforms that require legislative amendments, such as those concerning the National Council of the Judiciary (KRS), the Supreme Court, and the status of neo-judges, are to be postponed until the election of a new Polish president in 2025. In anticipation of a change in the presidency, the "10-pillar plan" is intended to make progress without the expected oppositional stance of the incumbent President *Andrzej Duda*.
- At the end of November 2024, it was announced that a Polish parliamentary committee of enquiry now intends to take tougher action against former Justice Minister *Zbigniew Ziobro*, who was in office under the PiS government. He has been refusing to testify in the Pegasus case. The inquiry into this case deals with the purchase and use of the Pegasus surveillance software by the PiS government, which allegedly spied on members of the opposition at the time. (TW)

Area of Freedom, Security and Justice

New Five-Year Programme on Future Priorities in the Fields of Justice and Home Affairs

spot light

At their meeting on 12 December 2024, the EU Member States' Minsters responsible for home and justice affairs approved a new strategic agenda that shapes the future direction of EU policy in the area of freedom, security and justice (AFSJ). According to the titled "strategic guidelines for legislative and operational planning within the area of freedom, security and justice", the EU institutions are called on to put the set priorities into action during the next legislative cycle in accordance with the Treaties.

In total, the document sets out 39 guidelines. It underlines the importance of the free movement of persons and recalls that internal border controls within the Schengen area remain a temporary measure of last resort, while at the same time there is a need for external border controls and Member State cooperation on security and migration. In the field of justice, the document emphasises that judicial cooperation is a key objective of the AFSJ, based on the cornerstone of the mutual recognition of judgments and judicial decisions between Member States. The guidelines also "commit to the joint effort in upholding the rule of law within the EU by all available tools in accordance with the Treaties". An important element will be specific thematic discussions on rule-of-law related issues within the Justice Affairs Council.

Other important guidelines include the following:

- Efforts should now mainly focus on the coherent and effective implementation of adopted legislation and policy measures already in place;
- The upcoming Multiannual Financial Framework must be aligned with the implementation and future obligations of the Member States in the AFSJ;
- A fully interoperable IT architecture remains one of the major priorities fostering mutual exchange of information in the area of justice and home affairs;
- The preventive approach on irregular migration should be strengthened, *inter alia* by developing "ambitious and durable comprehensive partnerships" with countries of origin and transit;
- The EU's legal framework to address new types of threats, such as instrumentalization of migrants and

hostile actors at the EU's external borders is to be strengthened;
- A more assertive and comprehensive approach to returns of persons who have no right to stay in the bloc will be developed and implemented;
- With regard to the fight against serious and organised crime, society should be made more resilient to organised crime by promoting public private partnerships, the administrative approach of prevention (e.g. prevention of the infiltration of the legal economy), and the use of AI for law enforcement;
- Crime prevention strategies and tools, such as the European Crime Prevention Network (EUCPN) and the European Network on the Administrative Approach (ENAA) should form an integral part of the EU's efforts in the fight against crime;
- Special attention should be given to the fight against corruption and the promotion of integrity as part of an overall EU approach, encompassing actions ranging from prevention and analysis to repression of corruption;
- Given that criminal organisations operate far beyond the EU, it is essential to further improve law enforcement and judicial cooperation with third countries at the level of the EU and of the Member States;
- The work of the High-level Group (HLG) on access to data for effective law enforcement and its recommendations (→eucrim news below, pp. 270–271) should be the basis for the political and practical future direction for the European vision of effective access to data for law enforcement purposes and the Commission should draft a respective roadmap for the implementation of the recommendations;
- A new counter-terrorism agenda addressing new and persisting challenges will be developed, with special attention to the victims of terrorism;
- The EU will continue to make progress in the use of AI in justice systems in order to facilitate and improve access to justice – at the same time, AI must be developed and used in a manner that is inclusive, sustainable, privacy-respecting and human-centred;
- EU institutions should engage in a reflection on all aspects of EU criminal and civil law in order to ensure consistency and focus on the implementation of the existing *acquis*;
- In the area of EU criminal law, priorities will be:
  - Further strengthening the judicial response to organised and particularly serious crime, including the fight against corruption;
  - Combating hate crimes and hate speech;
  - Supporting and protecting victims of crime;
  - Furthering work on data retention;
  - Improving the effectiveness of mutual recognition instruments, including the European Investigation Order and those on freezing and confiscation orders;
- The Member States and the Commission will remain committed to the European Judicial Network in Criminal Matters as well as other relevant networks aimed at deepening judicial cooperation, and will further analyse how to make the best use of these networks;
- The EU should continue its efforts to deepen judicial cooperation with third countries in both civil and criminal matters in order to ensure a coherent external dimension of the AFSJ;
- With regard to Russia's war of aggression against Ukraine, the EU will remain committed to supporting coordination and cooperation between all competent authorities at international and national levels with a view to holding fully accountable those responsible for the most serious international crimes through successful investigations and prosecutions of these crimes.
- The feasibility of potential new tasks of the EU agencies in the area of Justice and Home Affairs should be assessed while any future revision of their mandates should fully adhere to the supportive role assigned to the agencies;
- The European Public Prosecutor's Office, as an independent body of the EU, needs to be fully operational and effective to protect the EU's financial interests, in accordance with the Treaties.

Ultimately, with a view to the legislative process, the Council stresses that potential future initiatives implementing the guidelines must pay particular attention to coherence and consistency and be evidence based. The latter must be ensured by meaningful impact assessments, demonstrating the added value of an initiative/legislative proposal and taking into account subsidiarity, proportionality and impacts on the different legal systems and traditions of the Member States and also financial implications at the national level. The principle that national security remains the sole responsibility of each Member State is to be explicitly taken into account. (TW)

Schengen

Bulgaria and Romania Fully Join Schengen

Following a decision by the Council on 12 December 2024, Bulgaria and Romania fully joined the Schengen area as of 1 January 2025. Internal land border controls with Bulgaria and Romania are lifted. As of 1 January 2025, citizens enjoy unrestricted land travel between Bulgaria, Romania, and other Schengen countries.

As of 31 March 2024, the controls at the internal air and sea borders were lifted and the Schengen rules started to apply, which paved the way for the seamless operation of visa procedures and border controls (→eucrim 4/2023, 312).

The EU Commission praised Bulgaria and Romania for meeting all nec-

essary requirements for the compete integration of the two nations into the Schengen area. Both countries have played a vital role in addressing EU border security and migration challenges, with continued financial support and operational assistance from the Commission and Frontex. European Commission President *Ursula von der Leyen* celebrated the achievement, stating, "Today is a day of joy for all Bulgarians, Romanians, and our entire Union. Together, we will reap the benefits of a stronger and more connected Union."

This decision is another crucial step in uniting Europe under Schengen, the world's largest free movement zone, benefiting nearly 450 million people across the EU. Together with Bulgaria and Romania, the Schengen area now covers 29 countries (of which are 25 EU Member States).

The Schengen area is one of the main achievements of the European project. It started in 1985 as an intergovernmental project between five EU countries – France, Germany, Belgium, the Netherlands and Luxembourg – and has gradually expanded. Schengen is the name of a small village in Luxembourg, on the border with Germany and France, where the Schengen Agreement and the Schengen Convention were signed in 1985 and in 1990 respectively. The rules that apply at the external and internal borders of the Schengen area – including random border checks on persons and systematic border checks on persons for specific circumstances – are set out in the Schengen Borders Code. (AP)

Ukraine Conflict

EU Reactions to Russian War against Ukraine: Overview End of November 2024 – January 2025

This news item continues the reporting on key EU reactions following the Russian invasion of Ukraine on 24 February 2022: the impact on the EU's internal security policy, on criminal law, and on the protection of the EU's financial interests. The following overview covers the period from November 2024 to January 2025. For overviews of the previous developments →eucrim 3/2024, 174–176 and →eucrim 2/2024, 91–92, each with further references.

■ 22 November 2024: The European Commission releases updated guidelines on the "best efforts" obligation under Article 8a of Council Regulation (EU) No 833/2014, which governs sanctions against Russia and Belarus as a response to the illegal annexation of Crimea and Sevastopol. These updates clarify EU operators' responsibilities when managing entities outside the Union, ensuring they take all feasible actions to prevent their controlled entities from undermining sanctions. The guidelines emphasise that compliance measures should be tailored to each operator's size, nature, and level of control over non-EU entities. This includes implementing compliance programmes, monitoring activities, and ensuring due diligence. However, if external factors, such as third-country laws, make control impossible, liability may be mitigated. The update also clarifies the difference between "circumvention" and "undermining" of sanctions, with the latter referring to any activity that enables Russia to obtain restricted goods, technology, or financial resources. EU operators are expected to actively prevent such activities, especially when they control or own entities outside the EU. The new guidelines aim to ensure uniform enforcement of EU sanctions, strengthening efforts to limit Russia's ability to finance its war against Ukraine while maintaining fair compliance expectations for businesses operating globally.

■ 11 December 2024: In Case T326/22, the General Court of the European Union (GC) rules against *Dmitry Konov*, a Russian businessman, confirming the EU's restrictive measures against him. Konov challenged his inclusion on the sanctions list, which led to the freezing of his assets, arguing that he does not meet the criteria of an "influential businessman" and that the measures violate his fundamental rights. The GC finds that the EU Council provided sufficient evidence to justify the sanctions.

■ 16 December 2024: The Council adopts the 15th package of economic and individual restrictive measures against Russia (for the 14th package of sanctions →eucrim 1/2024, 11). It intends to further limit Russia's ability to continue its war against Ukraine. This latest set of restrictive measures targets individuals, companies, and industries supporting Russia's military and economic operations. It includes 84 new listings, sanctioning individuals responsible for war crimes, propaganda, and the deportation of Ukrainian children, as well as defense and shipping companies transporting oil and military supplies. In an effort to curb sanctions circumvention, 52 additional vessels have been banned for violating oil price caps or aiding Russia's war efforts, while 32 entities from third countries, including China, India, Iran, Serbia, and the UAE, now face stricter export controls on technology and dual-use goods. To protect European businesses, the Council blocks the recognition/enforcement of Russian court rulings against EU companies in the EU and extends deadlines for firms seeking to exit the Russian market, which is to ensure an orderly divestment process.

■ 18 December 2024: The Commission disburses €4.1 billion to Ukraine under the Ukraine Facility. It is the second regular payment under the Facility, which includes a total of €50 billion in the period 2024–2027. The disbursement follows a positive assessment of Ukraine's reform efforts in certain areas. These are related to business environment, labour market, regional

policy, energy market, environmental protection, and the fight against corruption as set out in the Ukraine Plan.

■ 18 December 2024: In case T-732/22, the General Court (GC) confirms the legality of Council decisions to impose restrictive measures against Russian oligarch *Oleg Vladimirovich Deripaska*. Deripaska challenged several EU decisions and regulations putting him on the sanctions list, and he requested compensation for immaterial damage suffered. In its judgment, the GC analyses concepts such as "influential businessman" and "businessman active in economic sectors providing a substantial source of revenue to the Russian government" as defined in Art. 2(1)(a) and (g) of Decision 2014/145/CFSP. The judgment addresses issues related to the obligation to state reasons, the right to effective judicial protection and defense rights, potential errors of assessment, proportionality, the right to property, and the right to be heard.

■ 19 December 2024: The European Council adopts conclusions on Ukraine. They condemn Russia's ongoing aggression and reaffirm the EU's commitment to military, financial, and humanitarian aid for Ukraine. The European Council highlights the following measures in support of Ukraine: accelerating the delivery of air defense systems, ammunition, and training; implementing the Ukraine Facility with €16.2 billion in 2024 and €12.5 billion in 2025, plus disbursement of €18.1 billion in 2025 from the G7-led Extraordinary Revenue Acceleration (ERA) loans initiative for defense and reconstruction; supporting Ukraine's power grid and intensifying EU energy integration; enforcing the 15th sanctions package (see above) and countering sanctions circumvention. The conclusions also stress that the EU remains committed to Ukraine's recovery and announce a Ukraine Recovery Conference to be held in July 2025 in Italy.

■ 10 January 2025: The Commission disburses the first €3 billion tranche of the G7 ERA loan. The G7 ERA loans initiative will collectively provide approximately €45 billion in financial support to Ukraine in 2025 (of which the EU will contribute €18.1 billion). The loan is designed to support Ukraine's current and future military, budget, and reconstruction needs. It complements the EU's Ukraine Facility. The G7 instrument offers very favourable terms to Ukraine, and repayment will be ensured through the extraordinary profits from immobilised Russian assets collected from the Ukraine Loan Cooperation Mechanism (ULCM). In doing so, the G7 countries send a clear signal to Russia that the burden of reconstructing Ukraine will be borne by those responsible for its destruction.

■ 10 January 2025: The Commission publishes a factsheet and a summary that inform about the EU's measures of solidarity with Ukraine. The documents include an overview of the EU's and Member States' funding of Ukraine since the beginning of the war in February 2022. The total support currently amounts to €132 billion. In addition, the key achievements of the solidarity with Ukraine are outlined: maintaining Ukraine's economy, keeping Ukraine open to international trade and ensuring food security, supplying the country with military and technological means, integrating Ukraine into the European family, imposing sanctions on Russia, and holding Russia accountable for its actions and making it pay for the destruction it causes.

■ 15 January 2025: The General Court (GC) dismisses an action for annulment brought by a major Russian mobile telephone and telecommunications operator (*MegaFon*) against the company's inclusion into the list of Russian entities subject to restrictive measures (Case T-193/23). The GC states that the Council did in fact set out the actual and specific reasons why it decided to apply restrictive measures to MegaFon. The Court also rejects MegaFon's arguments relating to the infringement of its rights of defence. It notes in particular that the Council was under no obligation to hear MegaFon before including it on the aforementioned list. Lastly, the judges in Luxembourg find that there was no error of assessment by including and maintaining the company's name on the list, and there was no violation of the company's freedom to conduct a business.

■ 23 January 2025: In a resolution, the European Parliament (EP) condemns Russia's use of disinformation and the Russian regime's historical claims about Ukraine as a means to justify an illegal war. The EP reiterates its call for the establishment of a special tribunal to investigate and prosecute the crime of aggression committed by the leadership of the Russian Federation against Ukraine and calls for the EU to expand its sanctions against Russian media outlets conducting disinformation and information manipulation campaigns. MEPs also voice concern over the decision by some social media companies to relax fact-checking rules.

■ 27 January 2025: The Foreign Affairs Council renews the EU restrictive measures against the Russian Federation's due to the country's continuing actions destabilising the situation in Ukraine for a further six months, until 31 July 2025. The restrictive measures, which above all curb business with Russia, were first introduced in 2014, and then significantly expanded since February 2022 in response to Russia's military aggression against Ukraine. (AP/TW)

Artificial Intelligence (AI)

EDPB Opinion on AI Data Processing

spot light

On 17 December 2024, the European Data Protection Board (EDPB) published its Opinion on certain data protection aspects related to the processing of personal data in the context of Artificial

Intelligence (AI) models. It follows a request addressed by the Irish data protection supervisory authority to the EDPB (pursuant to Art. 64(2) GDPR).

The Opinion addresses the following questions:

- When and how can an AI model be considered "anonymous"?
- How can controllers demonstrate the appropriateness of legitimate interest as a legal basis in the development phase?
- How can controllers demonstrate the appropriateness of legitimate interest as a legal basis in the deployment phase?
- What are the consequences of the unlawful processing of personal data in the development phase of an AI model on the subsequent processing or operation of the AI model?

The Opinion follows a request addressed by the Irish data protection supervisory authority to the EDPB (pursuant to Art. 64(2) GDPR).

In response to the first question, the EDPB confirms that not all AI models trained with personal data can necessarily be considered anonymous, and therefore the assessment of the anonymity of AI models should be carried out by competent supervisory authorities on a case-by-case basis. The Opinion provides a list of methods that may be used by controllers in their demonstration of anonymity. It can be considered by the supervisory authorities when assessing a controller's claim of anonymity.

Looking at the second and third questions, the Opinion reiterates that there is no hierarchy between the legal bases provided by the GDPR and that it is up to data controllers to identify the appropriate legal basis for their processing activities. To do so, they should apply the three-step test developed to assess legitimate interest under the GDPR: (1) identify a legitimate interest, (2) demonstrate that the processing is necessary to fulfil it, and (3) balance the processing against the rights and freedoms of the data subjects. The EDPB provides further advice on how the three-step test should be applied in the given context. With regard to the third step (balancing test), the Opinion particularly highlights the role of data subjects' reasonable expectations and that the context of the processing is important to be taken into account.

With regard to the fourth question, the EDPB emphasizes that supervisory authorities enjoy discretionary powers to assess any possible infringement(s) and to choose appropriate, necessary, and proportionate measures, taking into account the circumstances of each individual case. These discretionary powers vary, depending on the given scenario, i.e., whether the personal data retained by the AI model are processed lawfully/unlawfully by the same model or by another controller. (CR)

Legislation

EU Strengthened Cybersecurity with New Legislative Measures

The European Parliament and the Council adopted two new laws under the cybersecurity legislative package to bolster the EU's ability to detect, prepare for, and respond to cyber threats and incidents:

- The Cyber Solidarity Act (Regulation 2025/38);
- The targeted amendment to the Cybersecurity Act (CSA) (Regulation 2025/37).

Both legal acts were published in the EU's Official Journal of 15 January 2025.

These initiatives build on the 2019 CSA, which established the EU's first cybersecurity certification framework (→eucrim 2/2019, 98–99). A provisional agreement on both proposals was reached on 6 March 2024, paving the way for their adoption. The measures were based on proposals introduced by the European Commission on 18 April 2023, which included the European Cyber Shield concept and updates to the CSA (→eucrim 1/2023, 12).

➤ *Key Elements of the Cyber Solidarity Act*

The legislation established new EU capabilities to enhance resilience against cyber threats and improve cooperation mechanisms. Among its measures is the creation of a cybersecurity alert system, consisting of national and cross-border cyber hubs across the EU. These hubs, using advanced technologies like artificial intelligence and data analytics, will be tasked with detecting and responding to cyber threats while facilitating timely information sharing across borders.

The law also introduced a cybersecurity emergency mechanism to support preparedness and incident response within the EU, such as testing critical sectors (healthcare, transport, energy) for vulnerabilities and creating a new EU cybersecurity reserve. The reserve includes private-sector incident response services ready to assist Member States and EU institutions during significant cybersecurity incidents. Additionally, mutual technical assistance and an incident review mechanism have been established to assess the effectiveness of these measures and their impact on industry competitiveness.

➤ *Amendments to the 2019 Cybersecurity Act*

The targeted amendment to the CSA aimed to enhance the EU's cyber resilience by enabling European certification schemes for managed security services. Recognizing the growing importance of services like incident handling, penetration testing, and security audits, the amendment sought to ensure the quality and comparability of these services while preventing market fragmentation. By supporting the development of trusted cybersecurity

service providers, this amendment reinforces the EU's commitment to building a robust cybersecurity framework.

For the EU's work on promoting cyber resilience and ensuring a safe online society and economy, an overview can be found at the European Commission's website "Cybersecurity Policies. (AP)

Digital Space Regulation

High Level Group Recommendations on Law Enforcement Data Access

spot light

On 15 November 2024, the High-Level Group on access to data for effective law enforcement (HLEG) published its concluding report. The concluding report outlines possible solutions on how law enforcement authorities (LEAs) can overcome challenges in their daily work in connection with the access to data to prevent and fight crimes and to enhance public security in the digital age. The HLEG was established in 2023 in order to support the Commission and the Council in defining the future EU policy and legislation regarding adequate law enforcement access to data (→eucrim news of 12 March 2024).

➤ *Basis: the recommendations of spring 2024*

The concluding report builds on 42 recommendations that the HLEG presented in spring 2024. The recommendations addressed current and anticipated challenges in view of technological developments, such as problems for LEAs in accessing data in a readable format for criminal investigations. The recommendations aimed at enabling a comprehensive EU approach to ensure effective criminal investigations and prosecutions and were clustered in three blocks:

- Capacity building;
- Cooperation with industry and standardisation;
- Legislative measures.

➤ *The main points in the concluding report*

The concluding report seeks to give more impetus on how the recommendations could be operationalized, and to provide a clear and concise narrative on access to data for law enforcement. The report summarises the key challenges for lawful data access in the context of criminal investigations and prosecutions. In addition, it describes the main issues of and possible solutions for the three workstreams that guided the HLEGs mandate:

- Digital forensics;
- Data retention;
- Lawful interception.

Digital forensics refers to the collection, analysis and preservation of digital evidence (both communication metadata and content data) stored in any digital form on an electronic device, including information from computer hard drives, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, data stored in the cloud and other digital devices. As far as digital forensics are concerned, the HLEG points out that LEAs must boost their resources, skills and technical solutions with regard to accessing encrypted data. In this context, there is a need for more effective cross-border cooperation by sharing expertise, developing standardised tools and procedures, and pooling resources. Next to such capacity building measures, LEAs must be enabled to have access to data in a readable format under clearly regulated circumstances, which would be a more sustainable long-term solution.

Looking at data retention, i.e. the collection of potential evidence stored by communication providers in the form of metadata, the HLEG advocates a harmonised and consistent legislation "which complies fully with fundamental rights". Given the rapid advancement of technologies, law enforcement's timely access to relevant data stored by providers is becoming "increasingly valuable". The report outlines in particular that access to said metadata is essential for identifying suspects and understanding their activities.

With regard to lawful interception, which relates to the access to the content of a communication, a major issue is, according to the HLEG, the shift from traditional communication providers to "over-the-top (OTT) services" and the fact that criminals are increasingly moving to end-to-end encrypted platforms. Therefore, lawful access to communications in real time requires an assessment of the need for clear rules for cooperation between LEAs and technological companies. In addition, enhanced cooperation at EU level in order to facilitate cross-border requests is needed.

➤ *Reactions by the Council*

On 13 June 2024, the Home Affairs Ministers of the EU Member States held an exchange of views on the HLEG's 42 recommendations at the JHA Council meeting. They welcomed the recommendations and identified the following three priority areas of work that should be addressed during the next legislative term: (1) a harmonised EU legal framework for data retention, (2) the establishment of rules for access to data pertaining to interpersonal electronic communication, and (3) legally and technically sound solutions to access encrypted electronic communication in individual cases and subject to a judicial order for the purpose of preventing, investigating, and prosecuting serious and organised crime as well as terrorism.

At the Council meeting of 12 December 2024, the Home Affairs Ministers discussed the next steps after the HLEG finalised its work by the concluding report. In its conclusions on access to data for effective law enforcement, the Council called on the Commission to present, by the first half of 2025, a roadmap for the implementation of concrete measures to guarantee ac-

cess to data for effective law enforcement, "taking into account the relevant case law of the Court of Justice of the EU and with full respect for fundamental rights." The Ministers stressed that the matters raised by the HLEG should be treated with urgency and the needs of law enforcement to ensure public security should be explained "through a common communication narrative". The committees COSI and CATS are tasked with coordinating, discussing and monitoring the implementation of the envisaged roadmap prepared by the Commission.

➤ *Reaction by data protection experts*

On 4 November 2024, the European Data Protection Board (EDPB) issued a statement on the HLEG's 42 recommendations. The EDPB casted doubts whether all measures suggested by the HLEG would be compliant with the Charter of Fundamental Rights of the EU, especially the right to data protection and the respect for private and family life, given their potential serious intrusiveness. The EDPB criticised, for instance, the fact that the recommendations are not complemented and supported by objective evidence, including, where relevant, statistics, which makes it difficult to assess the necessity and proportionality of certain proposed measures. The EDPB also raised specific concerns over the HLEG's position on data retention. With regard to data security and encryption, the EDPB emphasised that "preventing the use of encryption or weakening the effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide."

➤ *Reaction by civil society*

On 11 December 2024, 55 associations and organisations from civil society voiced concerns over the HLEG's recommendations and concluding report in an open letter to the Justice and Home Affairs Council. In light of the HLEG's overall aim to grant law enforcement authorities maximal access possible to personal data, the associations/organisations identify important risks of mass surveillance as well as substantial security and privacy threats, if these recommendations were taken as a basis for future EU policies and legislation. Among other things, the associations/organisations recommend the following to policy makers:

- Discarding any measure that may bypass the protections afforded by encryption or weaken them, as it would create security and privacy threats to millions of people, public institutions and inevitably damage the broader digital information ecosystem;
- Giving up the plan to extend the data retention obligation, because this would generate in people's mind the feeling that their private life is the subject of constant surveillance and cannot be considered compliant with the legal requirements;
- Guaranteeing that any measure respects professional secrecy;
- Not accepting "backdoor mechanisms" for law enforcement, which can always be exploited by other actors, as numerous examples have shown.

Lastly, the open letter criticised the HLEG's outline of the enforcement framework, including harsh sanctions to deter and punish non-compliance with EU obligations and law enforcement orders (administrative sanctions, commercial ban, imprisonment). This would risk either driving reliable operators offering secure services out of the EU market or out of business if they are small or not-for-profit, or preventing them from developing secure solutions if established in the EU. In addition, such approach would be highly detrimental to the EU's cybersecurity initiatives and ambitions. In sum, the civil society associations/organisations are of the opinion that the law enforcement objectives of general interest can be met with less intrusive measures than mass surveillance and systemic weakening of essential security guarantees.

The critical voices show that the Commission is now in a delicate position. On the one hand, it has to implement the Council's mandate to lay down concrete proposals on "adequate" law enforcement access to data, while on the other, there are still many questions regarding the protection of fundamental rights, in particular the right to privacy and data protection. With the presentation of the roadmap envisaged for the second quarter of 2025, the discussion will pick up speed again. (TW)

Overview of the Latest Developments on the DSA: November 2024 – January 2025

The Digital Services Act (DSA) is designed to foster a safer, fairer, and more transparent online environment (→eucrim 4/2022, 228–230). It establishes new obligations for online platforms, thereby ensuring that EU users are safeguarded against the dissemination of illicit goods and content and that their rights are respected when they engage in interactions, share information, or make purchases online. The DSA is also highly relevant for law enforcement purposes (→eucrim 1/2024, 13).

This news item continues the reporting on the latest developments concerning the DSA in the form of a chronological overview. For overviews of the previous developments: April-August 2024 →eucrim 2/2024, 94–95; September-October 2024 →eucrim 3/2024, 178.

- 25 November 2024: The short message platform Bluesky is under increasing scrutiny from the European Commission for alleged non-compli-

ance with the DSA. The DSA imposes disclosure obligations on all online platforms operating in the EU, including requirements to provide details on user numbers, designate an EU-based contact person, and publish a dedicated webpage with legal and operational information. According to the Commission, Bluesky has not fulfilled these obligations. The EU Commission has tasked national Digital Services Coordinators (DSCs) to investigate whether Bluesky is adhering to the DSA requirements. In Germany, the Federal Network Agency confirmed it had been asked to determine whether Bluesky has a branch, legal representative, or contact person in the country. The agency reported that Bluesky has not complied with any of these obligations. While the Commission oversees large platforms, enforcement for smaller platforms like Bluesky falls under the jurisdiction of national authorities. The Commission has emphasized that it is up to individual DSCs to enforce compliance, with Germany and other Member States taking the lead in examining Bluesky's operations. Bluesky currently has around 20 million global users, far below the DSA threshold for classification as a "Very Large Online Platform" (VLOP), which requires at least 45 million monthly users in the EU. As such, the platform must meet baseline obligations, including appointment of an EU contact person and reporting user data. The Federal Network Agency in Germany has stated that no further action is currently required, as the Commission's inquiry into Bluesky is considered closed for now. However, should any national DSC take enforcement action, it will act on behalf of all EU Member States. Bluesky will be required to comply once a DSC formally intervenes.

■ 29 November 2024: The European Commission convenes a roundtable with major platforms like TikTok, Meta, Google, Microsoft, and X to discuss election readiness under the DSA in the context of Presidential and Parliamentary elections in Romania. The Commission requested platforms to share risk assessments and mitigation measures for threats like disinformation and platform manipulation. Discussions also addressed cooperation with stakeholders, recommender systems, and the need for independent researcher access to platform data. With election integrity a key DSA priority, the Commission is monitoring compliance, with ongoing proceedings against X, Facebook, and Instagram for alleged violations. TikTok has also been asked to clarify its handling of information manipulation risks.

■ 17 December 2024: The European Commission launches formal proceedings against TikTok for suspected violations of the DSA related to systemic risks impacting election integrity. The investigation follows allegations of foreign interference during Romania's recent presidential elections. The investigation will examine TikTok's management of risks linked to recommender systems, possible coordinated inauthentic activity, and policies on political advertisements and paid-for content. The probe will focus on whether TikTok properly addressed regional and linguistic risks tied to national elections. The Commission is working closely with Ireland's Digital Services Coordinator, given TikTok's EU establishment there. It will gather further evidence through additional information requests, monitoring actions, and inspections, including an analysis of TikTok's algorithms. The proceedings empower the Commission to enforce interim measures or accept commitments from TikTok to address the identified risks. The investigation into electoral integrity marks the third investigation into TikTok under the DSA, underscoring growing scrutiny of the platform in the EU.

■ 17 January 2025: The European Commission takes additional investigatory steps into X's compliance with the DSA regarding its recommender system. The measures include: a request for internal documentation on the platform's recommender system and recent changes, due 15 February 2025; a retention order requiring X to preserve documents related to future algorithm changes from 17 January to 31 December 2025 or until the investigation concludes; access to X's commercial APIs (Application Programming Interfaces) to assess content moderation and account virality. These steps aim to evaluate whether X's systems align with the DSA's goals of ensuring a fair, safe, and democratic online environment. The investigation remains ongoing.

■ 20 January 2025: The European Commission incorporates the revised Code of Conduct+ on Countering Illegal Hate Speech Online into the Digital Services Act framework. Major platforms, including Facebook, TikTok, X, and YouTube, have committed to reviewing flagged hate speech within 24 hours, improving transparency, and collaborating with experts and civil society. The Code supports DSA compliance and includes annual audits to ensure that platforms mitigate hate speech risks effectively. It builds on EU legal frameworks, aiming to combat hate speech while upholding democratic values and freedom of expression. Regular evaluations will ensure that the Code continues to meet emerging challenges.

■ 21 January 2025: The European Parliament debates the enforcement of the DSA to protect elections and democracy from disinformation, foreign interference, and biased algorithms. The Commission highlighted ongoing investigations into platforms like TikTok and X for election-related risks and emphasized transparency requirements, including user opt-out options for profiling and content moderation disclosures. The Commission also announces plans for a European

Democracy Shield to counter disinformation and strengthen electoral integrity, building on the European Democracy Action Plan. Collaboration with national Digital Services Coordinators and international partners will ensure robust enforcement, with staff and resources being doubled to address rising threats.

- 31 January 2025: The Federal Network Agency (FNA), in its capacity as Digital Services Coordinator (DSC) for Germany, conducts a stress test with VLOPs ahead of the Parliamentary elections in Germany. Participants included representatives of Google (YouTube), LinkedIn, Microsoft, Meta (Facebook, Instagram), Snapchat, TikTok, X, as well as of national authorities and civil society organisations. The test aims to test platforms' readiness to address behaviours on these platforms which could occur in the run-up to the elections and could pose a risk related to civic discourse and electoral processes. It follows a roundtable held on 24 January 2025 in which the FNA and the VLOPs discussed current election-related trends and risk-minimising measures by the major online platforms and search engines, in order to assure their election readiness (see also above 29 November as regards the elections in Romania). (AP)

Institutions

Council

PL, DK, CY: New Cycle of Trio of Council Presidencies

On 1 January 2025, the new trio of Presidencies of the Council of the EU began their 18-month programme, with Poland taking over the Presidency of the Council of the EU from 1 January 2025 to 30 June 2025 (→next news item). Denmark and Cyprus will take over in the second half of 2025 and the first half of 2026, respectively. The trio of presidencies begins the new institutional cycle against the backdrop of Russia's war of aggression against Ukraine, the dramatic situation in the Middle East and political turbulences in Western countries.

The trio's programme focuses on the following three main themes:

- A Strong and Secure Europe: This theme refers to external actions, security and defence, migration and border protection, enlargement, and internal reforms;
- A Prosperous and Competitive Europe: This theme concerns the various components that make up competitiveness, twin transition, innovation, the environment, and social affairs;
- A Free and Democratic Europe: This theme contains references to EU values, such as rule of law and human rights.

The priorities of the trio to ensure a strong and secure Europe are as follows:

- Coherent and influential external action;
- Strategic action on security and defence;
- A comprehensive approach to migration and border management;
- A well-prepared enlargement;
- Internal reforms.

In the area of criminal justice, the trio will work to prevent and fight crime, both online and offline, and to strengthen efforts to detect and combat terrorism, violent extremism, and serious and organised crime and corruption.

Another focus will be on securing free and pluralistic media and protect freedom online. Political priorities in this regard will include the fight against disinformation, the protection of civil society, tackling foreign interference, and ensuring greater transparency. Countering hate speech, ensuring democratic dialogue on tech platforms, protecting minors from harmful content online, and preventing the abuse of such platforms for criminal purposes will be addressed as well.

The trio will also launch work on the Multiannual Financial Framework post-2027, which will have to reflect the priorities in the strategic agenda 2024–2029. (CR)

Programme of the Polish Council Presidency

Poland assumed the Presidency of the Council of the EU for the period from 1 January 2025 to 30 June 2025 under the motto "Security, Europe!"

In the wake of Russia's armed aggression against Ukraine, the Presidency emphasises the need to strengthen the EU's own defence capacity. Therefore, the priorities of the Polish Presidency programme focus on supporting activities that strengthen European security in all its dimensions: external, internal, information, economic, energy, food and health.

In the field of defence and security, the priorities are to increase the EU's defence readiness, support the defence industry, and strengthen cooperation with NATO. Resisting foreign interference and disinformation is another priority of the programme. To ensure the security and freedom of businesses, the programme plans to intensify the internal market, reduce bureaucratic hurdles, and restore fair competition to EU industry on the global stage. Further priorities include measures to improve the reliable and secure supply of energy resources and to reduce the EU's dependence on imported technologies, while at the same time ensuring that citizens and businesses have access to energy in sufficient quantities and at affordable prices. A competitive and resilient agriculture with a strong Common Agriculture Policy, the digital transformation of healthcare, the improvement of EU medicines security, and the diversification of medicines supply chains, as well as support for their production in the EU will also play an important role.

Regarding internal security, the programme addresses issues such as combatting major cross-border criminal networks, hybrid threats, terrorism, and radicalisation. In terms of judicial cooperation in criminal matters, the Polish Presidency is focusing on the fight against corruption, trafficking of illicit drugs, human trafficking and migrant smuggling, and enhancing the level of protection for victims of crime. Another priority is the protection of minors from exploitation, including sexual abuse. In the light of technological developments and online threats, the Presidency aims to bring forward an updated legal framework for the protection of children from online exploitation, especially with regard to the draft Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material. Furthermore, the Polish Presidency will continue the work on the draft Directive establishing minimum rules concerning the definition of criminal offences and sanctions in the area of facilitation of unauthorised entry, transit and stay of third-country nationals, as well as measures to prevent and counter the commission of such criminal offences. Efforts will also continue to ensure accountability for perpetrators of crimes committed in connection with the war in Ukraine.

On the subject of economy and financial affairs, the Polish Council Presidency wants to hold "the first important discussions" on the future multiannual financial framework (MFF) and guide the Commission in the preparation of the MFF post-2027. While the EU's next multiannual budget will not come into force as early as 2028, Poland is already planning a conference on this topic in February 2025. Furthermore, Poland will support claims for a stronger link between cohesion policy and structural reforms.

The Polish Presidency also marks the beginning of the new trio of Presidencies. Denmark and Cyprus will take over in the second half of 2025 and the first half of 2026, respectively (for the trio presidency programme →previous news item). (CR)

Commission

New European Commission Took Office

After its election by the newly formed European Parliament and formal appointment by the European Council at the end of November, the new European Commission took office on 1 December 2024. The College is made up of Commissioners from 27 EU countries, each of them with equal status. Each Commissioner is responsible for a specific policy area. Re-elected President *Ursula von der Leyen* (from Germany) will lead the new College of Commissioners for a second term, together with High Representative and Vice-President *Kaja Kallas* (from Estonia) and five Executive Vice-Presidents.

The new Commission is guided by seven key priorities to create a faster, simpler, and more united Union. The priorities for the years 2024–2029 are as follows:

- A new plan for Europe's sustainable prosperity and competitiveness;
- A new era of European defence and security;
- Support for the people; the strengthening of the European social model and societies;
- Preservation of quality of life: food security, water, and nature;
- Protection of democracy; preservation of European values;
- A global Europe: leveraging Europe's power and partnerships;
- Mutual implementation of deliverables and preparation of the Union for the future.

In the area of Home Affairs and Migration, newly appointed Commissioner *Magnus Brunner* (from Austria) is expected to design and implement a new European Internal Security Strategy as well as strengthen law enforcement and judicial cooperation. He will also lead the efforts against serious and organised crime, cybercrime, and terrorism, above all by proposing a new European action plan against drug trafficking, a renewed EU action plan on firearms, and by leading the work in the fight against cybercrime and on a new Counter-Terrorism Agenda. He will lead the efforts in the fight against serious and organised crime and work to better protect children against sexual abuse, both online and offline. He is also tasked with ensuring that Europol becomes a truly operational police agency. Furthermore, Brunner will oversee the implementation of the Pact on Migration and Asylum, develop a new and common approach on the return of irregular migrants, and lead the efforts in the fight against migrant smuggling. He will promote integrated border management, strengthen Frontex, and work towards achieving a fully functional European digital border management.

The new Commissioner for Budget, Anti-Fraud and Public Administration *Piotr Serafin* (from Poland) will focus on preparing the next long-term budget. He is, *inter alia*, tasked with protecting the EU budget and with the fight against fraud. This includes coordination of the implementation of the Conditionality Regulation, to ensure that respect for the rule of law remains imperative for EU funds. Serafin will lead a review of the overall anti-fraud architecture linked to the EU's financial interests, ensuring effective and efficient cooperation with the European Public Prosecutor's Office to protect the EU budget.

Michael McGrath (from Ireland), the newly appointed Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, will be responsible, *inter alia*, for the development of a clear EU approach to

anti-corruption, ensuring that EU funding is put towards national measures to fight corruption. He will also ensure that EU budget instruments are always implemented in a way that is fully consistent with respect for the rule of law and fundamental rights. Looking at his portfolio for justice and consumer protection, one of his responsibilities concerns the full enforcement of the General Data Protection Regulation while ensuring that it stays up to date as well as the promotion of trusted data flows with international partners. In addition, another focus of his work will be on strengthening the European Arrest Warrant to allow judicial authorities to work more closely and to step up cooperation between Europol and Eurojust. (CR)

OLAF

OLAF's Operational Work July – December 2024

This news item summarises OLAF's operational work in the second half of 2024 in reverse chronological order. It follows the reports on operations supported by OLAF in the first half of 2024 published in →eucrim 1/2024, 17–18.

■ 20 December 2024: Information on the second edition of Operation BELENOS is made public. During two weeks in November 2024, Operation BELENOS II targeted illicit financial flows linked to money laundering, terrorism financing and organised crime (for the first edition → eucrim 4/2023, 318). According to first estimations, over €2.7 million in cash and valuable items such as gold and jewelry with a value exceeding €1.7 million were seized. The law enforcement action included checks of over 500 cash movements, the inspection of several postal purchases and the control of over 300 travelers. OLAF provided financial, analytical and technical support to the Member States; it also ensured the secure exchange of information during the operation by using its Virtual Operations Coordination Unit (VOCU) application. Operation BELENOS II was led by the French customs authorities and involved customs authorities from 23 EU Member States.

■ 20 November 2024: OLAF informs of the results of the Joint Customs Operation KHIONE that aimed at disrupting the illegal trade in refrigerant gases smuggled into the EU. The Operation ran from May to October 2024 and prevented that more than 400,000 tons of F-gases entered the EU market. The Operation was coordinated by OLAF and involved 16 EU Member States, Türkiye and Ukraine.

■ 28 October 2024: In the joint police-customs Operation DECOY, supported by Europol and OLAF, law enforcement authorities from 18 countries seize over €14 million in counterfeit money. The operation targeted the disruption of organised criminal networks distributing fake banknotes and coins via postal services across Europe. It led to the seizure of 174 parcels containing counterfeit currency and the interception of a total of 148,130 counterfeit items, including 134,949 euro banknotes and coins, 9,186 British pounds, and 3,595 US dollars. Europol and OLAF supported the operation by facilitating intelligence-sharing, helping to detect suspect parcels, and refining risk indicators for future efforts to combat counterfeit currency distribution.

■ 23 October 2024: Europol and OLAF publish the result of the 2024 Operation OPSON (meanwhile in its thirteenth run), which tackles food fraud, the counterfeiting of food and beverages, and the abuse of geographical indications (for the previous operation →eucrim 4/2024, 318–319 with further references). Involving authorities in 29 countries across Europe as well as food and beverage producers from the private sector, Operation OPSON XIII resulted in the seizure of around 22,000 tonnes of food and around 850,000 litres of (mostly alcoholic) beverages. 11 criminal networks were dismantled and 104 arrest warrants issued. One of the trends detected was that fraudsters are increasingly selling expired food. Olive oil and wines were among the products which were illegally traded bypassing protected designations of origin.

■ 22 October 2024: Thanks to intelligence provided by OLAF, Dutch authorities confiscated four containers filled with nearly 4,800 cylinders of F-gases at the port of Rotterdam. This is the largest-ever seizure of F-gases in the Netherlands. Given that the black market in F-gases (hydrofluorocarbons, or HFCs) is growing due to strict import quotas in the EU, OLAF has focused on monitoring the international traffic of F-gases to the EU from third countries.

■ 15 October 2024: OLAF assists Spanish law enforcement authorities which crack down a Spanish company involved in the illegal export of chemical products to Russia. The Spanish authorities seize 13 tons of chemical substances and arrest four persons. The operation reveals a criminal network that circumvented EU sanctions against Russia (following its invasion of Ukraine) by rerouting shipments of chemical products via Armenia and Kyrgyzstan to Russia. OLAF's assistance is part of the Joint Sanctions Enforcement Operation that OLAF has been running since July 2023 to enforce trade sanctions against Russia.

■ 3 October 2024: Romanian authorities seize 1,000 litres of counterfeit pesticides with a value of over €600,000. The products were manufactured outside the EU and seemingly smuggled from Eastern Europe to Romania. Two Ukrainian nationals allegedly involved in the smuggling are arrested. The operation was supported by OLAF which provided intelligence and informed about the suspicious shipment.

■ 12 August 2024: A joint operation led by OLAF, the Spanish National Police, the Spanish Tax Agency Customs Surveillance and the Italian Guardia di Finanza leads to the seizure of over 900,000 counterfeit razor blades of a well-know brand. A criminal network imported the counterfeit products from Chinese suppliers and distributed them to wholesalers in Spain and Italy who sold the goods as genuine products of the brand. OLAF supported the operation *inter alia* by tracking the suspicious shipments, identifying the recipient companies across the EU, informing the involved countries, and coordinating the investigations related to the case.

■ 1 August 2024: OLAF informs about the preliminary results of customs operations against counterfeit products related to the EURO 2024 Football Championship in Germany and the Olympic Games in Paris. Concerted actions led by OLAF, the French customs and the German Customs Investigation Office (ZKA) have already led to over 630,000 items seized, including sportswear, sports shoes, toys, and sporting equipment. As a result, not only illegitimate businesses but also dangers to the citizens' health and safety could be avoided.

■ 17 July 2024: An OLAF investigation leads to the successful dismantlement of a criminal network that established a large-scale smuggling scheme with counterfeit premium vodka and whisky. Almost 400,000 bottles with an estimated value of €14 million were seized. OLAF acted as the main coordination point for exchange of information among various EU and non-EU authorities, collected, analysed and disseminated critical operational intelligence related to the smuggling network, and provided specialised knowledge and technical assistance.

■ 4 July 2024: OLAF supports "Operation Dashboard". The Operation targeted a criminal network that imported scrap vehicles from the United Kingdom to Spain by circumventing the EU rules on hazardous waste. The criminal activities also involved Germany and France. The operation, executed by the Spanish Guardia Civil, led to seven detainees and five individuals under investigation for charges that include alleged crimes against natural resources and the environment, falsification of certificates, money laundering, tax fraud, and membership in a criminal group. It is estimated that over 600,000 kilo of scrap has been illegally imported into the EU since January 2021. OLAF joined the dots and brought the national law enforcement authorities of the involved countries together. (TW)

European Public Prosecutor's Office (EPPO)

First European Prosecutors for Poland and Sweden Appointed

On 12 December 2024, the Council appointed the European Prosecutors for Poland and Sweden. Both countries have recently joined the EPPO with Poland being the 23rd EU Member State joining the EPPO (→eucrim 1/2024, 18) and Sweden the 24th (→eucrim 2/2024, 101).

The first European Prosecutor for Poland is Ms *Grażyna Stronikowska*. As a former prosecutor, Ms Stronikowska has extensive experience in the fight against organised crime and corruption. She was a member of the Supervisory Committee of the European Anti-Fraud Office (OLAF) in Brussels from 2016 to 2022.

For Sweden, Mr *Martin Bresman* is appointed as first European Prosecutor. Prior to joining the EPPO, Mr Bresman was Chief Public Prosecutor and Head of Unit at the National Anti-corruption Unit (NACU) of the Swedish Prosecution Authority. He also had many years of experience as Senior Public Prosecutor at the Swedish Economic Crime Authority and the National Unit against International and Organised Crime.

European prosecutors supervise investigations and prosecutions and, together with the European Chief Prosecutor, form the EPPO College. They are appointed for a non-renewable term of six years. The Council may decide to extend their term for a maximum of three years at the end of this period. (CR)

EPPO Signs Working Arrangement with European Parliament

At the end of November 2024, the EPPO and the European Parliament (EP) signed a working arrangement laying down the modalities of their cooperation for the protection of the EU's financial interests. The aim of the arrangement is to facilitate and clarify procedures relating to the following issues:

■ The exchange of information between the EP and the EPPO;

■ The requests for the waiver of immunity of Members of the EP and staff;

■ The requests for waiver of the inviolability of the premises, buildings, and archives of the EP.

Under the arrangement, the EP is asked to report to the EPPO, without undue delay, any criminal conduct in respect of which the EPPO can exercise its competence. The EPPO, without prejudice to the proper conduct and confidentiality of its investigations, is asked to inform the EP of ongoing and closed investigations in order to enable it to take appropriate precautionary or administrative measures or to intervene as a civil party in proceedings. Both parties have been asked to designate contact points. (CR)

Croatian Solution to Conflict of Competence Worries EPPO

Following a conflict of competence with the Croatian Office for the Suppression of Corruption and Organised Crime (USKOK), European Chief Prosecutor *Laura Codruța Kövesi* sent a

formal letter to the European Commission on 21 November 2024 expressing concern about violations of the rule of law in Croatia. In her letter, *Kövesi* sees a systemic challenge for Croatia to comply with the principles of the rule of law as laid down in Art. 4 of Regulation (EU) 2020/2092 on a general regime of conditionality for the protection of the budget of the EU.

In the present case, USKOK turned to the Croatian State Attorney General to resolve a conflict of competence between its own investigation and that of the EPPO, which the State Attorney General resolved in favour of the USKOK. As a result, the EPPO relinquished its investigation to USKOK.

In her letter, the *Kövesi* draws the Commission's attention to the following concerns:

- The Croatian rule designating the Croatian State Attorney General as the authority to resolve conflicts of jurisdiction is contrary to EU law;
- In the given case, the State Attorney General, tasked with resolving conflicts of competence, further aggravated the situation by basing his decision solely on the interpretation of the USKOK, without giving the EPPO the chance to express its position, and thus undermining the impartiality of the conflict resolution;
- In the present case, when USKOK started its investigation into an EU-funded project, it did not notify the EPPO of the investigation, thus failing to fulfil its obligations under the EPPO Regulation.

It is anticipated that the European Commission will examine the concerns raised by the EPPO and that further action may be taken. (CR)

Overview of Convictions in EPPO Cases: July – December 2024

The following is an overview of court verdicts and alternative resolutions in EPPO cases. It summarises the EPPO's news reports from 1 July to 31 December 2024 and continues the overview presented in eucrim 2/2024, 102. The overview is in reverse chronological order.

- 20 December 2024: Operation "Cheap Ink" leads to the conviction of another three persons for their involvement in a criminal organisation selling toner cartridges and office supplies at low prices by systematically evading VAT. The sentences handed down by the judges at the Court of Padua ranged from nine to four years' imprisonment.
- 19 December 2024: The Regional Court in Düsseldorf convicts three individuals of organised VAT fraud as well as of aiding and abetting tax fraud. The court also orders the confiscation of assets worth €7.4 million from the individuals as part of the sentence. In addition, €1.7 million in seized cash is transferred to the German state treasury. The convictions were the result of operation "Huracán" that had already led to five convictions by the Regional Court in Düsseldorf on 30 October 2024 (see below).
- 3 December 2024: The ringleaders of an organised crime group behind a cross-border VAT fraud scheme are sentenced to four years of imprisonment by the Regional Court of Regensburg. The court also orders the recovery of €960,000. The court considered it established that the individuals had committed fraud involving sales of wireless earbuds through a chain of companies set up to evade VAT obligations, resulting in a combined VAT loss of over €6 million.
- 29 November 2024: The Munich Regional Court sentences five individuals for committing organised VAT fraud involving an estimated VAT loss of around €14 million (the leader of the organisation is sentenced to six years of imprisonment). According to the court, the individuals had organised a cross-border VAT carousel fraud trading scheme involving COVID-19 tests.
- 20 November 2024: The Landshut Regional Court sentences two individuals to three years of imprisonment and a suspended prison sentence of one year and six months, respectively, for organised VAT fraud involving an estimated loss of around €3.7 million. The court was convinced that the individuals had acted as strawmen for a buffer company that was part of a cross-border VAT carousel fraud trading scheme involving small electronic goods.
- 30 October 2024: The Regional Court in Düsseldorf convicts five individuals of organised VAT fraud and of aiding and abetting tax fraud. Following a large-scale fraud investigation, code-named "Hurácan", the court found that the individuals were part of a criminal organisation that fraudulently traded cars, generating a total fraudulent turnover of more than €190 million and creating VAT losses of €53.7 million. The prison sentences range from six years and two months to one year and nine months.
- 22 October 2024: The Specialised Criminal Court of Slovakia sentences a company and its managing director for fraud relating to the EU's Common Agricultural Policy (CAP). The court found it proven that the managing director had made false statements claiming that the company was farming agricultural land in accordance with the legal requirements of the funding, although inspections showed that this was not the case.
- 22 October 2024: The Regional Court of Vilnius convicts two individuals of illegally acquiring €130,000 through forgery of documents, fraudulent management of financial records, and bribery of a public official. The court found that the individuals had deliberately created fictitious chains of research and experimental development (R&D) services for EU and nationally funded project purchases and simulated money transfers.
- 15 October 2024: The Sofia City Court sentences an entrepreneur to

three years of imprisonment, suspended for five years, and orders him to repay the absconded funds with interest for using false documents to obtain EU funds for the construction of a dairy plant, for which the work had never been carried out.

■ 3 October 2024: The director of a company that fraudulently obtained funds from the European Agricultural Fund for Rural Development (EAFRD) is sentenced to one year in prison and fined for fraud. He also has to repay in full the amount defrauded from the EU amounting to €2,119,055.

■ 2 October 2024: The Paris Criminal Court convicts a French company of customs fraud related to the import of sanitary products. The company had deliberately misclassified products under the EU customs tariff to reduce the amount of duties and taxes owed and thus evade customs duties and import VAT, causing €419,000 in damage to both the French and EU budgets. The company was sentenced to pay a €150,000 fine.

■ 4 July 2024: The County Court in Zagreb finds one suspect guilty of subsidy fraud and document forgery, in relation to three projects valued at nearly €650,000, with subsidies requested for almost €370,000, which were co-financed by the European Agricultural Fund for Rural Development (EAFRD) at 85% and the Croatian state budget at 15%. Following a plea bargain in which the defendant pleaded guilty to all charges, he was sentenced to eleven months' imprisonment in exchange for community service and a fine of €25,000. (CR)

EPPO's Operational Activities: October 2024 – mid-January 2025

This news item provides an overview of the EPPO's main operational activities from1 October 2024 to 15 January 2025. It continues the periodic reports of the last issues eucrim 3/2024, 181–182 and is in reverse chronological order.

■ 1 October 2024: Three administrators of two companies importing stainless steel coils are accused of falsifying information on the origin of their products to benefit from duty exemptions and avoid nearly €2.4 million in additional duties introduced by the EU's Anti-Dumping Regulation ((EU) 2016/1036). At the request of the EPPO in Bologna (Italy), the investigating judge orders the preventive seizure of the money in the companies' bank accounts and the seizure of some steel coils from earlier searches.

■ 1 October 2024: An investigation by the EPPO in Milan (Italy) into a VAT fraud involving the sale of Voice over Internet Protocol (VoIP) services leads to the arrests of four suspects and the seizure of assets worth up to €97 million. VoIP is a technology allowing users to make calls via the Internet. By setting up several companies, straw-men, and missing traders in various EU Member States, the suspects had claimed VAT tax reimbursements from the tax authorities worth more than €97 million.

■ 8 October 2024: The EPPO in Berlin (Germany) and the State Criminal Police Office of Brandenburg carry out searches as part of an investigation into an entrepreneur alleged to have illegally obtained over €1.3 million in subsidies from the European Agricultural Fund for Rural Development (EAFRD) and the Brandenburg state budget for the cultivation of organic fennel. A field visit had revealed that the land was neglected and no harvest made in the designated area.

■ 10 October 2024: At the request of the EPPO in Bologna (Italy), Italian authorities seize more than 3.6 million linear meters of fabric, with an estimated value of €4.9 million. The investigation targeted several companies suspected of VAT fraud on illegal imports of textiles from China into the EU, worth around €63 million.

■ 11 October 2024: The EPPO in Sofia (Bulgaria) investigates the former mayor, the ex-governor of Varna, and two public officials from the Executive Agency Maritime Administration. The individuals are accused of falsifying official documents and providing false information to obtain funding from the European Maritime and Fisheries Fund in order to improve the infrastructure of a fishing port, which actually did not exist.

■ 15 October 2024: The EPPO in Milan (Italy) investigates several individuals suspected of procurement fraud. It is alleged that the same team of consultants had applied for numerous projects financed by the European Social Fund (ESF) and the European Regional Development Fund (ERDF) offering consulting services. By submitting repeated, overlapping proposals in multiple tenders for the same team, their working hours exceeded the monthly maximum of possible working hours.

■ 17 October 2024: An investigation by the EPPO in Palermo (Italy) uncovers a fraudulent scheme involving local politicians and individuals from Sicily. The suspects had allegedly misused more than €8.7 million from the European Social Fund (ESF) intended for vocational training and social projects by diverting it to personal expenses and political campaigns instead.

■ 21 October 2024: An investigation by the EPPO in Rome and Milan (Italy) into a €40 million VAT fraud leads to the issuing of a freezing order of €28.8 million. The investigation involves more than 50 defendants involved in the trading of airpods, worth at least €200 million, who had evaded the payment of VAT.

■ 24 October 2024: The EPPO in Zagreb (Croatia) launches an investigation against nine Croatian citizens and one legal entity on suspicion of defrauding over €9 million of EU subsidies and forging official documents. The suspects received funding to im-

prove animal welfare in their pig farming, but the necessary improvements were never established.

■ 25 October 2024: An investigation by the EPPO in Bologna and Milan (Italy) uncovers a complex scheme of international tax fraud, carried out through numerous missing traders who imported clothing and accessories from China into Italy. The turnover was at least €500 million and involved triangulations with Bulgaria and Greece to hide the origin of the goods, thereby evading the payment of €113 million in VAT and customs duties. The illicit profits were allegedly laundered through a Chinese underground banking network with clandestine branches in Italy and money passing through many European countries before reaching China. Some of the money returned to Italy via banking, where the organisation is alleged of investing it in legitimate commercial businesses.

■ 14 November 2024: Operation Moby Dick investigates more than 195 individuals and more than 400 companies involved in a €520 million VAT fraud. The investigation was led by the EPPO in Milan and Palermo (Italy) with the support of Europol and numerous partners in more than 10 countries; hundreds of police officers conducted more than 160 searches and arrested 43 suspects. The investigation revealed that people linked to several mafia clans invested into a criminal syndicate, which had set up a highly profitable tax evasion scheme committing VAT carousel fraud. A freezing order of €520 million is executed to compensate the damage to the EU and the national budgets.

■ 14 November 2024: The EPPO in Paris (France) investigates the illegal import of textiles, garments, and fashion from China into the EU via Greece; approximately €5.2 million in VAT and customs duties was not paid. Applying Art. 31 of the EPPO Regulation, the EPPO in Paris had requested that their colleagues in Greece carry out searches and witness interviews.

■ 15 November 2024: The EPPO in Zagreb (Croatia) initiates an investigation against eight individuals, including the Minister of Health and the directors of two hospitals in Zagreb, and two companies on suspicion of accepting and giving bribes as well as abuse of position and authority to prove that certain companies were allowed to sell medical robotic devices at unreasonably inflated prices. The scheme had affected several hospitals in Croatia and other projects co-financed from the Croatian national budget and within the framework of Croatia's National Recovery and Resilience Plan 2021–2026, financed by the EU's Recovery and Resilience Facility (RRF).

■ 28 November 2024: The EPPO in Cluj-Napoca (Romania) carries out 31 searches in conjunction with an investigation into possible fraud involving works on a Romanian ring road that had been financed with €37 million from the European Regional Development and Cohesion Fund. While the Romanian National Highways and National Roads Company was the beneficiary of the funds, the contract to execute the works was attributed to the Romanian branch of a Chinese company, which hired several subcontractors. It is alleged that these subcontractors colluded with the contractor to present false documents certifying that the works had been successfully completed, but the works did not fulfil the quality standards, and adequate checks had not been carried out by the Romanian National Highways and National Roads Company.

■ Between November and December 2024, operations "Admiral 2" and "Admiral 3" lead to the further dismantling of criminal networks involved in VAT fraud. The two operations continued the "Admiral" investigation (November 2022) and are considered part of the largest VAT fraud ever uncovered in the EU, with damages now estimated at €2.9 billion. All "Admiral" operations were conducted between the EPPO, law enforcement agencies from numerous countries, and Europol. In November 2024, operation *Admiral 2* uncovered another criminal syndicate suspected of a complex VAT fraud scheme involving the trade of popular electronic goods and generating an estimated VAT loss of €297 million. The suspects had established companies in 15 EU Member States, which acted as legitimate suppliers of electronic goods. Although the end customers paid VAT on their purchases, the selling companies failed to fulfil their tax obligations. By disappearing, they avoided paying the amounts owed to the respective national tax authorities. Other companies in the fraudulent chain would subsequently claim VAT reimbursement from these national tax authorities, resulting in an estimated VAT loss of €297 million. The proceeds of these criminal activities were then transferred to offshore accounts. During the days of the operation, the authorities seized a large number of smartphones and other electronic devices worth more than €47.5 million, several luxury cars, and €126,965 in cash; they also froze 62 bank accounts with a total value of more than €5.5 million. In addition, 32 people were arrested. Furthermore, in December 2024, operation *Admiral 3* uncovered a Greece-based syndicate using partly the same organisation and infrastructure as the perpetrators investigated under Admiral to carry out a massive VAT carousel fraud causing an estimated damage to the EU and Hellenic budgets of at least €38 million.

■ 6 December 2024: The EPPO in Berlin (Germany) carries out searches at a bank in Munich as part of an investigation into a company's managing director for a possible €200 million VAT fraud. The managing di-

rector is suspected of having set up the company for the sole purpose of creating a fictitious business identity to carry out transactions through his company's bank accounts with money obtained from VAT carousel fraud.

- 6 December 2024: Two suspects are arrested following an investigation by the EPPO in Munich (Germany) into a €32 million cross-border VAT carousel fraud involving the sale of mobile phones. The mobile phones had deliberately not been entered into the accounts and were sold without VAT.
- 7 January 2025: An investigation by the EPPO in Madrid (Spain) dismantles a transnational criminal network involved in the sale of luxury cars while evading VAT, with an estimated damage in Spain alone amounting to €17 million. As a result, thirty individuals were arrested and 34 properties worth around €11 million, 20 luxury cars, jewellery and high-end watches, and over €300,000 in cash seized. Furthermore, more than 200 bank accounts were blocked in Germany, Lithuania, Portugal, and Spain.
- 13 January 2025: An investigation by the EPPO in Sofia (Bulgaria) uncovers procurement fraud in a project to design and build signalling and telecommunication systems for the Bulgarian rail network. The contract for the execution of the project, worth over €94.5 million in EU financing, had been awarded to a consortium of four companies claiming to have experience in such work, when in fact they had none.
- 13 January 2024: Four suspects are arrested in the Netherlands and their bank accounts frozen on suspicion of large-scale customs fraud involving bicycles imported from China. The investigation by the EPPO in Rotterdam (Netherlands) uncovered that the suspects had evaded the payment of a significant share of the import and anti-dumping duties by systematically undervaluing the goods and falsely declaring their origin, causing an estimated damage of approximately €7.2 million. (CR)

Europol

Europol Intensifies Cooperation with Chile

In November 2024, Europol and Chile signed two legal instruments that put in practice a Working Arrangement that is in force since May 2021. On the basis of this Working Arrangement, the two parties were able to sign a Liaison Officer Agreement and a Memorandum of Understanding on SIENA. The Memorandum of Understanding allows Chile to establish a SIENA connection with Europol, giving Chilean law enforcement authorities the possibility to connect with law enforcement agencies in more than 70 countries. Under the Liaison Agreement, Chile can second one or more liaison officers to Europol, adding to the current network of over 300 liaison officers from EU Member States, third countries, and international organisations hosted by Europol. (CR)

Europol Signs Working Arrangement with Singapore

On 28 November 2024, Europol and the law enforcement authorities of Singapore signed a Working Arrangement to strengthen their cooperation in preventing and combating serious crime and terrorism. This Working Arrangement paves the way for further negotiations on related implementing agreements, such as a SIENA Memorandum of Understanding or a Liaison Agreement.

A Memorandum of Understanding on SIENA would allow law enforcement authorities from Singapore to connect with law enforcement agencies from over 70 countries. Under a Liaison Agreement, Singapore could second one or more liaison officers to Europol, adding to the current network of over 300 liaison officers from EU Member States, third countries, and international organisations hosted by Europol. (CR)

Eurojust

New National Member for Poland at Eurojust

At the beginning of January 2025, Mr *Paweł Wąsik* started his four-year mandate as the new National Member for Poland at Eurojust. Mr Wąsik's working experience at Eurojust dates back to 2016, when he joined the agency as assistant to the National Member for Poland. He also served as Deputy Head and Head of the Economic Crime Team at Eurojust. Prior to joining Eurojust, he had worked as a prosecutor in the Economic Crimes Department of the Circuit Prosecutor's Office in Poznan. Mr Wąsik succeeds Mr *Marius Skowronski*. (CR)

New Liaison Prosecutor for the United States at Eurojust

At the beginning of January 2025, Ms *Martyna Pospieszalska* took up her two-year mandate as the new Liaison Prosecutor for the USA at Eurojust. Prior to starting her new position, Ms Pospieszalska had worked as a trial attorney for the U.S. Department of Justice's Office of International Affairs (OIA), the United States' central authority, where she advised and assisted U.S. and foreign authorities on extraditions and requests for mutual legal assistance, with a particular focus on Europe. Ms Pospieszalska succeeds Mr *Philip Mirer-Singer*. She has been appointed for an initial term of two years. (CR)

Frontex

Frontex Reprimanded for Data Exchange with Europol

In early January 2025, the European Data Protection Supervisor (EDPS) reprimanded Frontex for failing to

comply with its Regulation (Regulation (EU) 2019/1896) when transmitting the personal data of suspects of cross-border crimes to Europol. During an audit (carried out in autumn 2022), the EDPS discovered that Frontex had systematically and proactively exchanged information with Europol – without any assessment of the necessity for such an exchange. The EDPS mainly focused on debriefing interviews by Frontex of individuals intercepted while crossing external borders. Specifically, according to the EDPS, Frontex did not assess whether the exchange of information with Europol on persons reported as suspects of cross-border crime was strictly necessary for Europol to fulfil its mandate, as required by the Frontex Regulation.

As Frontex stopped sharing information with Europol five days after the adoption of the EDPS's audit report and as the wrongdoing has not continued since then, the EDPS decided to let the matter rest at a reprimand. In the meantime, Frontex and Europol have begun to define criteria in order to assess whether the collection of certain information is strictly necessary for Europol to fulfil its mandate and to establish detailed rules for its exchange. (CR)

Specific Areas of Crime

Protection of Financial Interests

EU Budget 2025

On 27 November 2024, the European Parliament adopted the EU 2025 budget. The European Parliament and the Council agreed on the new annual budget within the multi-annual financial framework (MFF) for 2021–2027 on 16 November 2024. Total commitments are set at €192.76 billion and the total payments at €149.61 billion, excluding appropriations foreseen for special instruments outside the MFF 2021–2027. €800,5 million have been kept available under the expenditure ceilings of the current MFF, allowing the EU to react to unforeseeable needs.

The European Parliament successfully negotiated an additional €230.7 million in funding beyond the Commission's initial draft proposal. The money will support research, health, education, young farmers, coordination of social security schemes, crisis response to natural disasters, climate action, humanitarian aid, military mobility and border management. The agreement also secured additional staff and funds for the European Public Prosecutor's Office (EPPO) and Europol.

Compared to national budgets, the EU budget is relatively small. It has on average €160–180 billion annually in 2021–2027 and serves 27 countries with a total population of around 450 million. This is comparable to the national budget of Denmark, which serves 5.6 million people, and is about 30% smaller than the budget of Poland, which serves 38 million.

The 2025 EU budget is complemented by the NextGenerationEU, the EU's plan to recover from the COVID-19 pandemic (→eucrim 3/2021, 151). (TW)

Corruption

High-Risk Areas of Corruption in the EU: In-Depth Report Highlights Six Vulnerable Sectors

A comprehensive report released in November 2024 and commissioned by the European Commission has mapped and analyzed high-risk areas of corruption in the European Union. The study will feed the EU strategy against corruption, which is prepared by the Commission and will set out actions to prevent and fight corruption in high risk areas.

Produced in collaboration with Ecorys, the University of Gothenburg, and Local Research Correspondents on Corruption (LRCC), the study identified six sectors most susceptible to corruption on the basis of six main criteria: (1) they affect a broad cross-section of populations, communities, employees, and consumers across the EU; (2) have significant cross-border implications within the EU; (3) involve a wide range of public institutions, private companies, professions and disciplines; (4) feature most or all major forms of corruption; (5) have risen on the European and global anti-corruption agendas; and (6) interlink with other areas where corruption is commonplace and damaging.

➤ *Key findings: corruption in six high-risk sectors*

■ **Public procurement**

Public procurement represents one of the most corruption-prone activities, due to the vast sums of money involved (approximately €2 trillion annually in the EU). Corruption in this sector often takes the form of bribery, bid rigging, collusion, or embezzlement. The report highlights vulnerabilities stemming from complex processes, a lack of transparency, and close interactions between public officials and bidding companies. Corruption in public procurement undermines competition and efficiency, leading to substandard infrastructure, inflated costs, and misuse of taxpayer money.

■ **Healthcare**

Corruption in healthcare is a significant issue, given that the sector accounts for an average of 11% of EU Member States' GDP. It ranges from bribery and embezzlement in hospital administration to fraud in medical procurement and overpricing of pharmaceuticals. Vulnerabilities include weak regulatory oversight, opaque procurement processes, and reliance on global supply chains. With annual losses estimated at up to €56 billion due to corruption in healthcare, the report underscores the sector's critical need for enhanced governance and accountability.

■ **Finance**

The financial sector faces complex and widespread corruption risks, including money laundering, tax evasion, and fraud. The EU reportedly loses up to €1 trillion annually to tax-related crimes. Organized crime networks exploit regulatory gaps to launder illicit funds and facilitate tax evasion. Financial institutions also serve as both perpetrators and victims of corruption, as lax oversight and weak enforcement mechanisms exacerbate vulnerabilities.

■ **Defence and security**

Corruption in the defence and security sector is enabled by high levels of secrecy and vast budgets (approximately €250 billion annually in the EU). Issues include bribery in arms procurement, diversion of funds, and the illegal resale of weapons. The report emphasizes how such corruption not only weakens national security but also has cross-border implications, particularly in light of ongoing conflicts such as the war in Ukraine.

■ **Construction and infrastructure**

This sector contributes 5% to the EU's total gross value added and employs millions of people. Corruption is prevalent in contract awards, often resulting in unsafe infrastructure, inflated costs, and environmental harm. Up to 20% of construction costs in the EU may be lost to corruption, according to the report. It highlights the urgent need for better regulatory oversight and enforcement for large-scale infrastructure projects.

■ **Sports**

Corruption in sports is both financial and reputational, with issues ranging from match-fixing and illegal betting to fraud in major event procurement. While fewer than 1% of games are fixed, the financial scale of corruption is vast, particularly in football and tennis, where organized crime networks often operate. Corruption in sports erodes public trust and undermines the integrity of competitions, impacting fans and athletes alike.

➤ *Shared characteristics and challenges*

The study found commonalities across these sectors, including the widespread use of bribery, conflicts of interest, and exploitation of regulatory gaps. Weak institutional oversight, lack of transparency, and complex governance structures further enable corruption. Organised crime groups and professional enablers, such as lawyers and accountants, play a significant role in perpetuating these schemes.

➤ *Broader impacts of corruption*

Corruption undermines public trust in institutions, distorts resource allocation, and hinders economic growth. Financial losses are only one part of the problem — corruption also has severe societal consequences, including reduced access to quality healthcare, unsafe infrastructure, and diminished faith in democratic processes. The report cautions that unchecked corruption will continue to harm EU citizens and weaken governance across Member States.

➤ *Recommendations for the EU*

To address these risks, the report calls for the following:

■ Enhanced oversight: Strengthening monitoring mechanisms in high-risk sectors, particularly in public procurement and defence;

■ Transparency and accountability: Improving access to information and enforcing stricter disclosure requirements;

■ Cross-border cooperation: Establishing robust mechanisms for judicial and investigative collaboration among Member States to combat transnational corruption;

■ Certification and standardization: Creating EU-wide standards for high-risk areas, such as healthcare procurement and managed security services;

■ Capacity building: Increasing resources for anti-corruption agencies and fostering public-private partnerships to detect and deter corruption.

The report underscores the importance of a coordinated EU Anti-Corruption Strategy to address systemic vulnerabilities in these six high-risk sectors. By closing regulatory gaps, improving enforcement, and enhancing transparency, the EU can significantly reduce the impact of corruption, safeguarding its institutions and citizens. (AP)

Money Laundering

ECJ Ruled on Concept of "External Accountants" in AML Directive

On 5 December 2024, the ECJ delivered a ruling on the personal scope of application of the fourth Anti-Money Laundering Directive (Directive (EU) 2015/849). The underlying Latvian proceedings concerned the question of whether a company (a legal person) that provides accounting services for entities affiliated with it can be considered an "external accountant" within the meaning of Art. 2(1)(3)(a) of the Directive. If the answer was in the affirmative, the company would be subject to the duties of prevention and due diligence provided for in the Directive and would therefore also be exposed to possible sanctions in the event of non-compliance. The case is referred as C-3/24 (MISTRAL TRANS).

The ECJ explained that, according to the usual meaning of the term in everyday language, the context in which it occurs and the purpose of the provision, the term "external accountants", within the meaning of Article 2(1)(3)(a) of Directive 2015/849, covers natural or legal persons whose professional activity consists in independently providing accounting services, such as the preparation, keeping or auditing of accounts, to third parties. This does not apply to the Latvian company in the main case.

It took over the bookkeeping for its affiliated companies in order to pool resources and its main activity is the business of transporting goods. (TW)

Tax Evasion

FASTER Directive on Excess Withholding Taxes Published

On 10 January 2025, Council Directive (EU) 2025/50 on faster and safer relief of excess withholding taxes was published in the EU's Official Journal L, 2025/50. The new rules make withholding tax procedures in the EU more efficient, secure and simplified for investors, financial intermediaries and Member State tax administrations. The Directive is seen as a key initiative to ensure fair taxation and to prevent that refund procedures can be abused, as done in the Cum/Ex and Cum/Cum scandals that led to estimated tax losses of €150 billion between the years 2000 and 2020.

In order to strengthen Member States' ability to prevent and fight tax fraud and tax abuse, which is currently hampered by a general lack of reliable and timely information on investors, the Directive provides for a common framework for the relief of excess withholding taxes on cross-border investments in securities. This leads to convergence among the various relief procedures applied in the Member States while ensuring transparency and certainty with regard to the identity of investors for securities issuers, withholding tax agents, financial intermediaries and Member States. To that effect, the framework relies on automated procedures, such as the digitalisation of the tax residence certificate in terms of both procedure and form.

Overall, the new withholding tax framework will grant investors access to fast-track procedures, ensuring the tax rights they are entitled to and avoiding double taxation. Tax authorities will have full visibility of the financial chain through new, standardised reporting obligations. These will enable the tax authorities to check whether investors are eligible for reduced rates and to ensure that a withholding tax refund is correctly granted.

Member states will have to transpose the Directive into national legislation by 31 December 2028, and national rules will have to become applicable from 1 January 2030. (TW)

ECA Report: Still Gaps in Fight against Harmful Tax Regimes

The EU's fight against harmful tax practices and cooperate tax avoidance has gaps. This is the result of a special report published by the European Court of Auditors (ECA) on 28 November 2024.

ECA's audit assessed the appropriateness of measures and mechanisms employed in the EU by both the Commission and five EU Member States (Ireland, Cyprus, Luxembourg, Malta, and the Netherlands). In particular, the ECA focused on the design and implementation of the following three directives that seek to curb harmful tax practices: the Anti-Tax Avoidance Directive, the 5th amendment to the Directive on administrative cooperation in the field of taxation (DAC 6) and the Directive on Tax Dispute Resolution Mechanisms. The audit covered the period from 2019 to 2023.

Overall, the ECA found that the established EU framework serves as a necessary first line of defence to support the fight against harmful tax regimes and corporate tax avoidance within the limited scope of the EU's competences in matters of direct taxation. However, there are shortcomings in the way EU measures were drawn up and implemented, and there is no appropriate monitoring system for assessing their effectiveness. Other problems identified include the following:

- Lack of guidance from the part of the Commission which would clarify the application of the EU rules in practice;
- Failure of checks whether defensive measures bear fruit;
- Since comprehensive evaluations of all three directives are overdue, it remains unclear whether they have been able to achieve their goals;
- Although Member States have tools available for exchanging information on potentially harmful cross-border tax arrangements, they carry out few quality checks on reported information and make little use of the information received, which makes the fight against revenue-escaping taxation less effective;
- In some Member States, the penalty systems for not complying with reporting obligations may not have a dissuasive effect due to the manifestly low level of the related penalties;
- There is no uniform approach among Member States to take defensive measures against non-cooperative jurisdictions outside the EU.

Although the Commission's powers in the audited field is limited, the ECA recommend that the Commission should do the following:

- Clarify the EU legislative framework;
- Improve the quality of DAC 6 reports;
- Ensure that the impact of penalties is adequate;
- Enhance its support to the Code of Conduct Group (the EU's specialised body for business taxation);
- Monitor the results and impact of the fight against harmful tax regimes and corporate tax avoidance.

In response to the ECA's special report, the Commission announced guidelines to ensure a uniform interpretation of EU legislation and to evaluate existing legislation. Important ECJ case law, such as the judgments of 29 July 2024 (Case C-623/22, →eucrim 2/2024, 120–122) and of 26 September 2024 (Case C-432/32,

→eucrim 3/2024, 186–187) on reporting obligations under the DAC6 Directive, in which the Court strengthened the lawyer-client privilege, is to become part of the guidelines. (TW)

Organised Crime

Abuse of Legal Business Structures through Criminal Networks

On 18 December 2024, Europol published a report examining how criminal networks abuse legal business structures to strengthen their power and expand their criminal operations. The report titled "Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures" investigates the following questions:

- Which types of legal businesses are prone to criminal abuse or infiltration?
- Which organised crime activities are enabled by legal businesses?
- How legal businesses enable criminal activity?
- Where legal businesses are mainly abused?

It builds on the report "Decoding the EU's most threatening criminal networks" (→eucrim 1/2024 pp 31–32), which identified 821 criminal networks representing the highest threat to the EU's internal security.

The new report paints a worrying picture, identifying a vast scope for abuse of legal business structures (LBS) for illicit purposes by criminal networks spanning across all business sectors. 86% of the EU's most threatening criminal networks abuse LBS. According to the report, the criminal networks utilise these structures at all levels, from wholly-owned criminal enterprises to legitimate private sector firms that unwittingly facilitate illicit activities. The greatest threat concerns high-level infiltration or criminal ownership of legal business structures tailored to the requirements of the criminal activities and criminal actors. In addition, legal businesses are being misused to support all aspects of criminal operations, from committing and concealing crimes to laundering profits. Legal businesses facilitate criminal objectives across both online and offline environments, affecting all stages of the criminal process. Lastly, almost all criminal networks rely on LBS to sustain and expand their activities.

The report concludes that the misuse of LBS is a borderless phenomenon. In most cases, however, LBS need to be close to operations in order to be effective. Therefore, most of the exploited and infiltrated LBS used/abused by the EU criminal networks are located either in the EU itself, where all EU Member States are affected, or in the countries neighbouring the EU.

To counter the abuse of LBS, the report calls for a comprehensive, multi-layered strategy bringing together law enforcement, regulatory bodies, the private sector, international allies, and initiatives like the European Multidisciplinary Platform Against Criminal Threats (EMPACT). Reactive measures combined with proactive initiatives, such as the development of risk indicators to identify vulnerable companies susceptible to criminal interference, are seen as key to a successful response. (CR)

Environmental Crime

Directive on Ship-Source Pollution Amended

On 16 December 2024, Directive (EU) 2024/3101 of the European Parliament and of the Council of 27 November 2024 amending Directive 2005/35/EC as regards ship-source pollution and on the introduction of administrative penalties for infringements was published in the EU's Official Journal L, 2024/3101.

The Directive updates the 2005 legal framework and incorporates into Union law international standards on illegal discharges from ships at sea. It also aims to ensure that those responsible for such discharges are subject to dissuasive, effective and proportionate sanctions. The main features of the Directive are as follows:

- Alignment with the definition of the international convention for the prevention of pollution from ships (MARPOL) and extension of the 2005 Directive's scope to cover illegal discharges of harmful substances in packaged form, sewage, waste and discharged waters and residues from exhaust gas cleaning systems;
- Without prejudice to criminal penalties as laid down by Directive 2024/1203 (→eucrim 1/2024, 32–33), administrative penalties for the breach of defined acts of ship-source pollution are strengthened: they must take at least the form of fines imposed on the company of the ship held liable;
- National authorities are enabled to impose administrative sanctions to ship-source pollution incidents in all European seas in a dissuasive and consistent manner;
- The Directive lists the relevant circumstances of the infringement which the competent authorities must take into account when determining and applying the type and level of administrative penalty for a company or other legal or natural person found liable, such as:
  - the nature, gravity and the duration of the discharge;
  - the degree of culpability or fault of the responsible person;
  - the damage caused by the discharge to the environment or human health;
  - the financial capacity of the company or other legal or natural person liable;
  - the economic benefits generated;
  - the measures taken by the compa-

ny or other legal or natural person liable in order to prevent the discharge or mitigate its impact;
- the level of cooperation of the company with the competent authority;
- any previous ship-source pollution infringement by the company or other legal or natural person liable.

■ New rules on enforcement measures with respect to ships within a port of a Member State.

The Directive also includes provisions on the exchange of information and experience between the Member States and the Commission, with the assistance of the European Maritime Safety Agency (EMSA). In addition, the Commission is obliged to establish an electronic reporting tool, for the purposes of collection and exchange of information between Member States and the Commission on the implementation of the enforcement system provided for by the Directive.

Lastly, the Commission will, with the assistance of EMSA and in cooperation with Member States, facilitate the development of Member States' capabilities by providing, as appropriate, training to the authorities responsible for the detection and verification of infringements under the scope of this Directive and the enforcement of penalties or any other measures arising from such infringements.

Directive 2024/3101 entered into force on 5 January 2025 and Member States must transpose it by 6 July 2027. (TW)

Illegal Employment

New Regulation Will Ban Products Made with Forced Labour from Union Market

On 12 December 2024, Regulation (EU) 2024/3015 of 27 November 2024 on prohibiting products made with forced labour on the Union market and amending Directive (EU) 2019/1937 was published in the Official Journal. The new legal framework will prohibit to place and make available on the EU market (including online sales), or to export from the EU market, any product made using forced labour.

The Regulation goes back to a Commission proposal from September 2022, after an announcement to this effect by President *Ursula von der Leyen* in her State of the Union speech on 15 September 2021. The initiative aims to effectively ban placement on the EU market and export from the EU of products made with forced labour, including forced child labour and thus to improve the functioning of the internal market. The European Parliament approved the Regulation in April 2024 after agreeing with the Council on amendments to the original proposal, clarifying the responsibilities of the Commission and national competent authorities in the investigation and decision-making process.

The Regulation applies to all economic operators, regardless of their size or turnover. Economic operators must implement a due diligence system to identify, prevent, mitigate, and eliminate the use of forced labour in their operations and supply chains. In this regard, the Regulation refers to existing regulations that establish due diligence requirements, such as Directive (EU) 2024/1760 on corporate sustainability due diligence, which entered into force on 25 July 2024.

The Regulation follows a risk-based approach. The Commission and national competent authorities must apply the following, specific criteria when assessing the likelihood of violations of the regulation, i.e. whether products were made with forced labour, so that they cannot be placed/made available on the Union market or not be exported:

■ The scale and severity of the suspected forced labour, including whether state-imposed forced labour may be a concern;

■ The quantity or volume of products placed or made available on the Union market;

■ The share of the parts of the product likely to be made with forced labour in the final product;

■ The proximity of economic operators to the suspected forced labour risks in their supply chain as well as their leverage to address them.

In order to enforce the Regulation, each EU Member State will designate competent authorities. These authorities will have powers to investigate, prohibit, and withdraw from the market any products suspected of being made with forced labour. Competent authorities are required to coordinate and exchange information with relevant national authorities and the competent authorities of other EU Member States. They must also work closely with the European Commission to ensure effective and uniform implementation across the EU.

The Commission will lead investigations outside the territory of the EU. Where the risks are located on the territory of an EU Member State, the competent authority of that Member State will lead the investigation. Before initiating an investigation, the lead competent authority may request information from the economic operators under assessment and, where relevant, other product suppliers, on the relevant actions they have taken in order to identify, prevent, mitigate, bring to an end or remediate risks of forced labour in their operations and supply chains with respect to the products under assessment. In exceptional situations the lead competent authority can also conduct field inspections.

The final decision to ban, withdraw, and dispose of a product made with forced labour will be taken by the authority that led the investigation. Any decision taken by a national authority will apply in all other EU Member States, based on the principle of mu-

tual recognition. Economic operators must comply with the order within given time limits (in principle, 30 working days; in the case of perishable products, animals and plants, the time limit may not be less than 10 working days).

In cases of supply risks of critical products made with forced labour, the competent authority can decide not to demand their disposal and instead order the economic operator to withhold the product until it can demonstrate that there is no more forced labour in its operations or respective supply chains. If only a part of the product is found to be in violation of the Regulation, the order to dispose of the product shall apply only to the part in question – if it is replaceable.

The Regulation also lays down the role of customs authorities and their cooperation with the competent national authorities. Customs authorities will support the enforcement of respective decisions on products that cannot enter or leave the Union market.

To help economic operators and competent authorities comply with the requirements of the Regulation, the Commission will issue guidelines, including best practices for bringing to an end and remediating different types of forced labour. These guidelines will also include accompanying measures for micro-sized, small, and medium-sized enterprises. Furthermore, to facilitate the implementation of the Regulation, the Commission will establish a database containing verifiable and regularly updated information about forced labour risks, including reports from international organisations (such as the International Labour Organization). The database will support the work of the Commission and national competent authorities in assessing possible violations of the Regulation. It will be hosted on the Forced Labour Single Portal – a digital platform slated to be operational by June 2026 and maintained by the European Commission – which will serve as a centralized hub for information and resources related to forced labour prevention in the EU market.

Regulation 2024/3015 entered into force on 13 December 2024 and will be applied from 14 December 2027. (CR)

Terrorism

Europol TE-SAT 2024

On 12 December 2024, Europol published its EU Terrorism Situation and Trend Report (EU TE-SAT). The report provides a detailed overview of the evolving terrorism landscape in the European Union in 2023: jihadist, right-wing/left-wing and anarchist terrorism, ethno-nationalist and separatist terrorism as well as other forms of terrorism and extremism. It also provides an outlook on potential developments. For the editions of previous years →eucrim 2/2023, 146 and →eucrim 2/2022, 111, each with further references.

In 2023, the terrorist attack by Hamas against Israel on 7 October 2023 and the ensuing Israeli military response in Gaza was a devastating event that generated additional movements in all violent extremist and terrorist ideological scenes. Furthermore, developments in Artificial Intelligence and other technological innovations are being added to the toolbox used by terrorists and violent extremists to amplify their messages and facilitate their operations. Large Language Models (LLMs) and deepfakes are being exploited to create false identities, spread disinformation, and bolster propaganda campaigns.

In 2023, a total of 120 terrorist attacks (98 completed, 9 failed, and 13 foiled) were carried out in seven EU Member States, marking an increase compared to previous years. 70 completed terrorist attacks were perpetrated by separatist terrorists and 23 completed terrorist attacks were perpetrated by left-wing and anarchist actors. Of the 14 jihadist terrorist attacks, five were completed and were also the most lethal, with six victims killed and twelve injured. Two right-wing terrorist attacks were foiled. EU law enforcement authorities arrested 426 suspects for terrorism-related offences (compared to 380 in 2023) in 22 EU Member States, of which 334 were related to jihadist terrorism. 290 convictions and 68 acquittals for terrorist offences were passed by courts in the EU Member States.

Looking at the different types of terrorism, the report finds that jihadist terrorism is a key security concern for the EU, arising from a fragmented landscape of foreign terrorist groups, online networks, and individual actors. Right-wing terrorism is seen as a dynamic threat, with lone actors or small groups posing the highest threat and new right-wing violent extremist groups emerging online and seeking to act in real life.

A notable new development is the purchase of 3-D printed materials, with individuals from a variety of ideological backgrounds actively seeking online training materials and instruction manuals that contain attack tactics and information on how to make weapons, drones, bombs, and chemical weapons. (CR)

Council Conclusions on Future Priorities to Counter Terrorism

On 12 December 2024, the Council approved the first of two sets of conclusions on strengthening the common effort to counter terrorism. These conclusions set out strategic objectives and highlight key areas where increased efforts are needed to improve operational effectiveness. The aim is to shape the EU's counter-terrorism policies and actions over the next five years. The Member States note that worldwide unrest has led to

an increased terrorist threat in some Member States, which contributes to increased radicalisation and social polarisation across the Union.

The Council calls on Member States to enhance their preparedness and response capabilities in order to prevent terrorist and violent extremist attacks. The conclusions consider the following three main areas of intervention for strengthening counterterrorism efforts:

- Exchange of information;
- Detection and prevention of the infiltration of persons posing a terrorist threat;
- Fight against terrorism and violent extremism online.

The conclusions make several recommendations to the Member States and the Commission. They, *inter alia*, call on Member States to continue entering alerts into the Schengen Information System based on return decisions and to effectively implement the return of persons posing a security threat. The Commission is called to strictly enforce the Digital Services Act to address the challenges posed by non-compliant online platforms. Looking at horizontal issues, the conclusions propose, among other things, increasing the involvement of counterterrorism authorities in the European Multidisciplinary Platform Against Criminal Threats (EMPACT). The Commission is invited to "develop an effective approach" for the implementation of the recommendations of the High-level Group on Access to Data for Effective Law Enforcement which address the law enforcement authorities' needs to access electronic communications (→news item above, pp. 270–271).

The conclusions of 12 December 2024 were complemented by conclusions of 16 December 2024 that emphasised the EU's future policy to reinforce the links between the common foreign security policy and justice and home affairs action (→next news item). (TW)

Council Conclusions on Reinforcing External-Internal Anti-Terrorism Connections

On 16 December 2024, the Council approved conclusions to step up the fight against terrorism and violent extremism. These build on the counter-terrorism priorities adopted on 12 December 2024 and other previous Council conclusions on the fight against terrorism (→previous news item).

The conclusions of 16 December 2024 stress the EU's determination to work with partner countries and protect citizens as well as the need to enhance links between external and internal aspects of the EU's counter-terrorism response. They include several proposals for measures that should be implemented by the EU Counter-Terrorism Coordinator, the High Representative, the Commission, and the Member States.

The Council highlights the increasing heterogeneity and fragmentation of the threat from terrorism and violent extremism, in particular from the Da'esh Khorasan Province (ISKP), which has an increasing ability to conduct external operations, including in Europe. The deteriorating security situation in Africa and the ongoing crisis in the Middle East are driving radicalisation worldwide. The Council reiterates the need to fight terrorism and violent extremism through a coherent approach involving both the EU's common foreign and security policy and justice and home affairs action.

The Council reaffirms that the only sustainable response to these threats is to be based on democracy, the rule of law, transparency, accountability and gender-responsiveness. It also emphasises the need for further investment in cooperation with third countries, in particular through dialogues and capacity-building projects. The full potential of the network of EU counter-terrorism/security experts must be harvested. Lastly, the Council calls for Team Europe initiatives to make the EU's efforts in the fight against terrorism even more effective and better coordinated. (TW)

Procedural Law

Procedural Safeguards

ECJ Rules on Conditions for *in absentia* Judgments

In its judgment of 16 January 2025, the ECJ ruled on the compatibility of national provisions with the requirements for criminal proceedings *in absentia* set out in EU Directive 2016/343. Specifically, the judgment concerns the compatibility of the provisions in the Bulgarian Code of Criminal Procedure regarding the possibility of conducting criminal proceedings in the absence of the defendant (Case C-400/23, *VB II*).

➤ *Facts and background of the case*

In the underlying case, the referring Bulgarian court is conducting criminal proceedings against VB. However, VB has fled the proceedings and, despite a search having been launched, has not yet been found. He is accused of being a member of an organised criminal group that trades in narcotics and is in the possession of weapons.

The Bulgarian court found that VB had not been formally informed of the charges against him; he has also not been informed either that his case has been brought before a court, or, a fortiori, of the date and place of the trial or of the consequences of his non-appearance. Thus, the requirements of Art. 8(2) of Directive 2016/343, which allow for the implementation of proceedings *in absentia*, were not met. This circumstance led to an initial reference for preliminary ruling in 2022. In its judgment of 8 June 2023, the ECJ answered in the negative the question of whether the national court would be obliged, in the event of a conviction *in absentia*, to make express reference to the right to a new trial in

the judgment convicting the person concerned (Joined Cases C-430/22 and C-468/22, *VB I*).

With the second referral in the proceedings, the Bulgarian court wants to ensure that the continued criminal proceedings *in absentia* against VB are in line with the requirements of EU law, in particular Art. 8(4) and Art. 9 of Directive 2016/343. In this context, the Bulgarian court pointed out two circumstances in particular:

- First, it is unclear under Bulgarian law to which extent the person concerned must be informed about the decision by which he was convicted *in absentia*, in particular whether a copy of the full decision rendered *in absentia* must be provided to the person concerned at the time of his apprehension.
- Secondly, under Bulgarian law, the only way to obtain a new trial is to file an application for a retrial of the criminal proceedings. However, this application must be filed with the *Varhoven kasatsionen sad* (Supreme Court of Cassation) and not with the criminal court that rendered the decision *in absentia*; additonally: the application will only be considered if the person concerned appears personally before the Supreme Court of Cassation.

The referring court doubts whether this procedure is compatible with EU law. Furthermore, the court raised the question of the procedural modalities if it were to decide itself on compliance with the conditions of Art. 8(2) of the Directive, as well as the question of whether the information obligations and the right to a new trial under the Directive also apply in the case of an acquittal.

➤ *The ECJ's ruling with regard to the in absentia procedure*

First of all, the ECJ states that Directive 2016/343 does not preclude a Member State from introducing a procedural regime which does not automatically lead to the reopening of criminal proceedings, but which requires persons convicted *in absentia* and interested in such reopening to make an application to that effect before another court, distinct from the court which handed down the decision *in absentia*. However, the ECJ clarifies that proceedings before the court deciding on a new trial must observe the principles of equivalence and effectiveness. The latter condition requires, *inter alia*, that the proceedings relating to the request for a new trial allow in fact such a trial to be held in all cases where it is established, after verification, that the conditions laid down in Art. 8(2) of Directive 2016/343 were not satisfied. By contrast, the requirement of effectiveness is not satisfied where the person requesting a new trial is required to appear in person before the court having jurisdiction, failing which his/her request will be rejected without further action being taken.

Regarding the extent of information, the judges in Luxembourg state that it must be ascertained whether the person convicted *in absentia* receives, at the time when he is informed of the existence of the conviction or promptly thereafter, a copy of the entire decision rendered in absentia as well as easily understandable information on his procedural rights, including the possibility of applying to reopen the criminal proceedings and the court before which and the time limit within which such an application must be made.

➤ *The ECJ's position on the obligation to inform*

As regards the obligation to inform a person tried in absentia of his right to a retrial, the ECJ points out that the Union legislature has refrained from specifying the manner in which information relating to the "right to a retrial or to another legal remedy" must be provided. While Directive 2016/343 cannot be interpreted as requiring the court adjudicating *in absentia* to rule in its decision on the right to a retrial, it leaves a wide margin of discretion to the Member States as to its implementation. Nor, therefore, can it be interpreted as prohibiting that court from examining, in the course of a trial conducted *in absentia*, whether the conditions laid down in Art. 8(2) are met and, where those conditions are not met, from stating in its decision that the person concerned is entitled to a retrial. The requirements imposed by Directive 2016/343 are thus met where the court conducting a trial *in absentia* itself assesses, after hearing both the prosecution and the defence on the matter, whether the conditions laid down in Art. 8(2) of the Directive are met and, if not, indicates in the decision rendered *in absentia,* a full copy of which must be given to the person concerned when he is informed of that decision or promptly thereafter, that he is entitled to a retrial.

➤ *Application for acquittals*

Lastly, the ECJ ruled that the second sentence of Art. 8(4) and Art. 9 of Directive 2016/343 must be interpreted as applying not only in the event of a conviction *in absentia*, but also in the event of an acquittal *in absentia*. Reading the provisions in the context of Art. 8(2), the decision, resulting from criminal proceedings, relates both to the guilt *or innocence* of the accused person. (TW)

ECJ Ruled on Right to New Trial if Suspect Absconds

In its judgment of 17 January 2025 in Case C-644/23 (*IR II* or *Stangalov*), the ECJ explained the extent to which the conditions for conducting proceedings *in absentia* within the meaning of Directive 2016/343 are met. Specifically, the issue is the compatibility of provisions of the Bulgarian Code of Criminal Procedure with Articles 8 and 9 of the Directive. In the underlying proceedings of the reference for preliminary ruling, the ECJ had already ruled in the same case in 2022 (Case C-569/20, *IR* →eucrim 2/2022, 112–113). However, the referring Bulgarian criminal court had a need for further clarification and, in

particular, wished to establish whether the continuation of the proceedings against the defendant *in absentia* under the provisions of the Bulgarian Code of Criminal Procedure (NPK) was in line with EU law.

➤ *Facts and background of the case*

The underlying case concerns the conduct of criminal proceedings against IR for acts that may constitute tax offences punishable by custodial sentences. According to the findings of the referring court, IR received a "notice of charges" in the investigative proceedings under Bulgarian law. This notice contains only a brief statement of the facts and points of law in order to inform a suspect that he is being accused of a particular offence and he is given the opportunity to provide explanations in that regard. Incriminating and exculpatory evidence is not known at this stage, nor is the decision of the public prosecutor to draw up the indictment within the meaning of Article 246 of the NPK and thus bring the criminal case before the competent criminal court. However, the summons to the trial and a copy of the indictment could no longer be served on IR because he had fled. Although a lawyer was officially appointed by the court during the criminal proceedings, he had no contact with the defendant IR.

In light of this, the referring court is primarily concerned with the question of whether the requirements of Art. 8(2) of Directive 2016/343 are met, in particular Art. 8(2)(a), namely whether the suspect or accused person was informed in due time of the trial and of the consequences of non-appearance. If so, a person convicted *in absentia* can be derived of his/her right to a new trial.

➤ *The ECJ's reply*

The ECJ first of all made it clear in general terms that when determining whether the person was informed of the trial, particular attention must be paid to the diligence exercised by the public authorities in informing the person concerned of the trial and the diligence exercised by the person concerned in receiving the relevant information. Consequently, that person must be presumed to have no right to a new trial if it is apparent from precise and objective indicia that he or she, while having been officially informed that he or she is accused of having committed a criminal offence, and therefore aware that he or she is going to be brought to trial, takes deliberate steps to avoid receiving officially the information regarding the date and place of the trial.

In accordance with the case law of the ECtHR, it is sufficient for the finding that the person concerned has absconded from justice if he or she had learned that his or her criminal case would in all likelihood be brought to court. In the view of the ECJ, it is sufficient for this to have received the notice of charges in the pre-trial stage, as in the present case. By absconding after having received this notice, IR has thus prevented the competent authorities from informing him in person of the final indictment and of the date and place of the trial. This may result in IR being denied a new trial if he is located and arrested to serve his sentence imposed *in absentia*.

However, the ECJ makes an important reservation: the forfeiture of the right to a new trial must be limited to persons who, first, may be presumed, having regard to all the relevant circumstances, to have been informed of their trial and, second, were represented at the trial by a lawyer mandated by them in their absence or, if there was no such representation, were informed in due time that, if they absconded, they risk being tried in their absence.

It is for the referring court to examine whether those conditions have been met under Bulgarian law. Nonetheless, there are doubts as to whether the information on the consequences of non-appearance was provided in good time. At the very least, as in the present case, it cannot be assumed that the court-appointed lawyer was "mandated" if he has no contact with the defendant.

Note: Several proceedings are pending before the ECJ regarding the compatibility of Bulgarian law on *in absentia* proceedings with Directive 2016/343. On 16 January 2025, the ECJ ruled on a somewhat different case concerning *in absentia* proceedings in Bulgaria (*Case C-400/23, VB II* →previous new item). In this case, the Bulgarian court asked on the continuation of *in absentia* proceedings if the requirements of Art. 8(2) of Directive 2016/343 were not met. Here, too, the case was a second referral for a preliminary ruling in a case that had been decided upon previously (Joined Cases C-430/22 and C-468/22, *VB I*). (TW)

Data Protection

ECJ: Police Must Perform Necessity Test Before Sensitive Data Are Collected

On 28 November 2024, the ECJ ruled on the role of the competent authorities in deciding on the "strict necessity" of processing sensitive data in accordance with Art. 10 of Directive 2016/680 – the Law Enforcement Data Protection Directive. The referral concerns Bulgarian law, which provides that, for the purpose of a police record, the systematic collection of biometric and genetic data of all persons accused of an intentional offence subject to public prosecution is permitted without the Bulgarian police having to examine whether first the data collection is necessary for achieving the specific objectives pursued and, second, that those objectives cannot be achieved by collecting only a part of the data concerned .

In its judgment of 26 January 2023 in Case C-205/21 (→eucrim 32–33), the ECJ ruled that Bulgarian law only

complies with EU law if it is ensured that the processing of the special categories of data referred to in Art. 10 of the Directive is permitted "only" where it is "strictly necessary". In the now renewed reference for preliminary ruling in the same case, the competent Bulgarian criminal court asked for clarification as to how and on what material basis it must implement this requirement (Case C-80/23, *V.S. II*).

The ECJ replied that it is up to the competent authority (in the Bulgarian case: the police) to make the assessment required under Art. 10. The court seised by that competent authority for the purpose of the enforcement of the data collection cannot ensure the necessary legal protection if the obligation has not been imposed on the competent authority. (TW)

Victim Protection

Key Challenges for Effective Response to Victims of Crime

On 28 November 2024, the EU Agency for Fundamental Rights (FRA) published a paper titled "Stepping up the response to victims of crime: FRA's findings on challenges and solutions."

The paper outlines the main challenges and solutions in promoting and protecting victims' rights across the EU and provides an overview of all relevant FRA research on victims, with examples of relevant FRA opinions. It also briefly explains the legal framework for victims' rights in the EU, which consists of EU primary law and Art. 47 of the Charter (giving victims the right to an effective remedy and fair trial) as well as EU secondary law and the Victims' Rights Directive. The latter grants a wide range of rights to all victims of crime to ensure that they receive appropriate information, support, protection, and are able to effectively participate in criminal proceedings. Legislative amendments to establish more far-reaching minimum standards under the Victims' Rights Directive are currently under discussion (→eucrim 2/2023, 158). In addition, sector-specific Directives, such as the Directive to combat violence against women and domestic violence, focus on selected categories of victims by introducing additional safeguards.

The FRA paper looks at three main areas in which measures are needed:

- To facilitate reporting by victims and to avoid underreporting;
- To protect against secondary victimization;
- To guarantee effective victim support services.

According to the paper, there is a need to step up the response to victims of crime who suffer from the severe and lasting negative consequences caused by ineffective responses by Member States' authorities. To find solutions, the paper therefore draws on practices in various EU Member States that have proven effective in meeting the practical needs of victims and improving their access to rights.

Effective solutions to counter underreporting include alternative ways for victims to report crime, such as third-party reporting and proactive monitoring. Third-party reporting allows victims, family members, and witnesses to inform an appropriately trained third party about a crime. With the victim's consent, this third party can report the crime to the police without the victims having to be in direct contact with the police themselves. Proactive monitoring targets victims that live in situations controlled by others, with little chance to inform the police about their victimisation. Such situations may arise in institutions (e.g., involving children, the elderly, prisoners, and people with disabilities) or in situations of isolation (e.g., victims of labour exploitation or human trafficking). Proactive monitoring by independent authorities can help such victims report crimes.

Effective solutions to prevent secondary victimisation include a variety of measures, such as the *Barnahus* model, in which those responding to victims receive special training, follow evidence-based protocols, and have their interviews observed by members of a multidisciplinary team.

To ensure effective victim support, the paper suggests services that provide free and appropriate support in a manner that respects the victims' right to equal treatment: taking measures to establish effective coordination between victims support services, introducing a system of accreditation, and standardised referral mechanisms.

Lastly, when looking at emerging challenges, the paper highlights the increasing impact of online crime on victims and confirms FRA's intention to expand its research and knowledge base to inform EU and national policy- and lawmaking on victims' rights in this area. (CR)

Cooperation

Judicial Cooperation

Regulation on the Transfer of Criminal Proceedings Published

spot light

On 18 December 2024, Regulation (EU) 2024/3011 of the European Parliament and of the Council on the transfer of proceedings in criminal matters was published in the EU's Official Journal L 2024/3011. The Regulation lays down rules on the transfer of criminal proceedings between the EU Member States with a view to improving the efficient and proper administration of justice within the common area of freedom, security and justice. It applies in all cases of transfer of criminal proceedings conducted in Member States, including Ireland (which opted in), but except Denmark (which is not part due to its opt-out in the EU's justice and home affairs policies).

The main aim of the Regulation is that the best-placed Member State investigates and prosecutes a criminal offence, thus preventing unnecessary parallel criminal proceedings in different EU Member States. It also aims that criminal proceedings can take place if the surrender of a person for criminal prosecution is delayed or refused pursuant to the Framework Decision on the European Arrest Warrant, thus avoiding impunity.

The Regulation was proposed by the European Commission on 5 April 2023 (→eucrim 1/2023, 40) and a political agreement between the European Parliament and Council was reached in March 2024 (→eucrim 1/2024, 38–39). The legal act was finally signed on 27 November 2024. The following summarises the main elements of the Regulation.

➤ *Jurisdiction*

In order to ensure that it is possible for criminal proceedings to be transferred in accordance with the Regulation, the Regulation establishes jurisdiction in specific cases so that the requested State is able to exercise jurisdiction in relation to the criminal offences to which the national law of the requesting State is applicable. Jurisdiction is, for instance, established in situations in which the execution of a European Arrest Warrant is refused, if the criminal offence produces its effects or causes damage mainly in the requested state, and when criminal proceedings against the suspect or accused person are already ongoing.

➤ *Entitlements for requests*

A request for a transfer of criminal proceedings can be issued by an authority in a EU Member State in which criminal proceedings are being conducted (the requesting authority) either on its own initiative, or after consultations with an authority in a Member State which is to take over those proceedings (requested authority). A request can also be proposed by a suspect/accused person, or by a victim. The proposal can be made to the competent authorities of the requesting or the requested State. Such proposals, however, do not impose an obligation for the requesting authority to file a request or to consult the authority in the requested State.

➤ *Criteria for the transfer*

A a general rule, the Regulation clarified that a request for the transfer of criminal proceedings may be issued only where the requesting authority considers that the objective of efficient and proper administration of justice, including proportionality, would be better served by conducting the relevant criminal proceedings in another Member State. When considering whether to request the transfer of criminal proceeding, the requesting authority needs to take into account, *inter alia*, the following criteria:

- The criminal offence has been committed on the territory of the Member State to which the proceedings are to be transferred or most of the effects of the offence or a substantial part of the damage occurred in that Member State;
- One or more suspects or accused persons are nationals of or residents in the Member State to which the proceedings are to be transferred;
- One or more suspects or accused persons are present in the requested State and that State refuses to surrender those persons for whom a European arrest warrant has been issued, if it finds that there are, in exceptional situations, substantial grounds to believe, on the basis of specific and objective evidence, that surrender would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Art. 6 TEU and the Charter of Fundamental Rights of the EU;
- Most of the evidence relevant to the investigation or the majority of the relevant witnesses are located/reside in the requested Member State;
- There are ongoing criminal proceedings in respect of the same or other facts against the suspect or accused person in the Member State which would become responsible for the proceedings;
- The enforcement of the sentence in the requested State is likely to improve the prospects of social rehabilitation of the person sentenced or enforcement of the sentence in the requested Member State would be more appropriate due to other reasons;
- One or more victims are nationals of or residents in the requested State.

➤ *Procedure*

The request for the transfer of criminal proceedings must be drawn up by the requesting authority using the standardised form annexed to the Regulation and the request must be duly substantiated. The Regulation lays down the pieces of information that the request must contain, the documents to be accompanied and the modus operandi of the transmission.

➤ *Refusal*

The Regulation lays down mandatory and optional grounds for which the requested authority can refuse the transfer of criminal proceedings.

A mandatory ground is, for example, if the conduct, for which the transfer is sought, is not a criminal offence in the requested State. In addition, a request has to be refused if the taking over of criminal proceedings would be contrary to the principle of *ne bis in idem* or the suspect/accused person cannot be held criminally liable due to his/her age.

Importantly, a mandatory refusal ground also applies if the conditions for prosecuting the criminal offence in the requested State are not fulfilled. This could be the case, for example, if a complaint by the victim, which is necessary for prosecuting the criminal offence in the requested State, has not been filed in time.

Optional refusal grounds include, *inter alia*, if the suspect/accused person benefits from a privilege or immunity

under the national law of the requested State, and if the requested authority believes that the transfer at issue is not justified in the interests of efficient and proper administration of justice.

➤ *Time limit*

The requested authority will communicate on whether to accept or refuse the transfer of criminal proceedings without undue delay and in any case no later than 60 days after the receipt of the request for the transfer of criminal proceedings. The time limit set may be extended once by a maximum of 30 days.

➤ *Rights of the suspect/accused person and victim*

The country in which the criminal investigation is taking place and which wishes to transfer the proceedings to another country must, for instance, give due consideration to the legitimate interests of the suspect or accused person as well as the victim. In addition, the suspect/accused and the victim must be informed about the intention to transfer proceedings and should be given the opportunity to provide an opinion about this transfer. They are furthermore informed during other relevant phases of the procedure.

➤ *Right to an effective legal remedy*

Suspects, accused persons and victims must have the right to an effective legal remedy in the requested State against a decision to accept the transfer of criminal proceedings. The right will be exercised before a court or tribunal in the requested State. The time limit for seeking the remedy will be no longer than 15 days from the date of receipt of the reasoned decision to accept the transfer of criminal proceedings. The final decision on the legal remedy must be taken without undue delay and, where possible, within 60 days.

The recitals of the Regulation clarify that the requested authority has a broad discretion in assessing whether the transfer of criminal proceedings is in the interests of efficient and proper administration of justice and whether the request should be refused on any of the optional grounds for refusal. Thus, the judicial review should be restricted as to whether the limits of discretion have been manifestly exceeded. In addition, the legal remedy should not entail any review of the merits of the case, such as whether the evidence is sufficient to justify opening or continuing an investigation, whether the elements of the offence are established, or whether statements had been credible.

➤ *Effects of the transfer in the requesting State*

The acceptance of the transfer of criminal proceedings by the requested authority should result in the suspension or discontinuation of criminal proceedings in the requesting State. The latter can, however, undertake necessary urgent investigative or other procedural measures, including measures to prevent the suspect or accused person from absconding or freezing measure. The Regulation also allows the requesting State to continue or reopen criminal proceedings if the requested authority decided to discontinue criminal proceedings related to the facts underlying the transfer, under the condition that this would not entail a violation of the *ne bis in idem principle* in Arts. 54/55 CISA and Art. 50 CFR, as interpreted by the CJEU.

➤ *Effects of the transfer in the requested State*

Once criminal proceedings are transferred in accordance with the Regulation, the requested authority applies its relevant national law and procedures. In particular, it maintains any prosecutorial discretion provided for in national law.

Provided that it is not contrary to the fundamental principles of law of the requested State, any act carried out for the purposes of the criminal proceedings or preparatory inquiries performed by competent authorities in the requesting State shall have the same validity in the requested State as if it had been validly performed by competent authorities in the requested State. Furthermore, any act validly performed in the requesting State that interrupts or suspends the period of limitation shall have the same effect of interruption or suspension of the period of limitation in the requested State provided that such act would have that effect under its national law.

The Regulation clarifies that evidence gathered in the requesting State may be used in criminal proceedings in the requested State, provided that the admissibility of such evidence is in accordance with the national law of the requested State, including its fundamental principles of law. The power of the trial court to freely assess the evidence is not affected by the Regulation.

Regarding sentencing, the Regulation provides that in cases where the criminal offence was committed on the territory of the requesting State, the requested authority *may* take into consideration, in accordance with applicable national law, the maximum sentence under the national law of the requesting State, where to do so would be to the benefit of the accused person. The maximum sentence provided for in the national law of the requesting State should always be taken into account where jurisdiction of the requested State is based exclusively on the Regulation (see above).

➤ *Cooperation and communication*

The requesting authority and the requested authority may, at any stage of the procedure for the transfer of criminal proceedings, request the assistance of Eurojust or the European Judicial Network in accordance with their respective competences. In order to ensure swift, direct, interoperable, reliable and secure exchange of case-related data, including the exchange of the request form, communication under the Regulation between

the involved authorities should, as a rule, be carried out through a decentralised IT system. The Commission is tasked with establishing the IT system by 8 January 2027.

➤ *Next steps*

Regulation (EU) 2024/3011 entered into force on 7 January 2025 and applies from 1 February 2027. The Regulation will then replace the corresponding provisions in the respective Council of Europe Conventions which are applicable between the Member States bound by the Regulation. This framework will govern requests for the transfer of criminal proceedings received before 1 February 2027. (TW)

European Investigation Order

ECJ Ruled on Material Scope of EIO Directive

On 9 January 2025, the ECJ rendered a judgment on the material scope of Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO Directive). The ECJ had to decide whether French authorities were to refuse the execution of a Spanish order that requested first to serve on an accused person an indictment related to her, accompanied by an order that that person be remanded in custody and make a bail payment and, second, to allow that person to make observations on the matters set out in that indictment (Case C-583/23, *Delda*).

In essence, the ECJ had to define the concept of "investigative measure" for law enforcement purposes within the meaning of Arts. 1 and 3 of Directive 2014/41. Considering the wording of the term, its context and the purpose of the EIO, the ECJ clarified that the investigative measure must aim to ensure that the issuing Member State obtains "evidence". And evidence is identified as objects, documents or data pursuant to the EIO Directive.

In application of this definition, the ECJ concludes that neither an order by which a judicial authority of one Member State requests a judicial authority of another Member State to serve on a person an indictment relating to him/her nor an order to request a judicial authority of a Member State to remand a person in custody pending trial or to require the person concerned a bail payment, does constitute a European Investigation Order. An order by which a judicial authority of a Member State requests a judicial authority of another Member State to allow a person to make observations on the matters set out in the indictment relating to him/ her constitutes a European Investigation Order, in so far as that request for a hearing is intended to gather evidence. It had been up to the French authorities to check this intention with the issuing Spanish authority. If the Spanish authority had no objection, the request could have been partly executed. (TW)

e-Evidence

CCBE: Recommendation to Ensure Lawyers' Interests in Implementation of e-Evidence Regulation

On 21 November 2024, the Council of Bars and Law Societies of Europe (CCBE) issued recommendations on the implementation of the e-evidence Regulation (Regulation 2023/1543, →eucrim 2/2023, 165–168). They focus on issues which are both relevant and of importance to Bars and the legal profession. They aim at assisting Bars in their engagement with their respective Ministries during the national implementation process.

The Regulation, which was adopted on 12 July 2023, makes it possible to request electronic evidence directly from service providers in other Member States in criminal proceedings ("production order") or to request its preservation ("preservation order"). Lawyers can also request such orders on behalf of their clients. The CCBE emphasises two key areas for action:

- Clear procedures must be created for lawyers to request such orders;
- Lawyer-client confidentiality, as understood and protected at national level, must be effectively protected.

On the latter point, the CCBE recommends that the Bars must consider with their appropriate authorities how service providers manage information about the privileged nature of the data and are informed about the possibility to refuse orders if protected information is involved. In addition, it must be ensured that service providers service providers will be informed about the extent of lawyer-client privilege in the Member State, and to whom it applies (i.e. lawyers).

Given that the e-evidence Regulation applies from 18 August 2026, the CCBE recommends the Bars to begin a dialogue urgently with the relevant competent authorities in their own Member State, to take up the issues raised. (TW)

Sixth SIRIUS Report

At the end of November 2024, Eurojust, Europol, and the European Judicial Network (EJN) published the 2024 edition of the SIRIUS European Union (EU) Electronic Evidence Situation Report. The report provides an overview of the electronic evidence landscape in the EU from the perspective of law enforcement, the judiciary, and service providers – based on surveys and dedicated interviews (for the 2023 edition →eucrim 1/2024, 44–45). It also makes a series of recommendations aimed at improving existing processes and at preparing for the application of new rules in the future. In particular, this sixth edition focuses on the benefits and challenges of the new legal instruments in the EU e-evidence legislative package (→eucrim 2/2023, 165).

Challenges identified from a law enforcement perspective include lengthy

judicial cooperation procedures and the fragmentation of companies. With regard to the e-evidence package, law enforcement authorities raise questions about the lack of clarity in key concepts, the precise scope or providers covered, and the potential transformation of their roles. Future concerns relate to the potential misuse of AI-related technological developments. The report therefore makes the following recommendations to EU stakeholders/EU law enforcement agencies:

- Prepare for and adapt to the EU e-evidence legislative package;
- Broaden training efforts on cross-border access to electronic evidence covering current frameworks and future developments;
- Reinforce the approach of Single Point(s) of Contact (SPoC) and ensure active engagement with the SIRIUS SPoC Network.

Judicial authorities in the EU are hoping to see progress towards the introduction of the EU e-evidence legislative package and the Second Additional Protocol to the Budapest Convention on Cybercrime (→eucrim 2/2022, 128) – in order to create more robust and streamlined mechanisms for cross-border access to electronic evidence. However, the absence of a data retention framework for law enforcement purposes, which has not been addressed by the new legal framework, is considered highly problematic. The report also underlines the importance of continuous capacity building on both existing and forthcoming data acquisition modalities to enable EU judicial authorities to navigate the complex legal landscape and maximise the benefits of the new instruments for effective cross-border access to electronic evidence. EU stakeholders/EU judicial authorities were given the following recommendations:

- Enhance knowledge and capacity on available legal instruments for cross-border access to electronic evidence;
- Prepare judicial authorities to effectively use new instruments under the upcoming EU e-evidence legislative package and manifest other legislative changes concerning the cross-border acquisition of electronic evidence;
- Strengthen mutual trust and knowledge sharing among EU judicial practitioners on the cross-border gathering of electronic evidence.

Service providers confirmed the importance of SPoCs. The main concern for service providers is the planned decentralised IT system for secure digital communication and data exchange. Recommendations for stakeholders in relation to service providers therefore include preparing for compliance with the EU e-evidence legislative package, sharing early updates with EU authorities, and engaging closely and sharing updates with the SIRIUS Project Team.

Lastly, the report recommends that actors implementing the EU e-evidence legislative package at the EU and Member State levels should engage with the greater community of EU competent authorities and service providers and call in SIRIUS' experience by involving it early in implementation. (CR)

Law Enforcement Cooperation

New Legal Framework on Collection and Transmission of Advance Passenger Information for Law Enforcement Purposes

spot light

On 8 January 2025, the new legal EU framework on the collection and transfer of advance passenger information (API) for border control and law enforcement purposes was published in the EU's Official Journal. The legislative package consists of two regulations:

- Regulation (EU) 2025/12 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC, OJ L, 2025/12;
- Regulation (EU) 2025/13 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818, OJ L, 2025/13.

The new legal framework was proposed by the Commission in December 2022 (COM(2022) 729 final and COM(2022) 731 final). The need for two different legal instruments is due to the different legal basis: Arts. 77(2) and 79 TFEU for border management and migration; Arts. 82(1)(d) and 87(2) TFEU for judicial cooperation in criminal matters and law enforcement cooperation. Both regulations will replace Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. The Commission found divergences at the national level in the application of the Directive. In addition, the Commission identified security gaps since the Directive primarily focuses on facilitating border checks at the EU's external borders and on combating illegal immigration. Even though the Directive allowed Member States to use API data for law enforcement purposes, it did not further specify the scope, conditions, and safeguards for the processing of API data for these purposes. Since Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive) allows for the joint processing of API data and PNR data, clearer, more harmonised and more effective rules on API data were held necessary, so that law enforcement authorities can benefit from combining the two data sets. API refers to data collected by air carriers at check-in and sent to

competent authorities in the country of destination prior to take-off. PNR refers to data from air travellers' ticket reservations.

The Regulations will cover flights within, into and from the EU. However, as regards intra-EU flights, Regulation 2025/13 includes specific provisions that align the new legal framework with the PNR Directive and the CJEU's case law. In its 2022 judgement on the validity of the PNR Directive (→eucrim 2/2022, 113–115), the CJEU set strict limits to the processing of PNR data and ruled that PNR data cannot be processed automatically for all intra-EU flights. Such processing was only allowed when a Member State is "confronted with a terrorist threat which is shown to be genuine and present or foreseeable."

As a consequence, Member States can decide, in accordance with Art. 2 of Directive 2016/681, to apply that Directive and consequently Regulation 2025/13 to intra-EU flights, but they must select such intra-EU flights before API data can be transmitted to the national passenger information units (PIUs). Regulation 2025/13 specifies the elements of the assessment needed for selecting the intra-EU flights. This selection would have to be limited to what is strictly necessary.

Furthermore, the Regulation includes the following:

- Setting of a mandatory list of API data to be collected by air carriers from passengers;
- In order to increase the quality of the data, obligation for air carriers to collect data from passengers (family and first name, date of birth, nationality, etc.) using automated means, with manual insertions of the data in exceptional cases;
- Mandatory transfer of data to the Member States which will reduce time spent for border controls;
- Establishment of a single router via which API and PNR data are transferred from the air carriers to the PIUs. The router system will replace the current system of multiple connections between air carriers and national authorities. The router is developed and managed by eu-LISA and will include a secure channel to receive real-time flight traffic information. The measures to be taken in case of technical impossibility to use the router are specified.
- Data protection responsibilities: Air carriers will be controllers for the processing of API data constituting personal data in relation to their collection of that data and their transfer thereof to the router under the Regulation. Each Member State will designate a competent authority as data controller. Air carriers will provide passengers, on flights covered by the Regulation, with information on the purpose of the collection of their personal data, the type of personal data collected, the recipients of the personal data and the means to exercise their rights as data subjects.
- Governance structure for the transfer of API data consisting of the Programme Management Board, the API-PNR Advisory Group, the API-PNR Contact Group, and the API Expert Group.
- Sanctions: Member States will ensure that a recurrent failure to transfer API data is subject to proportionate financial penalties of up to 2% of the air carrier's global turnover for the preceding financial year. Failure to comply with other obligations set out in the Regulation will be subject to proportionate penalties, including financial penalties.

Regulation 2025/12 and Regulation 2025/13 entered into force on 28 January 2025. They will apply after the router is put into service. A longer transitional period is foreseen for the transmission of PNR data via the router. (TW)

Takedown of MATRIX

At the beginning of December 2024, a Joint Investigation Team from the Netherlands, France, Lithuania, Italy, and Spain took down the MATRIX (Mactrix/Totalsec/X-quantum/Q-safe), an encrypted messaging service created by criminals for criminals. The takedown was aided by Eurojust and Europol.

Criminal users could join the service by invitation. The platform consisted of over 40 servers in several countries, with important servers located in France and Germany. For three months, the authorities were able to intercept the messaging service and monitor the activity on the service, resulting in the interception and decryption of more than 2.3 million messages in 33 languages. The messages were linked to serious crimes such as international drug trafficking, arms trafficking, and money laundering.

On the day of the operation (3 December 2024), which took place in four countries, houses were searched, three people were arrested, and €145.000 in cash, €500.000 in cryptocurrency, four cars, and over 970 telephones seized. A freezing order was also placed on a villa with an estimated value of €15 million. (CR)

Shutdown of Global Illegal Streaming Service

On 26 November 2024, one of the largest illegal streaming services was shut down in a major operation involving Italian, Croatian, Dutch, Romanian, Swedish, Swiss, and UK authorities. The illegal service offered films, series, and TV channels, including sports channels, and served more than 22 million users worldwide. It generated more than €250 million in illegal profits per month, causing an estimated economic loss of €10 billion to the copyright holders of the material.

On the day of the action, which was supported by Europol and Eurojust, the servers hosting the illegal streaming were seized and shut down. In addition, over €1.6 million in cryptocurrency and €40,000 in cash were seized and 11 suspects arrested. (CR)

Council of Europe

Reported by Thomas Wahl

Foundations

Artificial Intelligence (AI)

Council of Europe Publishes Aid for AI Impact Assessments

On 2 December 2024, the Council of Europe presented the "HUDERIA Methodology". This document provides guidance for both public and private entities to carry out risk and impact assessments for artificial intelligence (AI) systems from the point of view of human rights, democracy, and the rule of law. The entities are supported in determining the extent to which risk management activities related to human rights, democracy and the rule of law may be called for. HUDERIA offers a methodology for risk and impact identification, assessment, prevention, and mitigation that is applicable to a variety of AI technologies and application contexts. It is also responsive to future developments in AI technologies and applications.

HUDERIA is not binding and not intended as an interpretive aid for the recently adopted Council of Europe Framework Convention on Artificial Intelligence (→eucrim 3/2024, 194–196). HUDERIA is meant to complement existing or future frameworks, policies, guidance, standards or tools for conducting AI risk and impact management.

The HUDERIA Methodology follows a socio-technical approach, which views all aspects of the AI system lifecycle as affected by the interconnected relationship of technology, human choices, and social structures. It provides for the creation of a risk mitigation plan to minimise or eliminate the identified risks, protecting the public from potential harm.

HUDERIA was adopted by the Council of Europe's Committee on Artificial Intelligence (CAI) at the end of November 2024. The HUDERIA Methodology will be complemented by the HUDERIA Model to be adopted in 2025. The Model will provide supporting materials and resources (such as flexible tools relevant for different elements of the HUDERIA process and scalable recommendations) that can aid in the implementation of the HUDERIA Methodology. (TW)

Specific Areas of Crime

Corruption

GRECO's President Statement to Mark International Anti-Corruption Day

On occasion of the International Anti-Corruption Day, held every year on 9 December, the President of GRECO, *Marin Mrčela*, emphasised the connection between the protection of democracy and anti-corruption efforts. He stated: "Against the risk of democratic backsliding, it is crucial that governments prove their commitment and show political will by adopting robust anti-corruption legislation and taking determined action against corrupt practices in all spheres of public life. Effective anti-corruption efforts will help restore the trust deficit that exists between institutions, politicians, officials and citizens. Anti-corruption progress is essential to safeguard democracy and the rule of law."

He also highlighted the need to mobilise young people to stand up for integrity and to involve the youth in anti-corruption efforts, otherwise a society built on freedoms and prosperity is at stake. *Mrčela* also referred to the Reykjavík Declaration on Principles for Democracy, which was adopted in May 2023. Here, the Heads of State and Government of the 46 Council of Europe member states committed to securing and strengthening democracy and good governance at all levels throughout Europe. They also committed, among other things, to pursuing "a relentless fight against corruption, including through prevention, and by holding accountable those exercising public power [...]."

Lastly, *Mrčela* pointed out the launch of GRECO's new (6th) evaluation round in 2025 focusing on preventing corruption and promoting integrity in local and regional authorities, i.e., the subnational level and therefore the closest to citizens' everyday lives. He stressed that GRECO "will support local and regional governments across Europe, the United States of America and Kazakhstan in sharpening their tools to combat corrupt practices. They should show zero tolerance for corruption." (TW)

GRECO: New President and Vice-President

At its 98th Plenary Meeting (held in Strasbourg from 18 to 22 November 2024), the representatives of the 48 GRECO member states elected David Meyer from the United Kingdom as

new President. He succeeds *Marin Mrčela*, Justice of the Supreme Court of the Republic of Croatia who has been GRECO's President since 2011 (see also Mr Mrčela's eucrim guest editorials).

David Meyer's term of office as GRECO President started on 1 January 2025. He is Head of International Engagement & Rule of Law at the UK Ministry of Justice. Meyer has also been closely affiliated with GRECO for a long time: He led the United Kingdom's delegation to GRECO since 2014, has been a member of the GRECO Bureau since 2016 and was a member of the Working Groups that developed the 5th and 6th evaluation rounds. Last but not least, he actively participated in several evaluations, ad-hoc evaluations and high-level visits, and acted as a rapporteur for multiple compliance reports.

New Vice-President of GRECO as of 1 January 2025 is *António Delicado* from Portugal succeeding *Monika Olsson* (Sweden). Part of the new GRECO Bureau are also: Ms *Alexia Kalispera* (Cyprus), Ms *Lise Chipault* (France), Ms *Panagiota Vatikalou* (Greece), Mr *Sorin Tanase* (Romania), and Mr Olivier Gonin (Switzerland). (TW)

GRECO: Fifth Round Evaluation Report on Switzerland

On 25 November 2024, GRECO published its 5th Round Evaluation Report on Switzerland. The report assessed the effectiveness of the framework in place in Switzerland to prevent corruption among persons with top executive functions (PTEFs) and members of the law enforcement authorities.

According to the report, Switzerland has a framework that is by and large adequate for tackling and preventing corruption. The rules on access to information, public consultation and transparency of the legislative process are exemplary. However, although Switzerland is among the top countries in indices for good governance and perceptions of corruption, and its population has considerable confidence in its institutions, the corruption risks in the two fields being assessed have not specifically been analysed in detail.

The Federal Council's anti-corruption Strategy could be more ambitious and concrete in terms of goals and substance. It is monitored to some extent by the Interdepartmental Working Group on Combating Corruption; however, the Group lacks the independence and resources to do so. Therefore, GRECO calls for a substantial strengthening of this body as well as an analysis of integrity risks and measures specifically targeting PTEFs, particularly on the key issues of lobbying and revolving doors. In addition, GRECO makes a number of other recommendations to remedy shortcomings, such as institutional checks at the level of the Federal Chancellor and the Federal Council, better transparency regarding PTEFs' business and financial interests, and ethics training.

The prevention of corruption has also not been adequately acknowledged in the two law enforcement authorities assessed, namely the federal criminal police (PJF) and the Operations and Prosecution Directorates of the Federal Office for Customs and Border Security (FOCBS). Hence, Switzerland should adopt a more proactive approach in this law enforcement field. In addition, the FOCBS should draw up a specific code of conduct for its staff and both the PJF and the FOCBS should introduce special arrangements for confidential guidance on issues of ethics and integrity. The protection of whistleblowers should be improved, particularly through awareness raising measures. Lastly, existing good practice for ensuring that women are adequately represented in these two agencies should be taken further.

GRECO called on Switzerland to submit a report on the measures taken to implement GRECO's 15 recommendations by 31 December 2025. (TW)

GRECO: 5th Round Evaluation Report on San Marino

On 2 December 2024, GRECO published its 5th Round Evaluation Report on San Marino. GRECO evaluated the effectiveness of the framework in place in San Marino to prevent corruption among persons with top executive functions ("PTEFs", i.e. members of the Congress of State, Heads of Departments (including the Director of Civil Service), ministers' political staff members and consultants with similar functions), and members of the "Police Corps" (i.e. the Gendarmerie, the Fortress Guard and the Civil Police).

GRECO found that San Marino does not have a national anti-corruption policy in place, but corruption prevention plans have been adopted in respect of some areas. In view of the executive powers exercised by PTEFs, San Marino should therefore develop and adopt a specific anti-corruption policy following a comprehensive risk assessment in relation to PTEFs. Moreover, to prevent and manage conflicts of interest, PTEFs should undergo integrity checks as part of their appointment and recruitment.

The provisions of the code of conduct for members of the Congress of State and the code of conduct for public officials should be harmonised and supplemented by a practical guide to improve consistency and effectiveness. It is also necessary to allocate additional resources (in particular adequate staffing) to the Ethics Committee and to establish an effective mechanism for PTEFs to obtain confidential counselling in relation to ethical issues.

GRECO made several recommendations to improve access to information and transparency. For example, the legal framework of 2011 on access to information should be reviewed,

and rules should be put in place with regard to the conduct of public consultations for draft legislation originating from the Congress of State as well as on governing the interaction of PTEFs with third parties/lobbyists who seek to influence the government's decision making. The obligation to make declarations of assets ought to be extended to all PTEFs.

Looking at the Police Corps, GRECO recommends that a comprehensive risk assessment of corruption-prone areas be carried out in the light of the findings of the report and a strategy be developed for all law enforcement agencies. Moreover, the Police Corps would greatly benefit from the setting up of a central autonomous body with internal oversight and control powers. Other recommendations in the area of law enforcement include:

- Establishing a (single) mechanism of confidential counselling for law enforcement officers outside of the chain of command;
- Conducting regular integrity checks vis-à-vis members of the Police Corps;
- Standardising and streamlining treatment of public complaints against misconduct of members of the Police Corps;
- Making the disciplinary system in respect of the Gendarmerie and the Fortress Guard more effective;
- Introducing whistleblower protection measures and providing dedicated training, not least because there are no cases of whistleblowing.

GRECO invited the authorities of San Marino to submit a report on the measures taken to implement its recommendations by 31 May 2026. (TW)

Money Laundering

EU Supranational Measures in MONEYVAL 5th Round Mutual Evaluation Report

On 20 December 2024, MONEYVAL published the findings of a horizontal study that has analysed how EU supra-national legislation, mechanisms and other initiatives have been considered and weighted in MONEYVAL's 5th round assessments. The study emphasised that more than a third of MONEYVAL member countries are EU Member States and, as such, subject to the EU's legal order that includes a comprehensive set of harmonisation measures with regard to anti-money laudnering and countering financing of terrorism (AML/CFT). In addition, a number of other MONEYVAL members are committed to harmonise their legislation with the EU's AML/CFT *acquis*.

The study was initiated after discussions during MONEYVAL's 5th round of mutual evaluations have often raised the question of how EU supranational measures should be interpreted and weighted when evaluating EU Member States. For this reason, MONEYVAL's Strategy 2023–2027 identified the need to develop a consistent understanding for the assessment of supranational mechanisms.

One of the key findings of the study is that some ambiguities have been identified in 5th round mutual evaluation reports of EU-MONEYVAL member states with respect to EU supranational mechanisms sometimes being described in diverse or inconsistent manner. (TW)

Cybercrime

CoE Report on Search and Seizure of Stored Computer Data in 74 Countries

On 18 December 2024, the Council of Europe's Cybercrime Convention Committee (T-CY) published a report that assessed the implementation of Art. 19 of the Budapest Cybercrime Convention by 74 countries that are Parties to the Convention. Art. 19 of the Budapest Cybercrime Convention sets out several obligations for each Party to adopt legislative and other measures with regard to the search and seizure of stored computer data – a vital tool in the global fight against cybercrime and in the collection of electronic evidence relating to any type of crime.

The report evaluated whether countries use general or specific powers, or a combination of both, to enforce Art. 19. It not only offers a comprehensive overview of current practices but also includes recommendations for strengthening the effectiveness of the various obligations in Art. 19, ensuring legal certainty, and enhancing safeguards as outlined in Art. 15 of the Convention.

The T-CY considers the release of this report "a significant milestone in improving the legal frameworks governing cybercrime investigations collection of electronic evidence worldwide. By providing clear guidelines and recommendations, it helps reinforce the global commitment to effectively combating cybercrime while respecting human rights and ensuring legal safeguards." (TW)

Procedural Law

Procedural Safeguards

CCJE Opinion on the Disciplinary Liability of Judges

On 13 December 2024, the Consultative Council of European Judges (CCJE) of the Council of Europe adopted an opinion on the disciplinary liability of judges. The opinion was drafted in the light of the fact that liability of judges has become a topic of great concern in recent years. Several decisions by the European courts found that the executive has used disciplinary measures to silence or remove judges who did not decide in their favour. Against this background, the opinion reflects on the basis, justification and limits of the disciplinary liability of judges. It

provides a set of core principles and recommendations applicable to all CoE member states and is designed to deal with situations where judicial independence and impartiality may be jeopardised.

The CCJE reaffirmed that disciplinary liability of judges contributes to maintaining public confidence in the administration of justice, but, at the same time, cannot undermine the function of the judiciary to decide cases impartially and according to law.

The opinion lists 23 recommendations, of which the key ones are:

- Establishing clear rules ensuring that the bodies initiating and deciding on disciplinary proceedings are independent of the executive and legislative powers;
- Enabling judges to participate fully in disciplinary proceedings and having the right to appeal, in accordance with Art. 6 ECHR;
- Exempting judges' decisions, including their interpretation of the law or weighing of evidence, from disciplinary sanctions (unless there are cases of malice or serious misconduct);
- Drawing up and making available an exhaustive list of sanctions, and considering dismissal only in exceptional circumstances;
- Ensuring that vetting does not replace disciplinary measures. (TW)

Articles

Articles / Aufsätze

Fil Rouge

In this special *eucrim* issue on the "25th Anniversary of the European Anti-Fraud Office" (OLAF), we are very proud to feature several articles by OLAF staff members. They chart the history of the Office and the long way it has come in improving the fight against fraud affecting the EU's financial interests.

In our guest editorial, *Ville Itälä*, OLAF's Director-General, tells the OLAF success story and outlines the developments since its creation in 1999. He tallies that OLAF investigators have uncovered around €16 billion since then that would otherwise have been lost to irregularities or fraud, with considerable damage to taxpayers' money. Anticipating future trends and developments, he also touches on the use of digital innovations – a topic which is picked up again in the following *eucrim* article section.

In the first article, *Maria Ntziouni-Doumas* looks back on the trajectory of OLAF, starting with its predecessor, UCLAF, all the way to its current role as an independent investigative body. She sketches the Office's history from several angles, including OLAF's legal framework, influential case law, and cooperation with the EPPO. Having celebrated important achievements along the way, she ends her account by highlighting the relevance of OLAF being an integral part of the EU anti-fraud architecture.

Following this overview, *Georg Roebling* and *Konstantinos Bovalis* dive into OLAF's digital transformation, from its humble digital beginnings to today's "digital first" approach. This continued evolution has allowed the Office to adapt to a changing and more connected world and to innovate. The authors also draw a parallel to the development of OLAF's legal framework regarding data collection and data processing. In the final section of the article, they shine the spotlight on the digital challenges ahead.

Next up, *Diana Riochet* and *Nikoleta Symela Mavromati* highlight how fundamental rights and procedural guarantees have evolved in OLAF investigations. They show how important it has been to progressively codify these rights over the years, as reflected in the successive modifications of the regulations governing the conduct of OLAF investigations. A particular focus is put on the creation of the new function of the Controller of procedural guarantees and the introduction of a new complaints mechanism following the last amendment of the OLAF Regulation in 2020 as significant steps towards reinforcing the protection of fundamental rights and procedural guarantees of persons concerned in OLAF investigations.

International relations is another area where OLAF has come a long way – and this is the main subject of the fourth article by *Lukáš Jelínek* and *Clemens Kreith*. They demonstrate that while there are several anti-fraud actors at EU level, OLAF is unique with regard to its international activities, including investigative. The authors first examine the basis for OLAF investigative powers in third countries within the EU's legal framework and shed light on some of the practical aspects of OLAF's international relations. Recalling OLAF's history, *Jelínek* and *Kreith* illustrate that many of the features which define OLAF's international relations today have their roots in the early years of the Office, even though they have gradually grown, expanded, and matured over the last quarter of a century.

Last but not least, *Alicia-Luna Scala-Amez* recollects the success story of the Hercule Programme, which was established in 2004 to financially support actions pertaining to the protection of the financial interests of the European Community and celebrated its 20th anniversary in 2024. The Hercule Programme has been managed by OLAF and became a component of the current Union Anti-Fraud Programme (UAFP) in 2021. *Scala-Amez* presents examples of the Programme's achievements, such as the purchasing of specialised equipment and tools like forensic laboratories, unmanned aerial vehicles (drones), underwater drones, etc. In light of the growing interest by potential beneficiaries, she concludes that a financial injection would be necessary to allow the Programme to continue to achieve its objectives in the future.

Dr. Frank Michlik, LL.M. (Cambridge), European Commission / European Anti-Fraud Office (OLAF), Head of Unit "Legislation and Policy"

Selina Grassin, European Commission / European Anti-fraud Office (OLAF), Unit "Legislation and Policy," Legal and Policy Officer

25 Years of OLAF: Looking Back and Ahead

Maria Ntziouni-Doumas*

The article examines the evolution of the European Anti-Fraud Office (OLAF) over the past 25 years from its establishment in 1999 to its current role as a pivotal player in the fight against fraud affecting the EU's financial interests. It starts by tracing OLAF's origins to its predecessor, the Unit for the Coordination of Fraud Prevention (UCLAF), and the circumstances surrounding OLAF's creation as a response to major corruption scandals. The article goes on to analyse the legal framework underpinning OLAF's mandate, in particular Regulation (EU, Euratom) No. 883/2013 and Directive 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law, which expanded OLAF's scope and facilitated its cooperation with the European Public Prosecutor's Office (EPPO). Furthermore, OLAF's evolving relationship with the EPPO is explored and significant case law that has shaped OLAF's investigative powers and procedural safeguards highlighted. The article concludes by reflecting on OLAF's achievements and the challenges it faces in combating fraud in an increasingly complex and multifaceted international financial landscape.

I. The Creation of OLAF: Historical Context and Predecessor UCLAF

*The **O**ffice Européen de **L**utte **A**nti-**F**raude* (European Anti-Fraud Office – OLAF) celebrates its 25th anniversary as a crucial actor in protecting the financial interests of the European Union (EU). OLAF's origins date back to its predecessor, the ***U**nité de **C**oordination de la **L**utte **A**nti-**F**raude* (the Task Force "Anti-Fraud Coordination Unit" – UCLAF), created in 1987 by the Commission within its Secretariat General. UCLAF laid the groundwork for what was to become a more robust and autonomous body. Established in 1999, OLAF's very formation marked a watershed moment in the EU's battle against fraud, corruption, and irregularities that threaten its financial system. As an independent body with investigative powers, OLAF's mandate covers investigations of administrative nature against fraud and irregularities that concern EU-related revenues and expenditures. This includes the general budget of the EU, budgets administered by the Union or on its behalf, and certain funds not covered by the budget but administered by the Union's agencies for the agencies' account. OLAF also extends its powers to all measures affecting or liable to affect the Union's assets. Lastly, OLAF is mandated to detect and investigate cases of serious misconduct of permanent employees (officials), other servants of the Union, and members of EU institutions[1] as well.

OLAF replaced and succeeded UCLAF. Although UCLAF was instrumental in introducing fraud prevention mechanisms, its scope was limited in several ways due to its lack of operational independence and narrower investigative powers. The widespread allegations of fraud, mismanagement, and nepotism that surrounded the *Santer* Commission and led to its collective resignation in 1999 further highlighted the need for an independent body that could investigate both internal and external fraud affecting the EU's budget. In response to these crises and scandals, OLAF was established by European Commission Decision 1999/352 on 28 April 1999.[2]

OLAF has had a hybrid status since its establishment: while it is formally part of the Commission, enabling it to exercise Commission powers, it is endowed with budgetary and administrative autonomy, designed to make it operationally independent.

Specifically, Commission Decision 1999/352 delegated to OLAF the Commission's powers to execute all operational activities relating to safeguarding Community interests against irregular conduct liable to result in administrative or criminal proceedings. This decision further granted OLAF a significant level of independence from the Commission. It empowers OLAF to conduct internal (EU institutions, bodies, offices, and agencies) and external (economic operators in the Member States) administrative investigations to detect fraud, corruption, and other illegal activities against the Union's financial interests, and to carry out investigative assignments in other areas at the request of EU institutions.

OLAF's investigations result in recommendations (judicial, financial, and administrative) to competent authorities. With these recommendations, OLAF asks the competent authorities to take action in order to redress the problems uncovered by its investigations. OLAF's recommendations always intend to protect the EU budget and to uphold the rule of law.

In addition, in line with its mandate, OLAF is the leading stakeholder when it comes to strengthening cooperation efforts with the Member States in the field of fraud prevention, preparing legislative initiatives designed to advance the fight against fraud, maintaining direct contact with national

law enforcement and judicial authorities, and representing the Commission in fraud prevention matters in general.

II. OLAF's Legal Framework

OLAF's mandate is governed by **Regulation (EU, Euratom) No. 883/2013**[3] concerning investigations conducted by OLAF, which details investigative procedures and guarantees its independence.

The Commission has delegated to OLAF all of its powers of investigation for the fight against fraud, corruption and any other illegal activity affecting the financial interests of the Union, as well as serious matters relating to the discharge of professional duties by Union officials. The Office exercises in complete independence the powers of investigation conferred on the Commission by Union legislation and conducts administrative investigations within the institutions and bodies, in conformity with 883/2013 as well as through Regulations 2988/1995[4] and 2185/1996[5], which complement OLAF's Regulation by establishing general principles for administrative penalties and financial corrections, and outlining provisions for on-the-spot checks and inspections respectively.

Regulation 883/2013 emphasises OLAF's pivotal role **in administrative investigations**, while the European Public Prosecutor Office (EPPO) and national authorities are tasked with pursuing criminal conduct.

Under this Regulation, OLAF has the power to:

- Conduct internal administrative investigations within EU institutions, bodies, agencies, and offices to detect serious irregularities and misconduct by officials or their members;
- Conduct external administrative investigations in Member States and third countries in collaboration with national authorities, focusing on the misuse of EU funds;
- Perform on-site inspections and access documentation that may be relevant to investigations;
- Recommend action, including financial, disciplinary, and judicial measures, following the conclusion of an investigation.

OLAF's independence is further enshrined in its ability to open investigations autonomously without requiring approval from the Commission or any other institution. However, OLAF's investigative role is administrative in nature, meaning it can only recommend judicial action, with the decision to prosecute resting with the European Public Prosecutor Office (EPPO) and national authorities.

III. OLAF's Director-Generals and Their Role

According to OLAF's regulatory framework, the Office is headed by a Director-General. The OLAF Regulation particularly stresses the Director-General's independence (he or she shall neither seek nor take instructions from any government or any institution, body, office, or agency in the performance of his or her duties with regard to the opening and carrying-out of external and internal investigations or to the drafting of reports following such investigations).[6] Since its establishment, OLAF has been led by three Director-Generals, each of which played a critical role in shaping the office's operational efficiency and independence: *Franz-Hermann Brüner* was OLAF's first Director-General, serving from 2000 until his death in 2010. Brüner built the foundational framework for OLAF's investigative independence, helping the Office to gain credibility and establishing key procedural safeguards. A major internal reorganisation of OLAF that took place in 2006 during his mandate aimed to place more emphasis on OLAF's operational work, improve internal communication, and strengthen its management. *Giovanni Kessler*, OLAF's second Director-General who took office in 2011, further solidified OLAF's role by intensifying its investigative activities and strengthening its cooperation with national authorities and EU institutions. Under his leadership, OLAF also pushed for more transparency and accountability in its internal procedures,[7] paving the way for closer alignment with the EPPO. *Ville Itälä*, who has been Director-General since 2018, has overseen OLAF's evolving role within the EU's broader anti-fraud landscape, focusing on modernising OLAF's investigative tools and reinforcing its collaboration with the EPPO and the European Delegated Prosecutors. The status of these Director-Generals is crucial, as OLAF must remain independent from political influence in order to ensure impartial investigations, a necessity highlighted in OLAF Regulation 883/2013 and in related case law concerning the protection of procedural fairness and fundamental rights.

IV. Supervision of OLAF

The Supervisory Committee of OLAF and the Controller of Procedural Guarantees are crucial mechanisms that ensure oversight and accountability in OLAF's investigative processes, balancing its robust powers with respect for individual rights. This has been confirmed by the case law, which reinforced the relevance of both the Supervisory Committee and the Controller of Procedural Guarantees in ensuring that OLAF operates within the bounds of EU law, respecting fundamental rights while carrying out its anti-fraud mandate. The Supervisory Committee, composed of independent

experts, monitors OLAF's investigative activities, ensuring compliance with procedural standards and safeguarding OLAF's independence (Art. 15 of Regulation 883/2013,). Additionally, the Controller of Procedural Guarantees, a function that was introduced in the OLAF Regulation under its latest amendment by Regulation 2020/2223, plays a key role in protecting the rights of individuals involved in OLAF's investigations, such as ensuring access to defence services and the right to be heard (Art. 9a of Regulation 883/2013).

V. The PIF Directive

Since OLAF was established, the EU has made significant progress in adopting legislative texts pertaining to criminal law aimed at protecting its budget.

Specifically, Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law (the PIF Directive)[8], which replaced the former Convention-based PIF framework,[9] significantly reinforced the EU's ability to address fraud and corruption by defining and harmonising criminal offences that directly affect the EU's budget, such as fraud, corruption, money laundering, and misappropriation.

One of the most important developments introduced by the PIF Directive is the criminalisation of VAT fraud affecting the Union's financial interests when the damages exceed €10 million. This advancement was crucial as it expanded the scope of offences that OLAF is entitled to investigate in coordination with national authorities, enabling more robust protection of EU resources.

The PIF Directive also laid the groundwork for the establishment of the EPPO, which investigates and prosecutes the crimes defined in the Directive, thus representing a further step in the integration of anti-fraud efforts at the EU level.

VI. OLAF and the European Public Prosecutor's Office

As mentioned in Sections I and II, OLAF investigates EU-wide fraud schemes, but lacks prosecutorial powers. However, the European Public Prosecutor's Office (EPPO) has now closed this gap. The body was specifically created to investigate and prosecute criminal activities that harm the EU's financial interests, effectively complementing OLAF's administrative mandate with criminal investigative powers. Intense preparations by OLAF preceded the creation of the EPPO, and both Offices work in close partnership to increase the level of protection of EU citizens and of their money. The establishment of the EPPO in 2017 and its operational start in June 2021 have transformed the landscape of EU anti-fraud architecture, in which Eurojust and Europol are also key partners.

While OLAF and the EPPO operate in tandem, their roles are distinct. As mentioned in Section II, OLAF focuses on administrative investigations; when it uncovers evidence of criminal activity, it refers the case to the EPPO for criminal prosecution. The cooperation is governed by Regulation (EU) 2020/2223, amending the OLAF Regulation 883/2013 and the administrative arrangements between OLAF and the EPPO, which establish clear guidelines for cooperation – ensuring that OLAF's investigations feed into EPPO's criminal prosecutions efficiently. OLAF's experience in conducting investigations and gathering evidence provides further invaluable support to the EPPO's prosecutorial function. For instance, OLAF's investigations often result in substantial findings that the EPPO can leverage in criminal courts across the EU. It is important to note that OLAF investigates its cases in relation to EPPO Member States in a way to avoid any duplication with EPPO investigations. OLAF strives for maximum complementarity with the EPPO and focuses on financial recovery and preventive administrative measures. For the efficiency of the fight against fraud, it is promising to see that OLAF and the EPPO have developed good working practices that have led to positive results, and continue to deepen their cooperation and trust.

Nevertheless, OLAF continues to play a key role in conducting investigations where the EPPO does not have jurisdiction, bridging any gaps in the protection of the EU's financial interests – for example, in Member States not participating in the EPPO scheme or in relation to fraud in third countries and in international organisations. Furthermore, OLAF is still responsible for non-PIF related offences (e.g. cases of harassment) by staff or members of EU institutions, bodies, agencies, and offices which do not fall within the EPPO's competence. OLAF also continues to investigate non-fraudulent irregularities, which can cause significant financial damage to the EU, and is determined to step up its efforts in discovering fake and unsafe goods, unhealthy food stuffs, and environmentally dangerous goods – areas that are not covered by the scope of the EPPO as well.

VII. OLAF's Achievements

In this quarter of a century, OLAF has carried out and closed a total of over 6,000 investigations and recommended around €16 billion for recovery to the EU budget.[10]

In the last 13 years alone, OLAF has completed over 2,800 investigations, and recommended the recovery of over €9.4 billion to the EU budget. It issued over 3,700 recommendations for judicial, financial, disciplinary, and administrative action to be taken up by the competent authorities of the Member States and the EU. As a result of its work, sums unduly spent were gradually returned to the EU budget, criminals faced prosecution before national courts, and better anti-fraud safeguards were put in place throughout the Union. As highlighted in its recent annual report, in 2023 alone, OLAF concluded 265 investigations, issuing 309 recommendations to the relevant national and EU authorities, opened 190 new investigations and recommended the recovery of €1.04 billion to the EU budget.[11] These figures underscore OLAF's effectiveness in identifying and addressing fraudulent activities that threaten the financial integrity of the European Union.

On top of that, OLAF has been investigating cases of misconduct by EU staff or members, detecting smuggling networks, tracking down counterfeit products, and developing policies that prevent fraud from happening in the first place.[12]

VIII. Significant Case Law Shaping OLAF's Role

Over the past 25 years, several landmark cases heard by the Court of Justice of the European Union (CJEU) have confirmed, defined, and emphasised the scope and limits of OLAF's investigative powers and its relationship with national authorities and EU institutions. The very first judgment of the CJEU that highlighted the fact that "Member States are required to take action against infringements of Community law in conditions analogous with those applicable to infringements of national law and to confer on the sanction an effective, proportionate and dissuasive character" concerned the landmark *Greek Maize* case (Case 68/88).[13]

The following section outlines some of the most significant judgments that have shaped OLAF's role:

- Case T-193/04, *Hans-Martin Tillack v Commission* (2006):[14] This case addressed OLAF's handling of information leaks to the press and involved an OLAF investigation into alleged corruption. The European Court of First Instance ruled that OLAF was justified in providing national authorities with information leading to a journalist's home and office being searched. However, the judgment emphasised the need for OLAF to adhere to procedural guarantees and the fundamental rights of individuals during investigations, including safeguarding journalists' sources. This ruling helped reinforce the protection of procedural guarantees and the fundamental rights of individuals during investigations.
- Case T-48/05, *Franchet and Byk v Commission* (2008):[15] This case concerned OLAF's investigation into alleged financial irregularities within Eurostat. The applicants, former Eurostat officials, argued that OLAF officials had violated their rights by leaking confidential information. The General Court found that OLAF had failed to properly manage the confidentiality of its investigations, emphasising the importance of ensuring the rights of defense and data protection throughout its processes.
- Case C-11/00, *Commission v European Central Bank* (2003):[16] In this case, the European Central Bank (ECB) challenged OLAF's jurisdiction over its internal matters. The Court of Justice ruled that OLAF did not have the authority to conduct internal investigations within the ECB, as the ECB is distinct from the other EU institutions. This ruling helped clarify the scope of OLAF's mandate in relation to certain independent EU bodies.
- Case C-15/00, *Commission v European Investment Bank* (2003):[17] Similar to the ECB case, this ruling concerned OLAF's ability to conduct investigations within the European Investment Bank (EIB). The Court of Justice held that OLAF's mandate covered the EIB, ensuring that its financial dealings would be subject to scrutiny under OLAF's investigative powers, and reinforcing the principle that EU funds must be protected across all EU bodies.
- The *Vialto* cases,[18] the actions for annulment brought by Poland and Hungary against the regime of conditionality for the protection of the EU budget,[19] and the *Sigma Orionis* case[20] underscore OLAF's critical role in investigating and combating fraud affecting the financial interests of the European Union. In the *Vialto* cases, OLAF's efforts focused on ensuring compliance with EU regulations and preventing misuse of EU funds, particularly in cross-border projects. The cases against the regime of conditionality attacked by Poland and Hungary further emphasised the need for transparency in the allocation of funds, especially in the context of cohesion policy, where OLAF has frequently intervened to mitigate irregularities. Finally, the *Sigma Orionis* case, involving fraudulent mismanagement of research and innovation funds, illustrates OLAF's vigilance in the Horizon 2020 programme framework, and highlighted the importance of accountability in EU-funded research initiatives. These cases collectively reflect OLAF's strategic mandate to investigate and protect EU funds, uphold financial integrity, and ensure that EU taxpayers' money is spent correctly and efficiently.

IX. Outlook

OLAF's 25-year history has been marked by significant achievements in protecting the EU budget against fraud, corruption, and other illegal activities, both on the revenue and on the expenditure side of the budget. From its beginnings as a Commission task force service (UCLAF) to its current role as an independent investigative body, OLAF has played a pivotal role in safeguarding the EU budget as an integral part of the toolbox of an EU-wide rule of law mechanism that the Commission is implementing. OLAF continues to contribute to the sound financial management of the EU budget as well as the safety and security of Europeans, and to upholding the reputation of the EU institutions and bodies. Through its regulatory framework, notably Regulation 883/2013 (the OLAF Regulation) and Directive 2017/1371 (the PIF Directive), OLAF has been equipped with the tools needed to carry out its mission. At the same time, case law surrounding OLAF's work demonstrates that its actions must balance investigative efficiency with the protection of fundamental rights, ensuring that justice is served while respecting procedural safeguards. Moreover, its cooperation with the EPPO marks a new chapter in the Union's anti-fraud efforts, strengthening the EU's ability to prosecute criminal offences that threaten its financial system.

As OLAF moves into its next phase, it must continue to adapt to the evolving nature of financial fraud, particularly in an increasingly digitised and globalised world.

OLAF's complementarity to the EPPO should be reinforced in the future. Effective and efficient cooperation with the EPPO to protect the EU budget and to ensure the swift recovery of EU funds is needed. Information exchange between the various investigative (OLAF and EPPO) and law enforcement bodies (for example Eurojust, Europol, and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)) at the EU level, whose mandates cover the EU's financial interests, is the key to success.

Furthermore, the political priorities of the 2024–2029 Commission[21] include the reinforcement of OLAF's mandate by supporting the enforcement of EU law across Member State borders. The Commission is continuously closing enforcement gaps in various EU policy fields, in particular in illegal shipment of waste[22], entry and circulation of illicit (chemical) products, food fraud, fight against counterfeiting and piracy and circumvention of EU sanctions by entrusting OLAF with investigative powers to carry out inspections and coordinating actions.

In conclusion, OLAF remains a cornerstone of the EU's broader legal and institutional framework. It ensures that the Union's financial interests are protected and that fraudsters face appropriate consequences. OLAF's mission was, is, and continues to be the support of a competitive and fair Europe that protects its citizens and their money.

* The views expressed in this article are solely those of the author and are not an expression of the views of the institution she is affiliated with.

1 Which also include the members of the European Parliament.

2 For an analytical diagram containing all the major milestones of OLAF, see: OLAF, "History" <https://anti-fraud.ec.europa.eu/about-us/history_en>, accessed 2 December 2024.

3 Regulation (EU, Euratom) No. 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No. 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No. 1074/1999, OJ L 248, 18.9.2013, 1. This Regulation replaced EP/Council Regulation (EC) 1073/1999 and Council Regulation (Euratom) 1074/1999.

4 Council Regulation (EC, Euratom) No. 2988/95 of 18 December 1995 on the protection of the European Communities financial interests, OJ L 312, 23.12.1995, 1.

5 Council Regulation (Euratom, EC) No. 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, 2.

6 Cf. Art. 17 Regulation 883/2013, *op. cit.* (n. 3), in particular its para. 3.

Maria Ntziouni-Doumas
European Commission / European Anti-Fraud Office (OLAF), Adviser

7 For example, in 2013, the Guidelines on Investigation Procedures (GIP) were issued. This is a set of internal rules that staff have to apply in order to ensure that OLAF investigations are carried out in a consistent and coherent way.

8 OJ L 198, 28.7.2017, 29. On the Directive, cf. A. Juszczak and E. Sason, "The Directive on the Fight against Fraud to the Union's Financial Interests by means of Criminal Law (PFI Directive)", (2017) *eucrim*, 80–87; W. Van Ballegooij, "Protecting the EU's Financial Interests through Criminal Law: the Implementation of the 'PIF Directive'", (2021) *eucrim* 177–181.

9 The PIF Directive drew upon the following legal instruments adopted on the basis of Title VI of the Treaty on European Union,

signed at Maastricht on 7 February 1992 (provisions on cooperation in the fields of justice and home affairs):
– The Convention on the Protection of the European Communities' Financial Interests, OJ C 316, 27.11.1995, 49; –- The First Protocol to the Convention on the Protection of the European Communities' Financial Interests, OJ C 313, 23.10.1996, 2;
– The Second Protocol to the Convention on the protection of the European Communities' Financial Interests, OJ C 221, 19.7.1997, 12;
– The Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, OJ C 195, 25.6.1997, 1.

10 See V. Itälä, Guest Editorial, *eucrim 4/2024*, in this issue.

11 OLAF, "OLAF in figures" <https://anti-fraud.ec.europa.eu/investigations/olaf-figures_en>, accessed 2 December 2024. See also T. Wahl, "The OLAF Report 2023", *eucrim* 2/2024, 100.

12 See also the regular reports on OLAF's operational work and cooperation with partners in the *eucrim* news section "Institutions > OLAF".

13 ECJ, 21 September 1989, Case C-68/88, *Commission of the European Communities v Hellenic Republic, ECLI:EU:C:1989:339*.

14 CFI, 4 October 2006, Case T-193/04, *Hans-Martin Tillack v Commission of the European Communities,* ECLI:EU:T:2006:292.

15 CFI, 8 July 2008, Case T-48/05, *Yves Franchet and Daniel Byk v European Commission,* ECLI:EU:T:2008:257.

16 ECJ, 10 July 2003, Case C-11/00, *Commission of the European Communities v European Central Bank,* ECLI:EU:C:2002:556.

17 ECJ, 10 July 2003, Case C-15/00, *Commission of the European Communities v European Investment Bank,* ECLI:EU:C:2003:396.

18 Vialto consisted of several cases before the General Court (GC) and appeals before the Court of Justice (ECJ). *Vialto Consulting* – a company incorporated under Hungarian law, which provides advisory services to undertakings and entities belonging to the private and public sectors – defended itself against OLAF investigations opened against the company on account of acts of corruption and fraud committed in connection with a project in Turkey financed by the Instrument for Pre-Accession Assistance (IPA). In detail, the CJEU rulings were as follows: ECJ, 30 May 2024, Case C-130/23 P (ECLI:EU:C:2024:439) – the case before the GC was T-537/18 (judgment of 21 December 2022, ECLI:EU:T:2022:852); ECJ, 28 October 2021, Case C-650/19 P (ECLI:EU:C:2021:879) – the case before the GC was T-617/17 (judgment of 26 June 2019, ECLI:EU:T:2019:446); and Case T-617/17 RENV, judgment of the General Court of 21 December 2022, ECLI:EU:T:2022:851.

19 ECJ (Full Court), 16 February 2022, Case C-156/21, *Hungary v European Parliament and Council of the European Union,* ECLI:EU:C:2022:97, and ECJ (Full Court), 16 February 2022, Case C-157/21, *Republic of Poland v European Parliament and Council of the European Union,* ECLI:EU:C:2022:98. The judgments are summarised by T. Wahl, "CJEU Dismisses Actions against Rule-of-Law Conditionality to Safeguard the EU Budget", *eucrim* 1/2022, 21–22.

20 GC, 3 May 2018, Case T-48/16, *Sigma Orionis SA v European Commission,* ECLI:EU:T:2018:245.

21 European Union, "European Union Priorities 2024–2029" <https://european-union.europa.eu/priorities-and-actions/eu-priorities/european-union-priorities-2024-2029_en>. For the mission letter to the Commissioner-Designate for Budget, Anti-Fraud and Public Administration, see: <https://commission.europa.eu/document/db369caa-19e7-4560-96e0-37dc2556f676_en>. Both hyperlinks were last accessed on 2 February 2025.

22 Within the scope of Regulation (EU) 2024/1157 on shipments of waste, Articles 67 to 71, the Commission is in the process of entrusting OLAF with investigative powers to carry out inspections and coordinating actions in respect of illegal shipments. See in this context S. Grassin and L.I. Garruto, "Fighting Waste Trafficking in the EU: A Stronger Role for the European Anti-Fraud Office – The Reviewed Waste Shipment Regulation and its Enforcement Provisions", (2024) *eucrim,* 143–145.

25 Years of OLAF – the Office's Digital Transformation and Some Reflections on What Lies Ahead

Konstantinos Bovalis and Georg Roebling*

In today's fast-changing world, the issue of digitalisation – or "tech" – is rapidly moving up the agenda. This observation also very much applies to the anti-fraud domain. On the occasion of the 25th anniversary of the European Anti-Fraud Office (OLAF) in 2024, this article provides a retrospective of the progressive digitalisation of work at the Office. Arriving at today's "digital first" paradigm has been a long journey since OLAF's humble digital beginnings in 1999. The authors also review the parallel evolution of OLAF's legal framework for data collection and data processing, and they offer some reflections on further digital challenges ahead.

I. Introduction

The last 25 years, which the European Anti-Fraud Office (OLAF) looks back on with pride, have witnessed many changes in the world around us. However, few have been as far-reaching and consequential as the pervasive digitalisation of virtually all aspects of our modern societies, including, notably, the work life. The work of fraud busters is of course no exception, and this applies both to the fraud and its busting.

This article first explores how the evolving legal framework governing OLAF's preventive and investigative work has supported and exerted an influence on OLAF's digital transition over the years. Secondly, it provides a practical overview of OLAF's digital transformation. And thirdly, we reflect on some of the digital challenges ahead.

II. OLAF's Evolving Legal Framework and Digital Evolution

OLAF has undergone several stages of its legal framework. The following examines OLAF's digital work within the initial legal framework, i.e., the OLAF Regulation 1073/1999[1] (hereinafter referred to as the "1999 OLAF Regulation"), and the current legal framework based on Regulation 883/2013[2], as amended notably by Regulation 2020/2223[3] (together referred to as "the current OLAF Regulation").

The analysis is built upon three main areas: First, the access to data that OLAF collects from a variety of sources via different means. Second, the processing of data following their acquisition. And third, we describe the digital setup in which OLAF performed its work under each legal framework. All these elements combined make up what we understand as OLAF's digital transformation.

1. Digital operations under OLAF's initial legal framework – the 1999 OLAF Regulation

OLAF's initial legal framework established by Regulation (EC) 1073/1999 was inevitably still a product of the twentieth century. Even though the dawn of the digital age was already on the horizon, the initial OLAF Regulation did not contain many, let alone exhaustive references to the issues we would today associate with digitalisation.

a) Access to data

In one key respect, the 1999 OLAF Regulation was already crafted in a sufficiently forward-looking manner to pave the way for the digital transition: regarding the type of data the Office would have access to. This is evidently a fundamental precondition for the Office to effectively carry out its mandate in a digital environment. As Advocate General *Francis Jacobs* observed in 2002 in the *EIB* case.[4]

> If OLAF were not empowered to access documents and data, take copies, ensure that documents and data are secured where necessary, and ask for oral information, its ability to uncover fraud and other irregularities would be severely limited.

The issue of accessing data, including electronic data was clearly set out in the 1999 OLAF Regulation in relation to **internal investigations**. In such instances, OLAF access was not limited to (paper) documents, but also covered other types of information. Pursuant to Art. 4(2) of that Regulation, OLAF was empowered to "take a copy of and obtain extracts from any document or the contents of any data medium held by the institutions, bodies, offices and agencies and, if necessary, assume custody of such documents or data to ensure that there is no danger of their disappearing."[5] This innovative provision already considered the concept of data to which OLAF was conferred a right of access. With data underpinning virtually all forms of digitalisation, this terminology laid the groundwork that would allow the OLAF Regulation to adjust flexibly to the evolving digital landscape.

As concerns **external investigations**, Art. 3 of Regulation 1073/1999 incorporated the provisions of Council Regulation No 2185/96 concerning on-the-spot checks and inspections carried out by the Commission.[6] The Regulation's Art. 7(1) established that inspectors shall have access, like national inspectors, "to all the information and documentation on the operations concerned".

The use of the two words "information and documentation" already implied that the concept of information was to be distinguished from a traditional document. Upon closer inspection, it becomes evident that the term "information" is to be understood very widely, and notably encompasses all possible forms of data: Art. 7 of Regulation 2185/96 provides a long list of examples as to what such information may comprise, including "computer data".[7]

Also elsewhere, the 1999 OLAF Regulation used a broad concept of the term "information", encompassing "documents" and "data". The term "information" was also used in this sense in Art. 7(2) and (3) of Regulation 1073/1999 expressing the duty – incumbent on both Member States and Community institutions, bodies, offices, and agencies – to let OLAF know of possible cases of fraud, corruption, and other illegal activities.

OLAF access to a wide variety of data, as described, has not substantially changed over the last 25 years. Rather, subsequent revisions of the OLAF Regulation have specified and strengthened this access to certain data categories which have been deemed essential to anti-fraud investigations.

b) Data processing

Article 3(3) of Regulation 2018/1725[8] setting out the data protection rules applicable to the EU institutions, bodies, offices and agencies provides a good summary of what such

processing may consist of: any operation or set of operations which is performed on data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The 1999 OLAF Regulation did not lay down in any detail how, where, and under which conditions the data collected by the Office should be processed. Notably, the question of *data storage* was not at all addressed in that Regulation.

However, as concerns *data analysis*, the 1999 Decision creating the Office[9] established in Art. 2(5)(b) that the Office shall be responsible for any other operational activity of the Commission in relation to the fight against fraud, including the collection and analysis of information. However, the Decision did not add any further conditions for the conduct of such analysis.

c) Being digital 25 years ago

In the years prior to the foundation of the Office in 1999, the administrative world in which it was embedded was based on digital databases with limited functionalities and split in scope. These were in essence the IRENE database (IRregularities, Enquiries, Exploration) for irregularities reported by the Member States, and Pre-IRENE, the then UCLAF internal case management database, which contained information on cases not reported by the Member States.

These databases suffered from weak performance, incompleteness of records, user-unfriendliness, limited querying capabilities (in turn preventing reporting), and a lack of standardisation related to the descriptions of fraud and irregularities. Interconnection was out of the question. As a result, the databases were not used systematically within the Office and a lot of information was still kept on paper or in electronic spreadsheets on local disc drives. Digital information maintained this way, mainly took the form of unstructured documents processed manually before being printed for further circulation (on trolleys being pushed from one office to another), reviewed, approved, and signed by hand.

During the Office's first on-the-spot checks, the amount of work carried out was typically expressed in meters (of physical file storage to plough through), not terabytes. And although digital forensics equipment existed and was occasionally used at the time, the pride and joy of the intelligence unit was a high-performance scanner that easily weighed 25kg and could process several thousand pages per hour.

Remote access to OLAF hosted systems and their data was not possible, and even from within the Office, desktop applications installed on the bulky personal computers of this still premature digital era were needed to enable access to local IT systems and applications. Access to the Internet was slow and subject to staff queuing behind the very limited number of computers connected to it. National and European authorities had barely begun implementing new data protection rules established by Regulation 95/46/EC.

2. Digital operations under OLAF's current legal framework – the 2013 OLAF Regulation (as amended in 2020)

The current OLAF Regulation still mentions the terms "documentation, information and also data" in various places, including the crucial clarification that this applies "irrespective of the medium on which it is stored".

However, today's approach is more consistent in the sense that the term "document" matches the definition given in Art. 3(a) of Regulation No 1049/2001, i.e., content (no matter the medium, written or digital) related to a subject matter (therefore carrying a specific meaning), whereas the term "data" is used as a complement of the above to denote a unit of raw material which does not carry a specific meaning. References to "personal data" should be read as information "related to an identified or identifiable natural person" as per Art. 3(1) of Regulation 2018/1725.

a) Access to data

The by now well-established OLAF access to a wide set of data in internal and external investigations has been **clarified and extended** in a number of directions in recent years. First of all, Art. 6(1) of the current OLAF Regulation establishes that the Office shall have, under certain conditions, access to "any relevant information in databases held by the institutions, bodies, offices or agencies" even prior to the opening of an investigation. Secondly, pursuant to Art. 7(3a), OLAF also has access to certain data concerning bank accounts, including – in cases where this is strictly necessary for the purposes of the investigation – the record of transactions. Thirdly, Arts. 3(5) and 4(2a) confirm, as a matter of principle, Office access to data on privately owned devices that are used for work purposes.

One of the most substantial changes over the last quarter of a century relates to OLAF access to relevant data via a **digital forensic acquisition**. In the context of internal investigations, such acquisitions of data held by the institutions, bodies, offices, and agencies may occur in or without the

presence of the data owner. Such operations are typically among the most privacy-invasive investigative measures which OLAF is empowered to undertake.

The possibility of such digital forensic acquisitions in internal investigations actually already existed prior to the entry into force of the 1999 OLAF Regulation.[10] This situation established by case law was then codified in Art. 4(2) of the 1999 OLAF Regulation and in Art. 7(1) Regulation 2185/1996, which also applies to external investigations. However, a quarter of a century ago, digital forensic acquisition was still a new and relatively rare investigative measure compared to today, mainly because of the low level of digital readiness in administration and businesses. In this sense, investigative practices in connection with digital forensic acquisition have changed profoundly.

In 2016 OLAF adopted Guidelines on Digital Forensic Procedures for OLAF Staff.[11] These Guidelines are binding and set out which procedural steps and technical precautions must be observed by the Office. They were confirmed by the ECJ in *Vialto*.[12] In substance, OLAF's digital forensic actions have always been carried out with potential use of the data as evidence in judicial proceedings in mind. Therefore, the Guidelines adhere to internationally accepted standards of digital forensic acquisitions (e.g., chain of evidence, documentation, and non-alteration of data).

The European courts have also established certain boundaries which apply when OLAF is collecting data. A good illustration is the Order of the General Court in the *LG case*[13], which indicates that the principle of legal professional privilege may also apply in the context of anti-fraud investigations in a similar way as it does in the anti-trust domain.

b) Data processing

In the same vein, the current OLAF Regulation remains largely silent on the conditions under which the Office may process data (in the wide sense presented above). The only exception is a reference in Art. 12g(2) (in the context of OLAF's cooperation with the European Public Prosecutor's Office) to managing OLAF's data in a **case management system**. Notably, the OLAF Regulation as such does not specify where the Office should store its data, e.g., on a server hosted locally or in the cloud.

Nonetheless, when designing an in-house **data storage** system, the Office needs to take confidentiality requirements into account so as to prevent leakages. This results, first of all, from Art. 10(1) and (2) of the current OLAF Regulation. Further legal constraints in that respect arise from the European data protection rules pursuant to Regulation 2018/1725. Art. 8(3) of the 1999 OLAF Regulation already explicitly spelled out that the Office had to comply with data protection rules, and that aspect has naturally not changed, as illustrated by Arts. 1(3)(e) and 10(1), (2) and (4) of the current OLAF Regulation.

In implementing Regulation 2018/1725, the Commission has adopted internal rules[14] concerning the processing of personal data by OLAF in relation to the provision of information to data subjects and the restriction of certain of their rights in accordance with Art. 25 of that Regulation. Those internal rules note in Recital 4 that in order to prevent unlawful access to or transfer of data to persons who do not have a need-to-know, OLAF stores personal data in a secured electronic environment.

Similarly, the OLAF Regulation is essentially silent on the ways in which OLAF can **handle** the data in its possession. Provisions of this kind can more often be found in sectoral legislation, such as the successive amendments of Regulation 515/97 on mutual administrative assistance in customs and agricultural matters.[15] These provisions have evolved substantively over the last 25 years.[16] On that basis, assistance has practically moved from exchanges of letters and then digital communication to the creation of large repositories with transaction level customs data hosted and managed by OLAF. Given the sensitivity of these data, the legislature has foreseen a number of restrictions as to who can access the data and for what purpose; restrictions that of course also affect OLAF's analytical and operational work.

Interestingly, Art. 2 of Regulation 515/97, as amended, contains relevant definitions of the important terms of "operational analysis" and "strategic analysis": **operational analysis** is understood as:

> the "analysis of operations which constitute, or appear to constitute, breaches of customs or agricultural legislation, involving the following stages in turn: (a) the collection of information, including personal data; (b) evaluation of the reliability of the information source and the information itself; (c) research, methodical presentation and interpretation of links between these items of information or between them and other significant data; (d) the formulation of observations, hypotheses or recommendations directly usable as risk information by the competent authorities and by the Commission to prevent and detect other operations in breach of customs and agricultural legislation and/or to identify with precision the person or businesses implicated in such operations".

By contrast, **strategic analysis** is defined as:

> "research and presentation of the general trends in breaches of customs and agricultural legislation through an evaluation of the threat, scale and impact of certain types of operation in breach of customs and agricultural legislation, with a view to subsequently setting priorities, gaining a better picture of

> the phenomenon or threat, reorienting action to prevent and detect fraud and reviewing departmental organisation. Only data from which identifying factors have been removed may be used for strategic analysis."

The coordination tools available to the Office provided for by Regulation 515/97 have subsequently been extended to a range of other sectors, such as the enforcement of intellectual property rights[17], export of cultural goods[18], transit of dual-use items[19], trade in drug precursors[20], the supervision of explosives for civil uses[21], manufacturing of and trafficking in firearms[22] as well as the EU's restrictive measures in response to Russia's actions in Ukraine in 2014[23].

But of course, the definitions and conditions for data access and handling set out in Regulation 515/97 only apply within the scope of the aforementioned instruments. By contrast, the current OLAF Regulation contains no equivalent rules. Yet, it is without doubt in relation to the various types of data processing operations that the most important developments have occurred over the last 25 years. OLAF is involved in a constant effort to extract and aggregate data from different sources, its own repositories and external databases, to clean and transform them in terms of format and upload them to data warehouses for processing and intelligence analysis.

When handling or processing personal data, the Office is naturally bound by **data protection** rules.[24] There is no doubt that the processing of investigative data, as long as it relates to the matter under investigation, is in principle necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body, in the sense of Art. 5(1)(a) of Regulation 2018/1725.[25]

The internal 2018 Commission Decision implementing Regulation 2018/1725 mentioned above[26] also sets out the applicable data protection regime in more detail for the specific investigative context. It addresses, for example, such issues as the period during which OLAF may retain investigative data (in principle for 15 years after dismissal or case closure) and the rights of data subjects. It includes transparency obligations and refers to OLAF's dedicated Data Protection Officer.

Within those boundaries, the European courts have accorded OLAF a certain discretion as to which processing operations may be required in the context of an investigation, as can be exemplified by the *Vialto* case relating to a digital forensic acquisition by OLAF.[27] In this case, the appellant had objected to the collection of data by OLAF forensic analysts, which the company considered unrelated to the project in question. At issue was the production of a digital forensic image of certain data on a digital storage medium to enable the data to be indexed. This indexation would in turn enable keyword searches using specific forensic computer software in order to identify the documents relevant for the OLAF investigation. The ECJ confirmed on appeal that the production of such a digital forensic image of all data stored on certain digital media was a legitimate intermediate step in the examination of those data.[28]

c) Progressive digitalisation

Even before the current OLAF Regulation was adopted, the Office had begun its digital transformation, i.e., the integration of digital technology in the practical implementation of the business process, so that the latter could be performed timely, efficiently and effectively. This did not happen overnight; it was a progressive effort to develop information systems, such as case management systems, organise the internal operational processes and manage information.

In these early years of the 21st century's digital revolution, digitalisation of business processes did not follow a holistic approach but, with the benefit of hindsight, appears more like a struggle to respond to fundamental challenges of this period.

- **Digital-first**: It may seem evident today, but 15 to 20 years ago, (re)designing business processes using digital means instead of paper circulation was a change to people's working culture. From today's perspective, the first efforts to apply this principle look almost clumsy, as operational bureaucracy was simply reproduced in digital terms. On the positive side, end users' experience improved, data were easier to collect and process, reporting to management was enhanced in quality, and security and data protection aspects were reinforced. The replacement of the legacy IRENE and Pre-IRENE databases with a new case management system (CMS) was an example of OLAF's shift towards a more digital way of organising document/record management based on electronic workflows, integrated search and increased security. Nevertheless, missing features, such as remote secure access to, effective reporting and digital document signing in the CMS were still to be implemented in the years that followed. Probably the ultimate effect of embracing a wider use of digital technologies was the established certainty that "digital is here to stay" and technology will determine the quality and effectiveness of administrative and operational activities of the Office.
- **Governance or "do it your own way"?** In the software development process of this era, known and pressing needs were implemented first, and emerging ones were tackled in subsequent phases. This resulted in information systems resembling digital patches of incoherent

modules, difficult to maintain and further evolve. The Office prioritised the flexibility to develop digital applications quickly and within available budget over a coherent approach that would first map all business needs and respond to them in order of priority. This inefficient way of building up information systems was tackled with the adoption of IT development and project management methodologies (Rational Unified Process and PM²)[29] to ensure a holistic response to automating business needs, resulting in a solid and scalable digital product able to address current and future requirements. Although these methodologies standardised the digital delivery process, they did not solve the issue of scattered IT developments and responsibilities in different units across OLAF. As was standard practice at the time, IT governance and decision-making were decentralised, creating digital silos.

- **Who's in the driving seat, IT or business?** That said, digital initiatives were still driven by IT. OLAF units and their staff involved in core investigative/operational activities, representing the business interest, tended to leave the design of IT systems to the IT experts. Involvement from the business side was limited and mainly at ideation or inception phase. IT project management followed a cascade model; broadly described business requirements were implemented in IT systems based on an incomplete understanding of the IT side for the actual business needs. This was spotted when completed digital end-products were found to only partially incorporate the business logic and outcomes. Escalation to management and internal reviews gave rise to stricter governance, with the business side beginning to assume responsibilities throughout the whole lifecycle of an IT project, from determining the business needs the IT system should address, to periodical evaluation of intermediate IT deliveries and acceptance testing before putting the information system in production mode.

d) Digital transformation in full swing

Over the last ten years, digital technology has exploded into every facet of people's work and private lives. OLAF has been no exception and has reached a mature stage of its own digital transformation journey. To achieve its strategic objectives, OLAF had to: build business capabilities for detecting, preventing, and investigating fraud; support anti-fraud policies by operating trans-European IT systems; collect, manage, and analyse data to produce intelligence; collaborate and exchange with stakeholders; all while ensuring security and trust. At the heart of this entire endeavour have always been data and OLAF's intention to transform itself into a data-driven organisation, i.e., to manage its data assets in such a way as to facilitate or even completely automate decision-making related to investigative activities.

For digital transformation to become a reality, certain digital capabilities should be in place as necessary preconditions or enablers:

- **Digital, data, and security governance:** Governance is the necessary condition for digital initiatives and operations to thrive and survive long term. It should cover, end to end, all types of business categories and their processes, technologies, services, and collected information within the responsibility of OLAF. Governance is organised in tiers to align with different expectations related to decisional power and accountability – starting with the top, where decisions are made on strategic alignment, portfolio prioritisation, policies and critical procedures, resources and risk, and where innovation is steered; to lower levels, which deal with projects, systems, changes, user support, and operations. An equally important function of governance is to set the principles shaping digital work, i.e., digital-by-default for all new business processes, one-stop-shop for access to data, reuse-first when it comes to developing a new information system, security-by-design to ensure that security is considered early in the design of any software application, etc., and to ensure they apply horizontally and establish a homogenous digital landscape across the Office.
- **Modern digital culture and workplace:** The digital transformation of business is doomed if the people who run businesses do not embrace the relevant changes. Considering that change in a work context is often synonymous with disruption, the first to steer change is management, who should mentor and lead by example and communicate to general staff the positive effects of change initiatives via awareness-raising campaigns and training sessions. A digitally-rich environment is also required, well-adapted to the specific requirements of a business, such as security and privacy, mobility, and remote access; this includes corporate and interconnected applications for resources, document, mission, time, financial, procurement management, collaboration with internal and external stakeholders. The cost of such transformation should not be neglected, as technology evolves fast and (especially) equipment is depreciated (financially and technologically) within a few years. The pace of technological transformation should be carefully assessed with view to the return on investment and be kept proportional to benefits produced. The Office is involved in such a continuous effort, by taking part in relevant corporate Commission IT initiatives and whenever necessary developing local/on-premises digital solutions best suited to its own needs (business or security related).

- **Digital transformation of business processes and data:** In the recent years, OLAF's digital transformation took off. Specifically, this concerned redesigning and streamlining processes within the Office and introducing the technical means to automate as much as possible. An example is the OLAF Case Management (OCM) system, which replaced its predecessor CMS and organises the lifecycle of cases throughout their different phases – i.e., selection, investigation, and monitoring – using features such as fully automated workflows based on manually or automatically generated activities and tasks, certificate-based user authentication, digital document signing and timestamping, remote access, integrated reporting, etc. OCM exports certain datasets to another internal environment (GET Intelligence), which is interconnected with other OLAF and Commission data sources to combine, analyse, and produce intelligence for analysts and investigators.
- **Innovation:** OLAF has long been using cutting-edge digital technologies in areas such as digital forensic examination and operational analysis in its own data and Open Source Intelligence (OSINT) environments. Although OLAF is not a research or technological organisation, whose sole purpose would be to produce innovation, the Office is open to using innovative digital technologies to improve the quality and speed of investigations and maximise impact in the anti-fraud domain. Nowadays, the Office is exploring how to benefit from the most influential example of innovation, Artificial Intelligence (AI), which is expected to influence and accelerate the way certain administrative and investigative tasks are conducted. In pursuit of innovation, a "right to fail" should be accepted, as failures feed future activities in the form of lessons learnt.

III. Looking Ahead, or What Does the Future Hold?

It comes as no surprise that there has been a paradigm shift in the way OLAF works when you compare its digital operations today with the situation 25 years ago, when the Office was first created. Digital processes are now at the core of its activities.

Yet we also need to acknowledge that investigations carried out by the Office can invade the privacy of those investigated. It goes without saying that the Office fully respects the applicable, stringent rules on data protection, and these go a long way towards ensuring an adequate balance between privacy and the effectiveness of investigations. But looking at current digital developments, the question arises whether OLAF's legal framework itself should evolve in lockstep with this digital transformation.

That said, the experience of the last quarter of a century has also shown that several regulatory mechanisms combined are able to largely guarantee an adequate protection of fundamental rights, privacy, and due process:

- Firstly, the legislative framework was relatively modern to start with; the digital era was already on the horizon as the 1999 OLAF Regulation was taking shape. This in mind, the legal text could incorporate certain aspects, even if it is not always very explicit. This is most noticeable in the above-described way that the term "data" was given centre stage as the basis of all of OLAF's digital work. Moreover, it is also likely that the 1998 *Tzoanos* judgement[30] that preceded OLAF's establishment by one year had opened the door to the concept of digital forensic operations, probably the most privacy-sensitive OLAF operation of all. The legal language of Art. 4(2) of the 1999 OLAF Regulation, including the use of the term "any data medium", is unusually detailed compared to other provisions and a clear testimony to the fact that the Union legislature intended to provide a basis for this key digital operation in the new regulation.
- Secondly, as a matter of regulatory technique, there is much to be said in favour of not overregulating technical details at the level of a basic regulation. This could lock in existing technologies and thus hinder the uptake of future innovations. The sections above show through how many digital transformations the Office has gone in the past years. Rather, implementing acts which are at least binding on the administration can often be updated in a more agile manner. The *Guidelines on Investigation Procedures for OLAF Staff*[31], which are regularly updated, and the aforementioned *Guidelines on Digital Forensic Procedures for OLAF Staff* are good examples of this approach.
- Thirdly, the OLAF Regulation naturally does not exist in isolation, but is firmly embedded in the EU's wider regulatory framework. This includes, for the present purposes, in particular Regulation 2018/1725 on data protection, the EPPO Regulation 2017/1939[32], and the AI Act[33]. In many respects, OLAF's digital practices are conditioned by these important legal acts, making it unnecessary for all issues to be separately addressed in the OLAF Regulation.
- Last but not least, jurisprudence from Luxembourg safeguarding the rights of individuals and companies in a large variety of cases will always be a driver for regulatory innovation.

This finding of a broadly adequate overall legal framework applicable to OLAF's digital operations notwithstanding, one can always legitimately ask where there is room for improvement.

The following section contains three examples, all taken from the context of OLAF's ongoing digital transition. They illustrate the need to continuously reflect on the appropriate level of prescriptive detail i Union legislation, in light of the invasive nature of some of OLAF's digital operations, especially to the privacy of natural persons.

1. Processing of cloud-based data by OLAF

First of all, it is clear that increasing amounts of data are no longer stored on a specific device or in a local network environment (work-related or otherwise), but in a cloud configuration hosted and operated by private companies. There are two elements of concern associated with the well-established technological trend of cloud use:

- *OLAF access to data stored in the cloud for investigative purposes:* OLAF Regulations do not include specific provisions for services delivered by and data hosted in the cloud; this means that the cloud is to be considered a typical digital technology, storing data subject to access or acquisition by the Office. The associated challenges are both procedural, i.e., data managed by a third party (cloud provider) who is unrelated to the investigation, but also technical, i.e., special tools needed to get access to and download cloud-based data, bandwidth restrictions, security, etc. A possible approach would be to include cloud-related provisions in revised guidelines (e.g., on digital forensic) and in operational and technical procedures driving investigative work.
- *Use of the cloud for OLAF-operated information systems and data:* The technological shift to the cloud has been widely embraced by the IT of the Commission for applications related to office automation, but also more generally for IT system development, in the latter case by applying the "cloud-first" approach which means that new information systems should be designed in such a way that they can be deployed in the cloud, whereas existing ones should be assessed for technical transformation to the cloud.[34] OLAF might, at some point in time, develop a cloud-specific policy following a careful assessment of its exposure to and potential use of the cloud to benefit from this technology's scalability, flexibility, and availability whilst minimising risks related to security, vendor lock-in, and limited visibility in data processing.

2. OLAF work on artificial intelligence

Like many other modern administrations, OLAF is also in the process of reflecting on to what extent the potential of new tools based on Large Language Models (LLM)/artificial intelligence could be harnessed to make OLAF's operations more efficient and more effective.[35] These deliberations are of course undertaken in full compliance with the AI Act, applicable data protection rules, and the Charter of Fundamental Rights of the European Union. It is obvious that AI tools will always be limited to a support role in anti-fraud prevention and investigation. The objective of the prudent use of AI by anti-fraud authorities must be to render the decision-making of human anti-fraud investigators more efficient and effective, and never to replace it.

However, from a regulatory perspective, OLAF's administrative investigations are not easy to categorise under the AI Act. *Prima facie,* OLAF's administrative processes cannot be considered "law enforcement" for the purposes of identifying which use of an AI tool has to be considered high-risk.[36] From the point of view of assessing AI-related risks, it seems more adequate to assimilate OLAF's administrative investigations with "administrative proceedings by tax and customs authorities", which are not generally considered high-risk under the AI Act.[37]

3. OLAF access to relevant data

Lastly, the question of how effectively OLAF can protect the financial interests of the Union in the digital era to some extent depends on the access that OLAF has to the right sets of data. But where to find that data depends not least on how spending and the corresponding reporting obligations are organised.

The Recovery and Resilience Facility (RRF) introduced a novel *modus operandi* for Union expenditure, which contributed significantly to the rapid disbursement of funds. In implementing the Facility, the Member States, as beneficiaries or borrowers of funds under the Facility, shall take all the appropriate measures to protect the financial interests of the Union and to ensure that the use of funds in relation to measures supported by the Facility complies with the applicable Union and national law, in particular regarding the prevention, detection, and correction of fraud, corruption, and conflicts of interests. To this effect, the Member States shall provide an effective and efficient internal control system and the recovery of amounts wrongly paid or incorrectly used. Member States may rely on their regular national budget management systems.[38]

From a data perspective, the hybrid control approach taken in the RRF poses challenges in terms of data availability. Each Member State has put their own reporting mechanisms in place to meet the RRF requirements. These fragmented data structures inevitably do not make it easier for the Office to investigate any irregularities, raising the question of how this could be remedied.

IV. Conclusions

OLAF's digital journey over the past quarter of a century was marked by the need to align its legislative and operational configuration with the rapid technological advancement of the digital landscape. As a result, that period witnessed a shift of paradigm towards the today well-established data-driven and digital-first principles.

As the digital revolution is still in full swing, especially with the advent of artificial intelligence, there is a strong case to maintain an overall regulatory approach where references in OLAF legislation to data access/handling remain high-level. Likewise, legislation should include provisions on digital aspects in a technologically neutral manner; specificities related to digital tools and processes should be formalised separately to allow for changes following the dynamic nature of information technology. Personal data protection matters are adequately addressed by the applicable general legislation. Operational/business related processes should be subject to working arrangements with the stakeholders or internal operational procedures. Overall, this carefully balanced approach has proven to be an efficient and flexible way to deliver OLAF's core businesses and to innovate, whilst adequately protecting fundamental rights and privacy.

We should also acknowledge that advancements in technology have a direct impact on the effectiveness of OLAF's operations. Fraudsters are making wide use of the latest technology to commit fraud smarter and faster, covering up their tracks. OLAF should not only technologically follow and be efficient and effective in detection and evidence production; especially when it comes to prevention we should be technologically mature to analyse relevant big amounts of data and produce intelligence which would allow, as appropriate, OLAF, the other European anti-fraud actors or the active national anti-fraud authorities to take up action as early as possible.

Unfortunately, technology has a cost, especially when it serves extraordinary forensic and analysis needs delivered under strict security requirements for the sensitive data OLAF manages. In the view of the authors, necessary financial provisions should be made to ensure a sound technological environment. Similarly, OLAF like many other anti-fraud authorities will have to continue invest to digitally educate staff members on how to lawfully reap all possible benefits technology can bring to their professional mission.

Last but not least, we are witnessing the – inevitable and important – arrival of self-thinking software and machines such as AI in support (but never in control) of anti-fraud activities. We need to acknowledge that these are not only offering a powerful support, but also come with risks. The use of state-of-the-art technologies, especially AI, within OLAF's digital ecosystem, should be subject to scrutiny and assessment for compliance with the relevant legislation and organisation's policies.

---

* This article only reflects the authors' personal opinions and cannot be attributed to the institution that employs them.

1 Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ L 136,31.5.1999, 1.

2 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, 1.

3 Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, OJ L 437, 28.12.2020, 49.

4 *AG Jacobs,* Opinion of 3 October 2002 in Case C-15/00 *Commission vs. EIB*, at para. 159.

5 Emphasis added.

6 Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, 2.

7 See on this point also ECJ, judgment of 28 October 2021 in Case C-650/19 P, *Vialto*, para. 70.

8 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, of 21.11.2018, p. 39.

9 Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-fraud Office (OLAF), OJ L 136, 31.5.1999, 22.

10 See the example in the judgment of the Court of First Instance of 19 March 1998 in Case T-74/96, *Georges Tzoanos v Commission of the European Communities,* paras. 319–322, relating to facts arising prior to the adoption of the 1999 OLAF Regulation.

11 The Guidelines are available at: <https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?filename=guidelines_en_bb84583638.pdf> accessed 7 February 2025.

12 ECJ, *Vialto*, *op. cit.* (n. 7), paras. 70–74.

13 GC, 20.5.2021, Case T-482/20, *LG and Others v Commission*, paras. 51–62.

14 See Commission Decision 2018/1962 of 11 December 2018, OJ L 315, 12.12.2018, p. 41.

15 Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, OJ L 82, 22.3.1997, 1.
16 See *E. Porebska,* "Paving the Way for Improved Mutual Assistance in the Context of Customs Fraud", (2016) *eucrim*, pp. 52–55.
17 Art. 36 of Regulation 608/2013 of 12 June 2013 concerning customs enforcement of intellectual property rights, OJ L 181, 29.6.2013, 15.
18 Art. 6 of Regulation 116/2009 of 18 December 2008 on export of cultural goods, OJ L 39, 10.2.2009, 1.
19 Art. 19 of Regulation 428/2009 of 5 May 2009 on setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ L 134, 29.5.2009, 1.
20 Art. 11 of Regulation (EC) No 273/2004 of 11 February 2004 on drug precursors as amended by Regulation 1258/2013, OJ L 41, 18.2.2004, 1, and Art. 27 of Council Regulation (EC) No 111/2005 of 22 December 2004 laying down rules for the monitoring of trade between the Community and third countries in drug precursors as amended by Regulation 1259/2013, OJ L 22, 21.1.2005, 1.
21 Art. 14 of Directive 2014/28/EU of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses, OJ L 96, 29.3.2014, 1.
22 Arts. 19–20 of Regulation 258/2012 of 14 March 2012 on Implementing Article 10 of the UN Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, OJ L 94, 30.3.2010, 1.
23 Art. 3 of Regulation 833/2014 of 31 July 2014 on restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 229, 31.7.2014, 1.
24 For an overview of the applicable data protection rules, see <https://anti-fraud.ec.europa.eu/olaf-and-you/data-protection_en#:~:text=OLAF%20maintains%20an%20independent%20register,conditions%20of%20the%20processing%20operations> accessed 7 February 2025.
25 See also in this sense the judgement of the General Court of 20 July 2016 in Case T-483/13 *Athanassios Oikonomopoulos v European Commission*, para. 60.
26 *Op. cit.* (n. 14).
27 GC, 26 June 2019, Case T-617/17, *Vialto*, para. 68; ECJ, 28 October 2021, Case C-650/19 P, *Vialto*, paras. 65–75.
28 In this context, the ECJ also made an analogy to anti-trust investigations and referred to its judgment of 16 July 2020 in Case C-606/18 P, *Nexans France*, para. 63.
29 See European Commission, "PM² Methodologies", <https://pm2.europa.eu/index_en> -> Project Management Methodology, accessed 7 February 2025.
30 *Op. cit.* (n. 10).

Konstantinos Bovalis
European Commission/European Anti-Fraud Office (OLAF), Head of Unit "Digital Strategy & Forensics"

Georg Roebling
European Commission/European Anti-Fraud Office (OLAF), Head of Unit "Intelligence & Operational Analysis"

31 The Guidelines are available at: <https://anti-fraud.ec.europa.eu/document/download/3dc10699-df07-4782-ae0d-232cd698286c_en?filename=gip_2021_en.pdf> accessed 7 February 2025.
32 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, 1.
33 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 2025/1689, 12.7.2024.
34 This approach calls for any new or upgraded information systems to be cloud-native, i.e., to have the potential of being easily put in the (private or public) cloud.
35 For a more detailed discussion of the use of AI-based tools by anti-fraud investigations see G. *Roebling and B. Necula,* "Reflections on Introducing Artificial Intelligence Tools in Support of Anti-Fraud", (2024) *eucrim*, 206–214.
36 See section 6 of Annex III of the AI Act, *op. cit.* (n. 33).
37 See in particular Recital 59 AI Act; similarly Recital 42 as concerns prohibitions.
38 Art. 22(1) of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, OJ L 82, 18.2.2021, 17, as amended.

The Protection of Fundamental Rights and Procedural Guarantees in OLAF Investigations: a 25-Year Journey

Diana Riochet and Nikoleta Mavromati*

The protection of fundamental rights and procedural guarantees in administrative investigations conducted by the European Anti-Fraud Office (OLAF) has constantly evolved since its creation in 1999. First, the catalogue of procedural rights and guarantees embedded in the successive regulations governing the conduct of OLAF's investigations was significantly expanded. Second, the existing mechanisms to ensure their protection were reinforced by the creation of the new function of the Controller of procedural guarantees and a new complaints mechanism. As a result, the legal framework under which OLAF operates at present is significantly more protective of fundamental rights and procedural guarantees than it was 25 years ago.

This article sheds light on these two key developments: the progressive codification of fundamental rights and procedural guarantees applicable to OLAF's investigations and the reinforcement of their protection by the creation of the new Controller and the new complaints mechanism.

I. Introduction

Throughout its 25 years of existence, OLAF has been operating under a composite legal framework.[1] The EU legislator not only vested OLAF with far-reaching investigative powers, but also gradually framed them by requiring OLAF to conduct its investigations in accordance with the provisions of EU primary and secondary law and with full respect for fundamental rights and procedural guarantees.[2]

The protection of fundamental rights and procedural guarantees applicable to OLAF's investigations has evolved significantly during this time, from Regulation 1073/1999[3] – the first regulation governing the conduct of OLAF investigations being almost silent in this respect – to the current Regulation 883/2013. The latter actually codified the applicable fundamental rights and procedural guarantees, and introduced, following its last amendment in 2020, a dedicated mechanism aimed at enforcing them.[4]

The evolution of the fundamental rights and procedural guarantees applicable to OLAF investigations is also reflected in OLAF's internal rules, which evolved alongside legislative changes. The current Guidelines on Investigation Procedures for OLAF Staff, adopted in 2021, reflect the changes introduced by the amended Regulation 883/2013, and replaced the Guidelines adopted in 2013.[5] Prior to these, OLAF had adopted Instructions to Staff on Investigative Procedures, which replaced a former OLAF Manual (both were based on the former Regulation 1073/1999).

II. The Progressive Codification of Fundamental Rights and Procedural Guarantees

When looking at how fundamental rights and procedural guarantees applicable to OLAF investigations have evolved from the early days of OLAF to the present, it is undeniable that their protection has matured along with the Office itself. This happened in different ways: (1) from the codification of what can now be seen as a catalogue of fundamental rights and procedural guarantees, to (2) a move to align, up to a certain extent, the rights and procedural guarantees applicable to external and internal investigations, and (3) the extension of protection to different categories of persons involved[6] in OLAF investigations.

1. An evolving catalogue of fundamental rights and procedural guarantees

The requirement to comply with fundamental rights has been anchored in the legislation governing the conduct of OLAF investigations since its creation in 1999. However, at the time, **Regulation 1073/1999** merely referred to the principles which OLAF was required to respect in general terms and in a recital: the principle of fairness; the right of persons involved to express their views on the facts concerning them; and the principle that the conclusions of an investigation may be based solely on elements which have evidential value.[7] These principles were not picked up specifically by concrete articles of the Regulation.

In addition, Regulation 1073/1999 defined some procedural guarantees – in relation to internal investigations

only – by way of cross-references to the internal decisions adopted by each EU institution, body, office, and agency.[8] Most of these internal decisions followed the model set out in the Interinstitutional Agreement of May 1999 between the European Parliament, the Council, and the Commission,[9] which sought to ensure that investigations can be carried out under equivalent conditions in these three institutions and in all other EU bodies, offices, and agencies adhering to it. The internal decisions integrate a rather slim set of procedural guarantees, requiring OLAF to inform the persons concerned in internal investigations of the opening of the investigation, or of the closing of the investigation with no further action taken; and to enable the persons concerned to express their views on all the facts concerning them before drawing conclusions referring to them by name (unless this obligation could be deferred, in cases necessitating the maintenance of absolute secrecy for the purposes of the investigation and requiring the use of investigative procedures falling within the remit of a national judicial authority).

Regulation 1073/1999 also guaranteed the protection of the confidentiality of information forwarded or obtained in the course of investigations, and of personal data.[10] Furthermore, the requirement to conduct investigations continuously over a period proportionate to the circumstances and complexity of the case was embedded in 1999[11] – and thus even before the right to have affairs handled within a reasonable period was enshrined in the Charter of Fundamental Rights of the European Union as a component of the right to good administration.[12]

These provisions were complemented by those set out in **Regulation 2185/96.** This Regulation has remained unchanged to date and forms the basis for on-the-spot checks and inspections by OLAF.[13] It includes the requirement that on-the-spot checks and inspections be carried out with due regard to the fundamental rights of the persons concerned and to the rules on professional secrecy and the protection of personal data, yet without being very detailed in this regard.

In parallel, and despite the scarcity of legal provisions in Regulations 1073/1999 and 2185/96, the EU Courts have progressively developed a catalogue of fundamental rights and procedural guarantees that OLAF must respect, based on the general principles of EU law. Indeed, fundamental rights are part of general principles of EU law and are also enshrined in the Charter of Fundamental Rights, which forms part of primary EU law that OLAF must comply with. Since the very first cases challenging the conduct of OLAF investigations,[14] the Courts have defined the conditions of application – in the specific context of OLAF investigations – of the rights of the defence and the right to be heard, the right of access to the file, the presumption of innocence, the right to an impartial investigation, and the reasonable-time requirement.

Regulation 883/2013 represented a major step forward in improving the protection of persons involved in OLAF investigations by codifying the fundamental rights and procedural guarantees applicable.[15]

Art. 9 of the Regulation – entitled "Procedural guarantees" – requires OLAF to seek evidence for and against the person concerned, and to conduct investigations objectively and impartially and in accordance with the principle of the presumption of innocence. Art. 9 also lays down safeguards applicable in the context of interviews, benefitting persons concerned and witnesses: the right to avoid self-incrimination, the right to be informed of the opening of an investigation, guarantees regarding the notice period and the record of the interview, the right to be assisted by a person of choice, and language rights. Furthermore, Art. 9 provides for the right to be heard, in the form that the person concerned has the opportunity to comment on facts concerning him or her before OLAF draws up conclusions referring to that person by name.

Additional provisions protecting rights and procedural guarantees at different stages of the investigation complement this article: Art. 10 reinforces the confidentiality and data protection requirements applicable throughout the entire lifecycle of OLAF investigations; Art. 11 provides, with some limitations, for the right of the persons concerned to be informed about the closure of an investigation when no evidence has been found against them, and for the right of informants to be informed of the closure of an investigation.

The **amendments to Regulation 883/2013 (by Regulation 2020/2223)**[16] further extended the existing catalogue of fundamental rights and procedural guarantees applicable to OLAF investigations. Its major innovation was the introduction, in the context of administrative OLAF investigations, of procedural guarantees applicable to criminal investigations. When the Office carries out, within its mandate, supporting measures requested by the European Public Prosecutor's Office (EPPO), it must ensure, in close cooperation with the EPPO, that the applicable procedural safeguards of Chapter VI of the EPPO Regulation are observed.[17] The amended Regulation also introduced, for the first time, in cases in which OLAF recommends a judicial follow-up, a right for the persons concerned to request from OLAF a copy of the final report.[18]

2. The progressive yet partial alignment of fundamental rights and procedural guarantees in internal and external investigations

While Regulation 1073/1999 required OLAF to conduct its investigations "with full respect for human rights and fundamental freedoms",[19] the few provisions protecting the rights and procedural guarantees of the persons concerned explicitly listed were limited to internal investigations, without any mention of persons concerned in external investigations. Over the years, both the EU legislator and the General Court have bridged this gap.

Conversely, Regulation 883/2013 laid down the principle that the procedural guarantees and fundamental rights of persons concerned and of witnesses should be respected **without discrimination** at all times and at all stages of **both external and internal investigations**[20] from the outset.

As such, most of the fundamental rights and procedural guarantees set out in Art. 9 therefore apply, without distinction, to both external and internal investigations. A notable exception concerns the right to be informed of the opening of an OLAF investigation. While Art. 9(3) provides for an EU official, other servant, member of an institution or body, head of office or agency, or staff member to be informed as soon as an OLAF investigation reveals that they may be persons concerned, there is no similar obligation for persons concerned in external investigations.

However, the General Court extended this obligation, by analogy, to external investigations. [21] Its approach is based on the general principle of respect of the rights of the defence. On the one hand, the Court noted that neither Regulation 2185/96 nor Regulation 1073/1999 contained an obligation – applicable at the time of the case before the Court – to inform a natural person as part of external OLAF investigations; on the other hand, it ruled that observance of the rights of the defence is sufficiently guaranteed in external investigations if, in line with what is provided for in relation to internal investigations, the person is promptly informed of the possibility of personal involvement in acts of fraud, corruption, or illegal activities detrimental to the interests of the Union, provided that information does not interfere with the investigation. Later on, the General Court extended this protection to *legal* persons concerned in external OLAF investigations.[22]

Therefore, both the legislative modifications and the case law developments indicate a clear move to align the rights and procedural guarantees applicable to external and internal investigations and thus to reinforce the protection of the persons concerned.

That said, it is also clear that such an alignment can never be comprehensive, as external and internal investigations follow, in part, distinct rules.[23] The most obvious example is the distinction made with regard to language rights of persons interviewed by OLAF in external and internal investigations. In the context of interviews, persons concerned in external investigations are entitled to use any of the official languages of the institutions of the Union, while EU officials or other servants who are persons concerned in internal investigations may be requested to use an official language of the institutions of the Union of which they have a thorough knowledge.[24] Likewise, the conditions for deferring the opportunity to comment provided to persons concerned before drawing conclusions (see above 1.) are different for external and internal investigations. In internal investigations, the deferral requires the prior consent of the Secretary-General or the equivalent authority of the institution, body, office, or agency to which the member or official concerned belongs,[25] whereas such a requirement does not exist in external investigations.

3. A gradual extension of the categories of persons protected

The few procedural guarantees included in Regulation 1073/1999 were originally designed to protect **persons concerned** only. The Regulation did not cover other categories of persons involved in OLAF investigations and their rights and procedural guarantees.

Regulation 883/2013 remedied this gap by including, for the first time, a requirement for OLAF to respect the procedural guarantees and fundamental rights of **witnesses**.[26] Witness rights encompass the right to avoid self-incrimination during an interview, safeguards taking effect when, in the course of an interview, evidence emerges that a witness may be a person concerned, rules on the notice period for the invitation to an interview, and procedural guarantees linked to the interview record (i.e., the possibility to have access to it in order to either approve the record or add observations).[27]

In addition, the initial version of Regulation 883/2013 referred, for the first time, to **sources of information**. It included the obligation for the Office to inform EU whistle-blowers (i.e., EU staff members or members of an EU institution, body, office, or agency who act in accordance with Art. 22a of the Staff Regulations) of the decision whether or not to open an investigation.[28] The Regulation also provided that, in cases where no internal investigation was opened but information was sent to the institution, body, office, or agency concerned, OLAF was to agree with that institution, body, office, or agency, on suitable measures to protect the confi-

dentiality of the source of that information, where appropriate.[29] Lastly, another noteworthy reference was the mention of the protection of journalistic sources, even though it was relegated to a recital.[30]

Despite these improvements, the protection afforded to sources of information seemed to be rather rudimentary in the initial version of the Regulation. This is why the amended Regulation 883/2013 (see above) represents a significant legislative step forward in the protection of sources of information, in various ways. The most notable one is the reinforced protection granted to **whistle-blowers** by means of including an explicit reference to the 2019 "Whistleblowing Directive".[31] The Directive applies to the reporting of fraud, corruption, and any other illegal activity affecting the financial interests of the Union and the protection of persons reporting such breaches.[32] The protection afforded by the Directive thus complements the protection already granted to EU whistle-blowers, which remained unchanged in the amended Regulation 883/2013.

In addition, while the amended Regulation now stipulates that a person concerned may request from OLAF a copy of a final report drawn up in cases where it recommended a judicial follow-up, it also limits the extent to which OLAF can provide such a copy. The exercise of this right by the persons concerned is subject to, among other conditions, respect of the confidentiality rights of **whistle-blowers and informants**.[33] Likewise, the extent to which the Director-General of OLAF reports to the European Parliament, the Council, the Commission, and the European Court of Auditors on OLAF investigations is also limited by the requirement to respect the rights of informants.[34]

Finally, yet importantly, the amended Regulation added an obligation for OLAF to notify an **informant** who has provided the Office with information that led to an investigation of the closure of that investigation.[35]

III. The Reinforcement of Mechanisms to Ensure Compliance with Fundamental Rights and Procedural Guarantees Applicable to OLAF Investigations

In addition to codifying the fundamental rights and procedural guarantees applicable to OLAF investigations, Regulation 883/2013 significantly reinforced their protection by improving the mechanisms designed to ensure that OLAF complies with them.

First, unlike its predecessor (Regulation 1073/1999), Regulation 883/2013 introduced a new internal advisory and control procedure, including an internal legality check relating to, *inter alia,* the respect for procedural guarantees and fundamental rights of persons concerned.[36] This legality check is performed by a review team dedicated to the task, both during and after the closure of the investigation, which verifies the legality, necessity, and proportionality of the activities undertaken during the investigation, and the respect of the rights of the persons concerned throughout the investigative procedure.[37]

Second, Regulation 883/2013 also formalised and clarified the role of the Supervisory Committee to monitor developments related to the application of procedural guarantees and the duration of OLAF investigations.[38]

Third, and most notably, the amended Regulation 883/2013 complemented the existing external avenues of judicial and non-judicial review available to all persons alleging a violation of their procedural rights by OLAF.

Judicial review may be sought directly before the EU Courts, via actions for annulment[39] or actions for damages[40], or indirectly, particularly via the preliminary reference procedure[41]. In addition, complaints concerning the protection of personal data can be brought before the European Data Protection Supervisor[42] while complaints concerning maladministration by OLAF can be brought before the European Ombudsperson[43]. Nevertheless, the absence, in both Regulation 1073/1999 and the initial version of Regulation 883/2013, of a formal procedure for handling individual complaints by persons concerned had long cast doubt on whether the existing mechanisms were indeed sufficient to safeguard fundamental rights and procedural guarantees in all circumstances.[44] After a long legislative journey,[45] the gaps identified were finally addressed by the latest amendments introduced through Regulation 2020/2223,[46] which established a new Controller of procedural guarantees and a complaints mechanism dedicated to it.

1. A new Controller of procedural guarantees

Pursuant to the new Art. 9a of the amended Regulation 883/2013, *"[a] Controller of procedural guarantees shall be appointed by the Commission"*. Accordingly, on 3 May 2022, the European Commission appointed *Julia Laffranque* as the first Controller of procedural guarantees for a non-renewable term of five years. The Controller took office in September 2022 and subsequently adopted the first Implementing Provisions for the handling of complaints in November 2022.[47]

The Controller handles individual complaints lodged by persons concerned regarding OLAF's compliance with the

procedural guarantees referred to in Art. 9 of Regulation 883/2013, as well as on the grounds of an infringement of the rules applicable to OLAF investigations,[48] in particular infringements of procedural requirements and fundamental rights. Of specific importance is the fact that the Controller cannot interfere with the conduct of an ongoing investigation, as such actions would constitute a breach of OLAF's independence.[49] Nor does the Controller seek to substitute her own assessment for that of OLAF. For instance, he or she may not interfere with the Director-General's decision on whether to open an investigation, the choice of investigative measures, the assessment of evidence, or the conclusions reached.[50] Instead, through actions suggesting how to resolve complaints and, ultimately, recommendations to the Director-General of OLAF, the Controller aims to resolve the issues raised by the complaint and, in a forward-looking manner, to improve OLAF's administrative and investigative practices.[51] For these reasons, the lodging of a complaint is deprived of any suspensive effect on the conduct of the OLAF investigation in question.[52]

Although the Controller is administratively attached to the Supervisory Committee of OLAF, he or she carries out his or her duties in full independence, including from the Supervisory Committee and OLAF, and shall neither seek nor take instructions from any party in the performance of his or her duties.[53] To assess complaints in a fair, independent, and impartial manner, the Controller is entrusted with information gathering powers, including through privileged access to the case file of the relevant OLAF investigation.[54] This direct access to OLAF case-related documents ensures that the Controller can thoroughly examine OLAF's investigative activities. He or she is bound to ensure that all information and documents provided by OLAF are treated confidentially and to protect the confidentiality of OLAF investigations, even after their closure.[55]

Lastly, yet again importantly, the Controller's added value is further reinforced by his or her ability to provide tailored advisory opinions, upon request of the Director-General of OLAF,[56] and to inform the Supervisory Committee of any systemic issues revealed through the assessment of complaints.[57]

2. A new complaints mechanism

The amended Regulation 883/2013 complemented the function of the Controller with the creation of a new complaints mechanism, established under Art. 9b. The mechanism comprises two distinct stages: (i) the assessment of the admissibility of the complaint and, if a complaint is admissible, (ii) the assessment of the substantive arguments raised by the complainant.

At the **admissibility stage**, the Controller assesses whether the complaint was lodged in compliance with the conditions set out in paragraphs 1 and 2 of Art. 9b of the amended Regulation 883/2013, as well as Arts. 5 and 6 of the Implementing Provisions (see above 1.). In particular, the complaint must be filed by a person concerned by an OLAF investigation,[58] alleging non-compliance by OLAF with the complainant's procedural guarantees, fundamental rights, and/or the rules applicable to OLAF investigations. For the complaint to be admissible, it should be lodged within one month of the complainant becoming aware of the relevant facts that constitute an alleged infringement of the procedural guarantees or the rules on investigation, and in any event, no more than one month after the closure of the investigation that is the subject of the complaint. Complaints related to the notice period referred to in Art. 9(2) (invitation to an interview) and Art. 9(4) (invitation to persons concerned to comment on facts concerning them) of Regulation 883/2013 must be lodged before the expiry of the 10-day notice period referred to in those provisions.[59] Furthermore, the complaint must not be manifestly without merits, repetitive, or abusive, and the matter of the complaint must not be the subject of any legal proceedings before either an EU or a national court.[60] In all instances where complaints are deemed inadmissible, the Controller closes the file and promptly notifies both the complainant and the Director-General of OLAF, providing the reasons of her decision.

Following the admission of a complaint, the Controller proceeds with an **assessment on the merits**, ensuring full adherence to the adversarial principle.[61] To this end, the Controller invites both OLAF and the complainant to present their arguments, to submit any supporting documentation, and to comment on each other's submissions within a specified time frame.[62] Additionally, the Controller may organise and conduct hearings with the participation of both OLAF and the complainant, with the aim of gathering relevant information and/or seeking a prompt resolution to the complaint.[63]

This adversarial nature of the complaints mechanism is balanced against the need to maintain the confidentiality of the OLAF investigation. In this regard, the Controller may decide not to disclose certain information or materials to the complainant, if doing so is necessary to protect the confidentiality and efficiency of the OLAF investigation, while still respecting the adversarial principle. Similarly, the adversarial procedure cannot be used by the complainant as a means to obtain access to documents from the OLAF case file to which the complainant is not entitled under other legal provisions, or documents to which OLAF has already denied access.[64]

Following the assessment of the collected information and evidence, the Controller either finds no breach of the complainant's fundamental rights and/or procedural guarantees or the rules applicable to OLAF investigations and therefore closes the case, or concludes that OLAF did not comply with them. In the latter case, the Controller invites OLAF to take appropriate action to resolve the complaint and inform the Controller accordingly within 15 working days.[65] If the solution provided by OLAF is deemed unsatisfactory, or if no information is received within the 15-day time limit, the Controller shall issue a recommendation on how to resolve the complaint, after consulting the Supervisory Committee for its opinion.[66] The recommended actions may include, *inter alia,* the amendment or repeal of OLAF's recommendations or reports, the repetition of investigative activities, or the introduction of improvements in OLAF's procedures concerning the matters raised in the complaint.[67] The Director-General of OLAF may, however, decide not to follow the Controller's recommendation, providing the main reasons for such decision.[68]

Finally, it should be noted that the complaints mechanism described above is without prejudice to the means of redress available under the Treaties.[69]

3. A two-year snapshot: early outcomes and key insights

During her first two years of operational activity (2022–2023)[70], the Controller received 31 complaints, 13 of which were already under OLAF's review, pending the Controller's appointment. Most of the complaints were submitted in English. 19 complaints were lodged by individuals who were persons concerned in OLAF internal investigations, while 11 complaints concerned external investigations, and one complaint related to coordination activities. Out of the total of 31 complaints, 20 were deemed admissible, while 11 were deemed inadmissible, mostly due to non-compliance with the time limits set in Art. 9b(2) of the amended Regulation 883/2013. As to the result of the cases decided by the end of 2023, 13 complaints were closed with no breach of the complainants' procedural guarantees found. In one instance, the Controller closed the case because the complainant had brought the same issues before a court, while two other cases were closed after OLAF accepted the Controller's invitation to resolve the complaint. One further complaint was closed for lack of interest of the complainant to pursue the matter before the Controller.

In most cases, the complainants alleged violations of their procedural guarantees under Art. 9 of Regulation 883/2013, as well as infringements of their fundamental rights as outlined in the Charter of Fundamental Rights. The complaints primarily dealt with the following: (i) the right to be heard and the effective exercise of their right to submit observations on facts concerning them (Art. 9(4)); (ii) the right to be informed (Art. 9(3)); (iii) violations of the principles of fairness, objectivity, and impartiality in the conduct of investigations; (iv) the right to have their affairs handled within a reasonable time frame (Art. 41 of the Charter of Fundamental Rights); and (v) the language regime governing the investigations. Additionally, complainants raised concerns regarding the applicable rules governing OLAF investigations, particularly in relation to on-the-spot checks, interviews, and digital forensic operations.[71]

IV. Conclusion

The successive modifications of the legal framework governing the conduct of OLAF investigations have led to major improvements when it comes to the protection of fundamental rights and procedural guarantees of persons involved in such investigations. Regulation 883/2013, in its initial and amended versions, codified a number of fundamental rights already protected under the Charter of Fundamental Rights and the general principles of EU law, as interpreted by the Court of Justice of the EU, as well as procedural guarantees associated with specific investigative activities, such as interviews. Not only did it develop a catalogue comprising more rights and procedural guarantees than those foreseen when OLAF was created, but it also gradually extended the level of protection to all categories of persons involved in OLAF investigations.

From an enforcement perspective, the establishment of the Controller of procedural guarantees has also marked a pivotal development in protecting the rights and procedural guarantees of persons concerned in OLAF investigations. Operating through a structured and transparent complaints mechanism designed for dealing with individual complaints, the Controller not only safeguards the rights of those subject to OLAF investigations, but also enhances the overall integrity and credibility of OLAF's investigative processes. This new mechanism serves as an additional layer of protection, designed to progressively achieve a fair and effective balance between OLAF's operational efficiency and the robust protection of the procedural rights of persons concerned. Looking ahead, the Controller's role holds clear potential for continuous improvement in the area of procedural safeguards, reflecting a strong commitment to upholding fundamental rights and fostering public trust in OLAF investigations.

Therefore, we can confidently say that, 25 years after its creation, OLAF has matured – and so has the protection of the fundamental rights and procedural guarantees of the persons involved in its investigations.

---

* The views expressed in this article are exclusively those of the authors and cannot be attributed to the institution that employs them.

1 For OLAF's legal background, see <https://anti-fraud.ec.europa.eu/about-us/legal-background_en>. All hyperlinks in this issue were last accessed on 28 November 2024.

2 For an overview of the legislative history on procedural safeguards applicable to OLAF investigations, see the European Parliament's briefing "Investigations conducted by the European Anti-Fraud Office (OLAF)", 2014, available at: <https://www.europarl.europa.eu/RegData/etudes/note/join/2014/536335/IPOL-IMPT_NT(2014)536335_EN.pdf>; see also K. Ligeti, "The protection of the procedural rights of persons concerned by OLAF administrative investigations and the admissibility of OLAF Final Reports as criminal evidence", (2017), available at: <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603790/IPOL_IDA(2017)603790_EN.pdf>.

3 Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ L 136, 31.5.1999, 1. Similar provisions were embedded in Regulation 1074/1999 (OJ L 136, 31.5.1999, 8) relating to the Euratom Treaty. For the purpose of this article, reference is made only to Regulation 1073/1999. These regulations were complemented by other horizontal and sectoral EU legislation over the years – see: <https://anti-fraud.ec.europa.eu/about-us/legal-background_en>.

4 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, 1. This regulation was last amended in 2020 by Regulation 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, OJ L 437, 28.12.2020, 49. A consolidated version of Regulation 883/2013 with no legal effect is available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013R0883-20210117&qid=1732792374409>.

5 See the 2021 and 2013 Guidelines on investigations for OLAF staff at: <https://anti-fraud.ec.europa.eu/guidelines-investigations-olaf-staff_en>.

6 The term "persons involved" used in this article covers different categories of persons who may play a role in OLAF investigations. These are mainly the "persons concerned" within the meaning of Art. 2(5) of Regulation 883/2013. In addition, this term may cover witnesses, informants, and whistle-blowers.

7 Recital 10 of Regulation 1073/1999, *op. cit*. (n. 3).

8 Art. 4(1) and (6) of Regulation 1073/1999, *op. cit*. (n. 3).

9 Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office (OLAF), OJ L 136, 31.5.1999, 15.

10 Art. 8 of Regulation 1073/1999, *op. cit*. (n. 3).

11 Art. 6(5) of Regulation 1073/1999, *op. cit*. (n. 3).

12 Art. 41 of the Charter of Fundamental Rights of the European Union.

13 Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, 2. See in particular recital 12 and Art. 8.

14 CFI, 18 December 2003, case T-215/02, *Gómez-Reino v Commission;* CFI, 6 April 2006, case T-309/03, *Camós Grau v Commission*; CFI, 12 September 2007, case T-259/03, *Nikolaou v Commission*; CFI, 8 July 2008, case T-48/05*, Franchet and Byk v Commisison.*

15 For a detailed analysis of the rights and procedural guarantees set out in Regulation 883/2013, see K. Ligeti, *op. cit.* (n. 2), part 1.

16 *Op. cit.* (n. 4).

17 Art. 12e (3) of Regulation 883/2013 as amended by Regulation 2020/2023 (*op. cit.* (n. 4).

18 Art. 10(3b) of the amended Regulation 883/2013, which also limits the exercise of this right.

19 Recital 10 of Regulation 1073/1999, *op. cit*. (n. 3).

20 Recital 23 of Regulation 883/2013, *op. cit.* (n. 4).

21 GC, 20 July 2016, case T-483/13, *Oikonomopoulos v Commission*, paras. 228–231.

22 GC, 29 June 2022, T609/20, *LA International Cooperation Srl v Commission*, paras. 22–23.

23 Recital 21 of Regulation 883/2013, *op. cit.* (n. 4).

24 Art. 9(5) of Regulation 883/2013, *op. cit.* (n. 4).

25 Art. 9(4) last subparagraph of Regulation 883/2013, *op. cit.* (n. 4).

26 Recital 23 of Regulation 883/2013, *op. cit.* (n. 4).

27 Art. 9(2) of Regulation 883/2013, *op. cit.* (n. 4), the amended version of the Regulation did not change the provisions related to witnesses.

28 Art. 5(4) of Regulation 883/2013, *op. cit.* (n. 4).

29 Art. 5(5) of Regulation 883/2013, *op. cit.* (n. 4). The scope of this provision was extended in the amended Regulation 883/2013. It now also covers external investigations, and cases where information is sent to the competent authorities of the Member State concerned.

30 Recital 26 of Regulation 883/2013, *op. cit.* (n. 4).

31 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, OJ L 305, 26.11.2019, 17.

32 Art. 10(3a) of Regulation 883/2013 as amended by Regulation 2020/2023, *op. cit.* (n. 4).

33 Art. 10(3b) of the amended Regulation 883/2013.

34 Art. 17(4) of the amended Regulation 883/2013.

35 Art. 11(8) of the amended Regulation 883/2013. This article also makes it possible to derogate from this rule.

36 Art. 17(7) of Regulation 883/2013, *op. cit.* (n. 4).

37 Arts. 16 and 26 of the 2021 Guidelines on Investigation Procedures for OLAF Staff, *op. cit.* (n. 5).

38 Art. 15(1). See also CFI, *Franchet and Byk v Commisison, op. cit.* (n. 14), para. 168.

39 Art. 263 TFEU. Actions for annulment against OLAF's investigative acts are, in principle, inadmissible, as such acts are not deemed to affect the interests of the persons concerned by bringing about a distinct change in their legal position.

40 Arts. 268 and 340(2) TFEU.

41 Art. 267 TFEU.

42 Art. 57 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, OJ L 295, 21.11.2018, 39.

43 Art. 43 of the Charter of Fundamental Rights of the European Union and Regulation (EU, Euratom) 2021/1163 of the European Parliament of 24 June 2021 laying down the regulations and general conditions

Diana Riochet
European Commission/European Anti-Fraud Office (OLAF), Unit D2 "Legal Advice Unit", Deputy Head of Unit

Nikoleta Symela Mavromati
European Commission/European Anti-Fraud Office (OLAF), Unit D2 "Legal Advice Unit", Legal Assistant

governing the performance of the Ombudsman's duties (Statute of the European Ombudsman), OJ L 253, 16/07/2021, 1.

44 For a more extensive analysis, see European Commission, Commission staff working document, Analysis of Impacts "*Accompanying the document Proposal for a Regulation of the European Parliament and of the Council Amending Regulation No 883/2013 as regards the establishment of a Controller of procedural guarantees*", SWD(2014) 183 final. See also OLAF Supervisory Committee, Annual Activity Report 2012, in particular Section 2, Annex III; OLAF Supervisory Committee, Opinion 2/13 on "*Establishing an internal OLAF procedure for complaints*", December 2013. For an overview of judicial remedies against OLAF acts, see J.F.H. Inghelram, "Judicial review of investigative acts of the European Anti-Fraud Office (OLAF): a search for balance", (2012) 49 *Common Market Law Review*, pp. 601–628.

45 The idea for a Controller of procedural guarantees first appeared in the Commission Proposal of 11 June 2014, COM(2014)340 final. The proposal was highly contested and ultimately withdrawn. For the evolution of the proposal, see indicatively: OLAF Supervisory Committee, *Annual Activity Report 2014*, pp. 2–3; OLAF Supervisory Committee, Opinion 2/17 "*Accompanying the Commission Evaluation report on the application of Regulation (EU) of the European Parliament and of the Council No 883/2013*", 28 September 2017, pp. 26–28; Council of the European Union, "*Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 as regards the establishment of a Controller of procedural guarantees – Outcome of proceedings*", Council doc. 14075/14 of 27 October 2014.

46 Regulation (EU, Euratom) 2020/2223, *op. cit.* (n. 4).

47 Decision of the Controller of procedural guarantees adopting implementing provisions for the handling of complaints 2022/ C 494/07, OJ C 494, 28.12.2022, 17.

48 Such rules include the Guidelines on Investigation Procedures for OLAF Staff, *op. cit.* (5) and the Guidelines on Digital Forensic Procedures for OLAF Staff, available at: <https://anti-fraud.ec.europa.eu/investigations/digital-forensics_en>.

49 Art. 9b(6) of Regulation 883/2013 as amended by Regulation 2020/2023 (*op. cit.* (n. 4)).

50 The Controller's Annual Activity Report 2023, 19 July 2024, p. 5.

51 The Controller's Annual Activity Report 2023, *op. cit.* (n. 50), pp. 2–3.

52 Art. 9b(1) of the amended Regulation 883/2013.

53 Art. 9a(6) of the amended Regulation 883/2013.

54 Implementing provisions, *op. cit.* (n. 47), Art. 8(1) and (2).

55 Art. 9a(9) of the amended Regulation 883/2013.

56 Art. 9b(9) of the amended Regulation 883/2013.

57 Article 9a(9) of the amended Regulation 883/2013.

58 Currently, other persons involved in an OLAF investigation, such as informants, whistle-blowers, or witnesses, may lodge a complaint with the Director-General of OLAF. In addition, EU staff members may submit a request or complaint to the Director-General of OLAF pursuant to Art. 90a of the Staff Regulations in respect of any act adversely affecting them in the context of an OLAF investigation. Further details can be found on OLAF's dedicated website for complaints and requests, available at: <https://anti-fraud.ec.europa.eu/olaf-and-you/complaints-and-requests_en>.

59 Art. 9b(2) of Regulation 883/2013 as amended by Regulation 2020/2023 (*op. cit.* (n. 4)).

60 Implementing provisions, *op. cit.* (n. 47), Arts. 5(5) and 6.

61 Art. 9b(6) first subparagraph of the amended Regulation 883/2013.

62 Implementing provisions, *op. cit.* (n. 47), Art. 7.

63 Implementing provisions, *op. cit.* (n. 47), Art. 9.

64 Implementing provisions, *op. cit.* (n. 47), Art. 7(2).

65 Art. 9b(3) third subparagraph of the amended Regulation 883/2013; Implementing provisions, *op. cit.* (n. 47), Art. 11 (1) and (2).

66 Art. 9b(5), first subparagraph of the amended Regulation 883/2013.

67 Art. 9b(5), third subparagraph of the amended Regulation 883/2013; Implementing provisions, *op. cit.* (n. 47), Art. 12(4).

68 Art. 9b(7) of the amended Regulation 883/2013.

69 Art. 9b(8) of the amended Regulation 883/2013.

70 These figures are derived from the Controller's Annual Activity Reports for 2022–2023. As of the date of this article's publication, the 2024 Annual Activity Report has not yet been released.

71 For an analytical overview of the complaints raised in 2022–2023, see the Controller's Annual Activity Reports 2022 and 2023, available at: <https://supervisory-committee-olaf.europa.eu/controller-procedural-guarantees/annual-activity-reports_en>.

Protecting EU Taxpayer Money together with Global Partners

25 Years of International Relations of the European Anti-Fraud Office

Lukáš Jelínek and Clemens Kreith*

The European Anti-Fraud Office (OLAF) was created 25 years ago, in 1999, to fight fraud, corruption, and any other illegal activities affecting the EU budget. While there are several anti-fraud actors at EU level, OLAF is unique with regard to its international activities. In particular, OLAF is mandated to conduct investigative activities directly on territory outside the EU. Against this background, the article traces the evolution of the EU legal framework for OLAF's international investigations and the parallel development of OLAF's international relations in practice. The analysis of OLAF's engagement with international partners focuses on several key activities of the Office to protect EU funds abroad, especially negotiating anti-fraud provisions in international instruments, concluding administrative cooperation arrangements with non-EU countries and international organisations, and building networks of partners around the globe. Looking back at the past quarter of a century, the article demonstrates that many features which are hallmarks of OLAF's international relations today can be traced back to the early years of the Office. The article also shows how these practices have grown and matured over time.

I. Introduction

In 1999, in the aftermath of the Santer Commission scandal, a Directorate of the Secretariat General of the European Commission was hastily converted into a fully-fledged Directorate-General *sui generis*. From its modest beginnings a decade earlier as a mere unit for the coordination of the fight against fraud with only 10 staff members, the then Anti-Fraud Coordination Unit (UCLAF) became the European Anti-Fraud Office (OLAF). At that time, few people could have imagined that a quarter of a century later OLAF would become one of the frontrunners of international cooperation and a model for similar entities established both at national and international level. Yet, when OLAF was set up, very little attention was paid to the Office's investigative powers beyond the borders of the EU. Instead, OLAF was given two seemingly straightforward tasks: to protect EU taxpayer money against fraudsters *wherever* the money goes; and to protect the reputation of EU institutions against misconduct of its members and staff *wherever* the misconduct happens.

Among the anti-fraud actors established at EU level, including Europol, Eurojust, the European Public Prosecutor's Office (EPPO), and to a certain extent the European Court of Auditors, OLAF is unique with regard to its international activities in two aspects:

- OLAF is mandated to conduct investigative activities directly on the territory of third countries and vis-a-vis international organisations.
- OLAF does not have a legal personality and acts as part of the Commission, not on its behalf.

In a former *eucrim* article on OLAF's investigations outside the EU, *Claire Scharf-Kröner* and *Jennifer Seyderhelm* already provided a snapshot of OLAF's international investigations and the underlying legal basis for investigative work outside the EU.[1] The present article therefore aims to complement the static dimension of the previous article with a dynamic perspective on the evolution of the legal framework and the parallel development of OLAF's international relations in practice.

To this end, the article will first examine the development of OLAF's basis for investigative powers in third countries within the EU's legal framework since the establishment of the Office in 1999. In the second part, the article will shed light on some practical aspects of OLAF's international relations, in particular regarding the protection of EU financial interests on the expenditure side of the budget (e.g., EU funds).[2] This will be done by tracing the evolution of three characteristic activities that have defined OLAF international engagement over the last 25 years, namely:[3]

- Including anti-fraud provisions in international instruments;
- Negotiating administrative cooperation arrangements;
- Building global and regional partner networks.

Looking back, the article will show that many features which define OLAF's international relations today have their foundation in the early years of the Office, even though they have gradually grown, expanded, and matured over the last quarter of a century.

II. Development of the Legal Framework for OLAF Investigations Outside the EU

By its Decision 1999/352,[4] the European Commission established OLAF as an investigative office whose mandate goes beyond the protection of EU financial interests.[5] Since 1999, the core legislation governing the Office's activities has nonetheless been based on the EU's primary law provision on countering fraud, i.e., Art. 280 of the Treaty establishing the European Community under the Amsterdam Treaty and – following the Lisbon Treaty – Art. 325 of the Treaty on the Functioning of the EU (TFEU). Even today, the protection of EU financial interests remains the main focus of the Office's external investigations carried out in accordance with Art. 3 of Regulation 883/2013[6] – OLAF's current main legal basis. Although the wording of Art. 325 TFEU refers to an EU *internal* shared competence, it also implicitly contains an external aspect.[7]

1. UCLAF powers

Even before the establishment of OLAF and before the Treaty of Amsterdam introduced the protection of EU financial interests as a competence shared between the EU and its Member States, UCLAF was able to exercise certain investigative powers in third countries. Regulation 945/87,[8] adopted by unanimity on the basis of what is now Art. 352 TFEU, introduced, under Art. 15b of Regulation (EEC) No 1468/81[9], a specific power of the Commission under which Commission officials were mandated to lead "Community administrative and investigative cooperation missions" in third countries in coordination and close cooperation with the competent authorities of the Member States. The same power is still exercised by OLAF investigators under Art. 20 of Regulation 515/97 in investigations in the area of fraud on customs and anti-dumping duties. In addition, Art. 8(5) of Regulation No 2185/96[10], also adopted by unanimity on the basis of what is now Art. 352 TFEU, recognised the possibility that Commission inspectors could carry out inspections outside of EU territory, but did not provide for any further conditions under which such inspections could be conducted.

2. OLAF powers under the founding 1999 Regulations

Hence, as UCLAF powers were rather limited, it was only by establishing OLAF and adopting legislation pursuant to the legal basis introduced by the Amsterdam Treaty in 1999, the foundations of truly independent international anti-fraud investigations carried out by EU staff were laid. Since then, legal acts have been providing gradually more detailed rules for OLAF investigations.

The twin Regulations 1073/1999[11] and 1074/1999[12] (hereinafter "the 1999 Regulations") established a general framework for OLAF's actions when the Office was created within the framework of the Amsterdam Treaty. Art. 1(1) of the 1999 Regulations confirmed the transition of the Commission's investigative powers to OLAF based on EU "rules and Regulations and *agreements* in force". Art. 3 of the 1999 Regulations merely incorporated the pre-existing Commission investigative powers under Regulation 2185/96, as well as those governed by Regulation (EC, Euratom) No 2988/95 and the sectoral rules referred to in its Art. 9(2).[13] However, for the first time and *in addition* to these pre-existing rules, the 1999 Regulations explicitly referred to the power to carry out on-the-spot checks and inspections under those rules in third countries "in accordance with the cooperation agreements in force". Back then, the 1999 Regulations remained silent on possible OLAF powers vis-à-vis international organisations. They also did not mention other investigative powers within the territory of third countries, such as witness interviews. The third Recital of the 1999 Regulations nonetheless mentioned that "all available means must be deployed fully to attain [the] objective [of the protection of the EU's financial interests]." Art. 2 of the 1999 Regulations then defined administrative investigations as "all inspections, checks and *other measures* undertaken by employees of the Office in the performance of their duties, in accordance with Arts. 3 and 4, with a view to achieving the objectives set out in [the Regulation] and to establishing, where necessary, the irregular nature of the activities under investigation."[14] The General Court later confirmed that the enumeration of OLAF powers in the 1999 Regulations was not taxative and the Office was, in principle, entitled to deploy other investigative measures corresponding to those used by national administrative authorities.[15]

It should also be noted that the territorial competence of OLAF also extended beyond EU borders in the area of internal investigations under Art. 4 of the OLAF Regulations. Namely, OLAF has the right of immediate and unannounced access to the premises of all EU institutions, bodies, offices, and agencies, including those of the EU Delegations in third countries. For this access, no particular international agreement is necessary, as the Office operates as part of an autonomous institutional internal control mechanism.

3. The further development under the current OLAF Regulation

Regulation 883/2013, which replaced the 1999 Regulations, codified the established practice of OLAF investigations and brought more detailed provisions concerning OLAF (and EU) powers in relation to international actors. The Regula-

tion recognised the necessity for OLAF to be able to engage with the competent authorities of third countries, in particular in the area of external aid (Recital 36). Furthermore, the wording of Art. 3 was supplemented with an explicit reference to international organisations and broadened the relatively narrow notion of "cooperation agreements" as the legal basis of investigative activities to "any other legal instruments in force".

However, for two reasons even an explicit reference to international agreements could not, in itself, overcome an inherent limitation to OLAF investigations outside the EU territory. First, the system of international agreements in place in 1999 mostly lacked any explicit reference to the Commission's or OLAF's investigative powers. In spite of a possible extensive interpretation of the notion of "cooperation agreements in force", as was done by the European Ombudsman in a case in which the Ombudsman recognised that even an *ad hoc* consent of the third country's competent authorities to a planned OLAF activity on its territory could uphold the legality of OLAF's actions,[16] a more permanent recognition of OLAF's competence had to be progressively negotiated – as will be shown in Section III.1 ("Anti-fraud provisions in international instruments") below.

Second, the OLAF Regulation and other EU legislation do not apply directly to economic operators on the territory of third countries, and even explicit provisions in international agreements are usually not sufficient to confer an obligation to cooperate with the Office on private persons and entities. It is also important to note that an explicit obligation of economic operators to cooperate with the Office was not introduced until Art. 3(3) of Regulation 883/2013 by Regulation 2020/2223.[17] Before this amendment, the obligation was merely based on private law.

Contractual clauses

The necessity to include relevant contractual clauses in financing and similar agreements under both private and international public law was fully reflected in the framework of the 2012 Financial Regulation: in particular, Arts. 58(3), 126(4), 140(5) of the 2012 version of the Financial Regulation[18] and Arts. 40(g), 180 and 212 of the Implementing Rules[19] obliged the Commission to include provisions regarding OLAF's competence to conduct investigations in any financing agreement concluded with a third party, including those located in third countries. The 2018 revision of the Financial Regulation further strengthened and clarified the legal framework. Rather than only containing references in various sections, Art. 129 stipulates unequivocally and in one place, i.e., in the Chapter that applies horizontally to all management modes of EU funding, that any recipient of EU funds is obliged to cooperate in the protection of the EU's financial interests and to grant the necessary rights and access to OLAF. In addition, for EU funds under direct and indirect management, the 2018 revision of the Financial Regulation introduced a clear reference to the requirement of "cascading down" the access right provisions, if there are one or more intermediaries up to the level of the final recipient of the funds. This requirement applies regardless of whether the recipient is inside or outside the EU.[20]

Even though a private law obligation may not have the same value as public law or an international agreement between the EU and states, these contractual provisions certainly have specific advantages:

- Global coverage, as they are signed each time the EU makes a financial contribution regardless of the fact whether a corresponding provision of an international agreement for a given third country is in place;
- Enforcement before domestic EU courts, as the governing law of these contracts is the law of one of the Member States, usually Belgium.

In some cases, the Commission also uses this type of contracts in relations with international organisations when they are direct recipients of funds from the EU.

It will therefore remain a priority of OLAF's international engagement to work with relevant services of the European Commission on the wording of these contractual clauses, as they complement the provisions in international agreements. While the international agreements ensure compatibility of OLAF's actions with regard to the principle of sovereignty of third countries and privileges and immunities of international organisations, legality of evidence collected, and a legal framework for support by local authorities and exchange of information, the private contracts safeguard the effectiveness of OLAF's investigative activities outside the EU.

As shown in this section, the evolution of the legal framework over the last 25 years demonstrates that the EU legislator not only recognised the importance of an independent role of OLAF in protecting the EU financial interests on the territory of third countries and vis-à-vis international organisations, but also further clarified OLAF's competence and powers in that area based on the evolving nature of the EU international engagements. This evolution went hand in hand with increased international OLAF activity and the building of international partnerships, which will be the subject of Section III.

III. OLAF's International Relations

Adopting a clear basis within the EU's legal framework for the conduct of OLAF investigations outside of the EU territory would not suffice for the Office to carry out its mandate effectively if there were no anti-fraud provisions in international instruments or if OLAF could not rely on its partners. The dichotomy of the legal basis for OLAF investigations under private contractual law and public international law needs to be complemented by OLAF efforts to formalise the relations with its most prominent partners in third countries and within international organisations and to create more or less formal international multilateral structures for the exchange of expertise and for enhancing mutual trust among like-minded and like-empowered entities.

Therefore, in this section we will take a closer look at the development of OLAF international relations from three angles. These have become the three basic pillars of OLAF's engagement in international relations and will be explained in more detail in the following subsections:

- Including anti-fraud provisions in international instruments;
- Negotiating administrative cooperation arrangements;
- Building global and regional partner networks.

1. Anti-fraud provisions in international instruments

As mentioned in the previous section, Art. 3 of Regulation 883/2013 enables OLAF to conduct on-the-spot checks outside the EU territory in accordance with relevant legal instruments of international law. In this context, one can broadly distinguish between two categories of instruments: international agreements on the one hand (below a)) and contractual clauses in financing agreements (or similar agreements) on the other (below b)).

The instruments in question do not simply allow for on-the-spot checks, but may also set up some specific procedural requirements. It is important to ensure that such requirements do not substantially derogate from the standard procedures pursuant to Regulation 883/2013. Furthermore, under Art. 129 in conjunction with Arts. 158(7) and 161(2) of the Financial Regulation,[21] the financing, contribution, and guarantee agreements with third countries and international organisations entrusted with indirect management of EU funds must contain provisions on the right of OLAF to carry out *investigations*, including on-the-spot checks and inspections, in accordance with Regulation 883/2013. In addition, they must grant the necessary rights and access required for OLAF.

a) International agreements

International agreements are negotiated and concluded by the EU, such as partnership and cooperation agreements or association agreements, and create obligations for the contracting parties under international law. Therefore, including specific provisions on anti-fraud cooperation and OLAF's competences in these agreements is of particular value for the Office, as this gives OLAF a sound legal basis for investigations concerning non-EU countries.

Hence, it is a logical priority for OLAF to ensure that these legal instruments contain appropriate provisions for OLAF to discharge its duties and conduct investigations outside the EU territory. In this respect, OLAF can fully take advantage of its dual nature as an independent investigative office and, at the same time, a service of the Commission. In particular, it is able – in its latter capacity – to be part of the Commission negotiation team and directly negotiate the terms under which OLAF, the investigative office, may carry out its independent mandate. As a service of the Commission, OLAF actively engages with the respective lead service responsible for the negotiation of an agreement, usually the European External Action Service, to ensure that provisions on the protection of EU funds, including cooperation with OLAF, are systematically part of bilateral agreements with non-EU countries, which may benefit from financial and technical assistance through the relevant EU funding mechanisms and instruments.[22]

Historically, OLAF's involvement in negotiations of international agreements can be traced back to the first few years after the establishment of OLAF, as a comparison between earlier and later agreements shows. For example, the EU–Azerbaijan Partnership and Cooperation Agreement (in force since 1999)[23] or the EU–Egypt Association Agreement (in force since 2004)[24] do not contain any specific provisions on the protection of the EU's financial interests.

By contrast, the EU–Ukraine Association Agreement for example, negotiations for which started in 2007 and which was signed in 2014, contains detailed provisions on the protection of the EU's financial interests, including on cooperation with OLAF, such as a requirement to report cases of suspected fraud or to assist OLAF when conducting on-the-spot checks. The agreement also includes wider policy commitments, such as a requirement to align the national legal framework with certain elements of EU legislation on the protection of EU financial interests.[25]

The association agreements with Georgia (signed in 2014)[26] and Moldova (signed in 2014)[27] and the EU–Armenia Com-

prehensive and Enhanced Partnership Agreement (signed in 2017)[28] contain similar provisions. Other international agreements vary in the scope of their anti-fraud provisions. For example, the agreements with Kazakhstan[29], Afghanistan[30], and Uzbekistan[31] generally include similar provisions regarding practical cooperation with OLAF, but do not comprise an alignment of legislation. At a minimum, the agreements negotiated after the establishment of OLAF contain a general reference to cooperation with OLAF (see for example the respective agreements with Mongolia[32], Iraq[33], or the Members of the Organisation of African, Caribbean and Pacific States[34]). The Withdrawal Agreement[35] and Trade and Cooperation Agreement[36] between the EU and the UK represent specific cases of a general international agreement with detailed provisions on the protection of the EU's financial interests.

Despite the clear value of having such provisions in international agreements, a practical limitation remains the geographic reach of those provisions: there is simply only a certain number of countries the EU has negotiated such international agreements with. Hence, anti-fraud provisions in financing or contribution agreements, which will be discussed in the next subsection, remain important.

b) Financing or contribution agreements

Financing or contribution agreements are concluded with third countries, third country authorities, and international organisations in accordance with the Financial Regulation. They are of a less general nature and usually use specific templates provided by the Commission for that purpose. Guarantee agreements with international organisations or national development banks may also fall within this category of international instruments. Financial framework partnership agreements with individual countries[37] or international organisations, which may be of a more permanent nature, again represent a specific group of agreements. Although instrumental to the Financial Regulation, these financing, contribution, and framework agreements also qualify as instruments under international law and fall under the term "other legal instruments in force" referred to in Art. 3 of Regulation 883/2013.

Unlike general international agreements, these agreements only focus on the relations between the Commission as the donor and the third country or the international organisation as the manager of the entrusted funds. For this reason, they are a perfect vehicle for provisions on OLAF. As demonstrated in the template agreement for contributions to international organisations, for example, these provisions in particular include an agreement by the organisation that OLAF may carry out investigations, including on-the-spot checks, and a requirement for the organisation to provide access to information and documents.[38] OLAF is usually consulted on the established templates or possible updates to them. The Office is also occasionally associated to the discussions and negotiations with external partners.

An interesting and specific recent example of OLAF's involvement in the negotiation of financing and contribution agreements was the Framework Agreement between the European Union and Ukraine laying down the principles of financial cooperation under the Ukraine Facility concluded in 2024, where OLAF contributed directly to the initial architecture of the agreement. This instrument therefore includes provisions reflecting new OLAF powers introduced by the most recent amendments to Regulation 883/2013 and the establishment of dedicated national data systems facilitating OLAF access to relevant data. Another recent example of international agreements with a limited scope but robust anti-fraud provisions are association agreements to specific EU programmes, such as Horizon Europe. These types of agreements are negotiated individually at a higher political level, and OLAF is not only part of the negotiation team but often contributes directly to the initial agreement architecture.

2. Administrative cooperation arrangements

The aim of OLAF's international relations work is to ensure that cooperation with international partners runs like a well-oiled machine. Using this metaphor, creating an international legal framework resembles the mechanical parts of the machine. Establishing and strengthening relations with individual partners or networks of partners is the oil that keeps the machine running. OLAF officials very quickly realised that they could not fulfil their mandate effectively without cooperating with partners around the globe.

Yet, their ambition to promote international partnerships faced an institutional problem inherent in the unique nature of the Office. As mentioned at the beginning of this article, while OLAF enjoys functional independence from the Commission, it does not have a distinct legal personality and remains an autonomous service of the Commission. The possibilities of formal engagement with external partners have therefore been rather limited. In that respect, memoranda of understanding and administrative arrangements with their simple and legally non-binding character appeared an elegant solution.

Looking back at the history of OLAF, this certainly seems to have been the view of Office officials from the outset.

For example, the very first report by OLAF on its operational activities from its establishment in June 1999 to May 2000 mentions that the "Office endeavours to remedy the difficulties inherent in international cooperation by improving relations with non-member countries […] through a range of administrative agreements and arrangements".[39]

Subsequent reports describe the implementation of this policy. For example, the report covering activities until June 2004 mentions that, in addition to an agreement with the United Nations, a new cooperative arrangement was signed with the World Bank "to conduct joint investigations based on mutual interest and on identified common needs".[40] This trend not only continued but also clearly accelerated. In 2007 for example, the Office signed six arrangements in one year – mainly with African partner authorities, but also with one in Latin America. [41]

Yet, for a long time, the legislation governing OLAF remained silent on the nature and effects of administrative arrangements that the young Office was so eager to exploit to boost its international standing, not to mention the very procedure under which such an instrument could be concluded. At that time, the Office could only rely on sporadic interpretation provided by the EU judiciary. In general, the conclusion of international agreements is governed by a specific procedure outlined in Art. 218 TFEU. The European Court of Justice has stated that this provision does not only cover documents formally designated as "agreements" but "any undertaking entered into by entities subject to international law which has binding force, whatever its formal designation."[42] Nonetheless, Advocate General *Giuseppe Tesauro* clarified in his opinion in Case C-327/91 that there are, on one hand, binding international agreements and "non-binding" gentlemen agreements concluded by bodies empowered to do so, and on the other hand "administrative arrangements" "brought into being by specific administrative entities with a view to establishing forms of cooperation with the authorities of other States having similar powers." [43] Such arrangements may then also be concluded by *bodies lacking power to bind* the State effectively at international level; "they amount to concerted practices between authorities which act in the exercise of their discretion and which are therefore acts that are clearly not governed by international law".[44]

Regulation 883/2013 eventually introduced a specific legal basis in Art. 14 enabling the Office to conclude administrative arrangements with authorities in third countries and with international organisations, in particular concerning the "exchange of operational, strategic or technical information". It also defined the term "administrative arrangements" in Point 6 of Art. 2 as "arrangements of a technical and/or operational nature concluded by the Office, which may in particular aim at facilitating the cooperation and the exchange of information between the parties thereto, and which do not create *additional* legal obligations."

To ensure sufficient inter-service coordination in this context, Art. 14 of the Regulation also stipulates that OLAF "shall coordinate its action, as appropriate, with the competent Commission services and with the European External Action Service, in particular before agreeing on such arrangements". This shows that the legislators clearly recognise the need for OLAF to engage with international actors to support its mandate of conducting investigations independent of the Commission, while at the same time requiring these actions to be well coordinated and in line with wider EU policies on external relations.

As mentioned above, these arrangements do not constitute international agreements as such. But even if administrative cooperation arrangements do not create a "hard" legal basis, they are nevertheless useful tools for strengthening the cooperation with international partners in several ways, both as stand-alone instruments and as a document that further clarifies – at a practical level – the rules stemming from other binding agreements concluded at the EU level. There are mainly three advantages: First, they serve as an expression of a willingness to work together, i.e. they reflect the intentions of the partners to cooperate. In that sense, they have become a useful vehicle of OLAF's "diplomacy", even in cases where no cooperation has occurred yet. Second, and more importantly, they set a practical framework for operational exchanges by summarising the mandate and legal framework of the partners, establishing contact points, setting deadlines and practicalities for the exchange of information as well as covering other aspects of cooperation. As such, they serve as an everyday practical tool for investigators, helping them to identify potential partners for their investigations and opening the necessary channels. Third, the very process of negotiating these arrangements is educational on its own and helps to manage expectations for cooperation on both sides and to clarify – or sometimes even resolve – possible different legal interpretation at the outset. The main objective of all administrative arrangements is not to create an additional administrative burden but to clear the way for mutual cooperation.

Fast-forwarding to the present, it becomes evident how the policy of concluding administrative arrangements established in the early days has paid off and created a global network of partner authorities. As of February 2025, OLAF

has arrangements in place with 39 authorities around the globe and 17 offices of international organisations, including the United Nations and the World Bank. [45]

3. Global and regional initiatives

As useful as administrative arrangements are, they essentially remain bilateral in nature. Therefore, another focus of OLAF's international relations work is the creation and strengthening of multilateral or regional networks. Again, the roots of this practice can be traced to the early days of OLAF.

For example, the first Director-General of OLAF, *Franz-Hermann Brüner* was an ardent advocate of increased cooperation among international organisations. In this context, it is interesting to note that around the time of OLAF's establishment in 1999 similar developments could be witnessed in several international organisations, i.e., the introduction of independent investigative services to fight fraud or other misconduct. The inception of the United Nations Office of Internal Oversight Services in 1994[46] and the Department of Institutional Integrity (now the Integrity Vice Presidency) at the World Bank in 2001[47] are cases in point.

Conference of International Investigators (CII)

1999 also saw the creation of the Conference of International Investigators (CII). Faced with similar challenges and opportunities for cooperation, the investigative offices of international organisations came together to exchange good practices and discuss recent developments with view to integrity, fraud, and corruption.[48] OLAF started to actively engage with the CII community, especially the United Nations and the World Bank. The aim was to create a set of investigative standards that can be used by the respective offices to enhance their effectiveness and facilitate the cooperation.[49] OLAF even went on to host the 4th edition of the conference in April 2003, in which participants endorsed these common investigative standards in the form of "Uniform Guidelines for Investigations".[50]

During his mandate as Director-General of OLAF, *Mr Brüner* was considered crucial in promoting the CII community of international investigators in those early years and in expanding the number of organisations participating in the conference. To honour his achievement and commitment to the community, the conference introduced the Franz-Hermann Brüner Memorial Lecture following his death in 2010. Since then, this lecture has been given by distinguished industry professionals, scholars, and dignitaries on the opening day of the conference.[51]

As is the case with the policy of concluding administrative cooperation arrangements mentioned above, the measures initiated in the early years are still the foundation for much of the cooperation today. For example, the guidelines mentioned above still exist in an updated form and continue to serve the investigators of international organisations as a benchmark and leading practice.[52] Similarly, not only does the CII still take place today, its membership has nearly doubled compared to 2004 and now constitutes a thriving community of 57 participating organisations.[53]

Pilot Group

The same evolution can be observed with regard to initiatives to create regional networks. The foundations for two such networks were laid in the early years of OLAF, which still continue to be a priority of OLAF's international relations today, namely the Pilot Group with African partner countries and the network of relevant authorities in EU candidate countries and potential candidates.

The Pilot Group was first created in 2007 and has been meeting regularly since. It was established to enhance the cooperation between OLAF and African authorities, as well as to increase trans-African cooperation, especially concerning the sharing of experiences and leading practices to prevent, detect, and investigate fraud. The most recent meeting in this format took place in July 2022.[54]

Similarly, engagement with candidate countries and potential candidates as part of the EU enlargement process has been a strategic priority from the very beginning. As with the Pilot Group, the focus not only lies on establishing contacts to facilitate investigative cooperation regarding potential cases of fraud affecting EU funds, but also on the exchange of knowledge and capacity building.

Anti-fraud coordination services

Recognising the crucial importance of helping countries that are in the process of joining the EU, OLAF encouraged candidate countries as early as 2002 to designate an anti-fraud coordination service (AFCOS) with the task of "co-ordinating all legislative, administrative and operational aspects" regarding the protection of EU financial interests, and the Office started to provide specific support measures in this regard.[55] For example, the Office organised an AFCOS roundtable in October 2002 with participants from all acceding and candidate countries at the time. These efforts soon produced tangible results: By early 2003, 12 countries had nominated an AFCOS.[56]

As the then candidate countries became EU Member States, an interesting situation arose: "new" EU Member States had an AFCOS in place, while "old" EU Member States did not. However, the system of dedicated contacts points for OLAF proved so useful that Regulation 883/2013 introduced a requirement for *all* EU Member States do designate an AFCOS. This makes it an interesting case of a concept being developed originally and specifically in the enlargement context only to be turned into a standard for all EU Member States.

As with other policy areas examined in this section, the story goes on as OLAF continues to work closely with the current candidate countries and potential candidates to support them in their efforts to fulfil the requirements of EU membership in the area of protecting the EU's financial interests. Case in point, the latest edition of a conference bringing together the AFCOS offices (and other relevant authorities) of Member States, candidate countries, and potential candidates took place as recently as October 2024.[57]

Cooperation among the EU anti-fraud actors in the context of Ukraine

Recently, relations with a specific candidate country – Ukraine – served as a possible stepping stone for developing another project of vital EU interest on the list of top priorities of the current Commission: an effective cooperation among the EU anti-fraud actors, namely OLAF, the EPPO, Europol, and Eurojust. This work helped to identify possible areas of synergies in cooperation between the partners and practical ways forward. The experience currently serves as a basis for further discussions on the EU anti-fraud architecture steered by the Commission.

IV. Conclusion

The development of OLAF's international relations has been profoundly marked by the *effet utile* of the protection of the EU's financial interests embedded in Art. 325 TFEU (and its predecessor provisions), and, even more broadly, by the interests of the EU and its citizens in general. The powers, know-how, and reputation of OLAF have evolved hand in hand based on practical imperatives to protect EU taxpayer money (and increasingly the interests of European consumers).

Over the last quarter of a century, the efforts of OLAF in the area of international relations have been focussing on three main objectives: improving the legal framework governing the protection of EU financial interests beyond EU borders, establishing meaningful and trustworthy relations with international partners, and initiating and building up multilateral forums for the exchange of information, best practices, and expertise.

Since the establishment of OLAF, the EU has been steadily expanding its international engagement. Recent international EU initiatives launched in response to new challenges are unprecedented both in nature and scope. For example, in response to Russia's unprovoked war of aggression against Ukraine, the EU mobilised over €134 billion in support to Ukraine and Ukrainians.[58] In the framework of its Global Gateway initiative, the EU is prepared to deploy around €300 billion for investments in Africa, Asia, and Latin America.[59]

Such an amount of money intended for the public good necessarily attracts the attention of fraudsters. And fraud does not know any boundaries. The European Parliament has therefore repeatedly called for strengthening fraud prevention and ensuring sufficient capacities for fighting fraud. In line with its global engagements, the EU needs to keep pace with new fraud trends to protect the EU reputation and the money of its taxpayers. Without a strong international anti-fraud system in place, without a robust but flexible legal framework, and without reliable and committed international partners, such a task would become nearly impossible.

As this article has demonstrated, many of OLAF's international activities have their roots in the early years of the Office. They have grown, expanded, and matured – but still essentially embody the spirit of the beginning. In that context, OLAF's proactive attitude to international relations, which started taking shape a quarter of a century ago and has become well-established since, is proving more necessary than ever in the current world. The Office's "soft" power of administrative investigations helps overcome territorial boundaries. In addition, OLAF's openness to international alliances with likeminded partners builds trust within the anti-fraud community. OLAF's determination at the international scene to pursue its mandate wherever EU money goes sends a strong signal to fraudsters that there is no place to hide wherever they go.

---

* The views expressed in this article are exclusively those of the authors and cannot be attributed to the institution that employs them.

1 C. Scharf-Kröner and J. Seyderhelm, "OLAF Investigations Outside the European Union – Practical and Legal Aspects", (2019) *eucrim*, 209.

2 In view of the limited space, this article will have to leave aside an equally dynamic chapter of OLAF's international relations: OLAF's engagement in the area of international customs cooperation, which have included negotiations of protocols on mutual administrative

assistance of customs authorities, organisation of joint customs operations and establishment of links with customs authorities around the globe.

3 See in detail section III below.

4 Commission Decision 1999/352/EC, ECSC, Euratom of 28 April 1999 establishing the European Anti-fraud Office (OLAF), OJ L 136, 31.5.1999, 20.

5 See the fifth recital of Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ L 136, 31.5.1999, 1, and the sixth recital of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, 1.

6 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, 1.

7 See in more detail Scharf-Kröner and Seyderhelm, *op. cit.* (n. 1), 210.

8 Council Regulation (EEC) No 945/87 of 30 March 1987 amending Regulation (EEC) No 1468/81 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters, OJ L 090 , 2.4.1987, 3).

9 Council Regulation (EEC) No 1468/81 of 19 May 1981 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters, OJ L 144, 2.6.1981, 1.

10 Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, 2.

11 Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ L 136, 31.5.1999, 1.

12 Council Regulation (Euratom) No 1074/1999 of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OCAF), OJ L 136, 31.5.1999, 8.

13 Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests, OJ L 312, 23.12.1995, 1.

14 Emphasis added by authors.

15 Judgment of the General Court of 20 July 2016, Case T-483/13, *Oikonomopoulos v Commission*, ECLI:EU:T:2016:421, paras 188 ff.

16 The European Ombudsman in her decision of 13 March 2014, closing inquiry OF/8/2010(VIK)CK, explicitly recognised that "nothing prevents OLAF from conducting an inspection on the basis of a de facto agreement, in this case, the consent given by the competent authorities of Country X." (para. 64), <https://www.ombudsman.europa.eu/en/decision/en/53814>. All hyperlinks in this article were last accessed on 18 February 2025.

17 Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, OJ L 437, 28.12.2020, 49.

18 Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002, OJ L 298, 26.10.2012, 1.

19 Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 on the rules of application of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council on the financial rules applicable to the general budget of the Union, OJ L 362, 31.12.2012, 1.

20 Art. 129(2) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012, OJ L 193, 30.07.2018, p. 1, stipulated: "Any person or entity receiving Union funds under direct and indirect management shall agree in writing to grant the necessary rights as referred to in paragraph 1 and shall ensure that any third parties involved in the implementation of Union funds grant equivalent rights."

21 Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast), OJ L, 2024/2509, 26.9.2024.

22 Apart from anti-fraud provisions concerning the protection of EU expenditure, many international agreements contain provisions on customs cooperation. However, those are distinct from the provisions discussed here and further analysis of them would go beyond the scope of the article.

23 Partnership and Cooperation Agreement between the European Communities and their Member States, of the one part, and the Republic of Azerbaijan, of the other part, OJ L 246, 17.9.1999, 3–51.

24 Euro-Mediterranean Agreement establishing an Association between the European Communities and their Member States, of the one part, and the Arab Republic of Egypt, of the other part, OJ L 304, 30.9.2004, 39–208.

25 Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part, OJ L 161, 29.5.2014, 3-2137; for the anti-fraud provisions see in particular Title VI as well as Annex XLIII and Annex XLIV. For the dates of the negotiations see: European Commission – Press release "EU-Ukraine Association Agreement fully enters into force",1 September 2017, available at: <https://ec.europa.eu/commission/presscorner/api/files/document/print/hu/ip_17_3045/IP_17_3045_EN.pdf>.

26 Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part, OJ L 261, 30.8.2014, 4–743.

27 Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Moldova, of the other part, OJ L 260, 30.8.2014, 4–738.

28 Comprehensive and enhanced Partnership Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Armenia, of the other part, OJ L 23, 26.1.2018, 4–466.

29 Enhanced Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Kazakhstan, of the other part, OJ L 29, 4.2.2016, 3–150.

30 Cooperation Agreement on Partnership and Development between the European Union and its Member States, of the one part, and the Islamic Republic of Afghanistan, of the other part, OJ L 67, 14.3.2017, 3–30.

Lukáš Jelínek
European Commission / European Anti-Fraud Office (OLAF), Deputy Head of Unit "Inter-Institutional & International Relations and Communication"

Clemens Kreith
European Commission / European Anti-Fraud Office (OLAF), "Inter-Institutional & International Relations and Communication", Team Leader International Relations

31 Proposal for a Council Decision on the signing, on behalf of the European Union, of the Enhanced Partnership and Cooperation Agreement between the European Union, of the one part, and the Republic of Uzbekistan, of the other part COM/2024/471 final; the agreement was initialled but not yet signed.
32 Framework Agreement on Partnership and Cooperation between the European Union and its Member States, of the one part, and Mongolia, of the other part, OJ L 326, 9.12.2017, 7–35.
33 Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Iraq, of the other part, OJ L 204, 31.7.2012, 20–130.
34 Partnership Agreement between the European Union and its Member States, of the one part, and the Members of the Organisation of African, Caribbean and Pacific States, of the other part, OJ L, 2023/2862, 28.12.2023.
35 Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, OJ L 29, 31.1.2020, 7–187.
36 Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L 149, 30.04.2021, 10–2539.
37 For example, candidate countries or potential candidates that are beneficiaries of the Instrument for Pre-Accession Assistance.
38 See: Contribution Agreement Manual, available at: <https://international-partnerships.ec.europa.eu/system/files/2023-07/contribution-agreement_manual_en.pdf>.
39 Report by the European Anti-Fraud Office, First Report on the operational activities 1 June 1999 – 31 May 2000, pp. 39–40, available at: <https://anti-fraud.ec.europa.eu/document/download/3554f343-9db6-4dfc-8cc8-d90a0e42d93d_en?filename=rep_olaf_2000_en.pdf>.
40 Report by the European Anti-Fraud Office, Fifth Activity Report for the year ending June 2004, p. 51, available at: <https://anti-fraud.ec.europa.eu/document/download/ae3d879c-5430-4056-8d06-a73d-c7ce7368_en?filename=rep_olaf_2003_2004_en.pdf>.
41 List of administrative cooperation arrangements signed by OLAF, available at: <https://anti-fraud.ec.europa.eu/document/download/4220e17e-a51e-4bff-8d2b-8e467f59c2bf_en?filename=list_signed_acas_en.pdf>.
42 ECJ, 11 November 1975, Opinion 1/75, *OECD*, ECLI:EU:C:1975:145.
43 Opinion of AG Tesauro, delivered on 16 December 1993 in Case C-327/91, *France v Commission*, ECLI:EU:C:1993:941, para. 22.
44 Ibid.
45 List of administrative cooperation arrangements signed by OLAF, *op. cit.* (n. 41).
46 See: <https://oios.un.org/content/who-we-are>.
47 The World Bank Group, Annual Report on investigations and sanctions of staff misconduct and fraud and corruption in bank-financed projects, Fiscal Year 2004, p. 1 available at: <https://thedocs.worldbank.org/en/doc/b7739244fe434dedb953b51abecb85e1-0090012021/original/INT-FY04-Annual-Report.pdf>.
48 See: <https://www.ciinvestigators.org>.
49 Report of the European Anti-Fraud Office, Third Activity report for the year ending June 2002, p.15; available at: <https://anti-fraud.ec.europa.eu/document/download/9fbcab19-4f48-44b0-bfa1-27588fd07247_en?filename=rep_olaf_2002_en.pdf>.
50 Report of the European Anti-Fraud Office, Fourth Activity Report for the year ending June 2003, p. 51–52; available at: <https://anti-fraud.ec.europa.eu/document/download/34f4bed5-a012-4df5-b30c-9bc2d2d0800d_en?filename=rep_olaf_2002_2003_en.pdf>.
51 See: <https://www.ciinvestigators.org/the-memorial-lecture>.
52 See: <https://www.ciinvestigators.org/cii-guidelines>.
53 See: <https://www.ciinvestigators.org/participating-organisations>.
54 OLAF Press release No 9/2022, "OLAF meets with African partners to strengthen EU–Africa cooperation in fighting fraud of EU budget", available at: <https://anti-fraud.ec.europa.eu/media-corner/news/olaf-meets-african-partners-strengthen-eu-africa-cooperation-fighting-fraud-eu-budget-2022-06-28_en>.
55 OLAF report for the year ending June 2002, *op. cit.* (n. 49), pp. 30–31.
56 OLAF report for the year ending June 2003, *op. cit.* (n. 50), p. 48.
57 OLAF Press release No 18/2024, "Fighting fraud together", available at: <https://anti-fraud.ec.europa.eu/media-corner/news/fighting-fraud-together-2024-10-18_en>.
58 See European Commission, Factsheet – EU Solidarity with Ukraine, February 2025, available at: <https://ec.europa.eu/commission/presscorner/api/files/attachment/880467/Factsheet%20-%20EU%20Solidarity%20with%20Ukraine.pdf>.
59 See European Commission website "Global Gateway", <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en>.

Hercule – a History of Success

20 Years of Financing Support and Equipping the Fight against Fraud

Alicia-Luna Scala-Amez*

In 2004, the European Community set up the Hercule programme to promote activities related to the protection of its financial interests. Since then, this unique initiative aimed at financing the fight against fraud has thrived and is now celebrating 20 years of success. It mainly funds the purchase of technical equipment and tools, training, staff exchanges, risk analysis workshops, conferences and comparative studies. These measures seek to support and equip EU Member States in legal, operational and technical/IT terms, enabling them to deliver on their shared obligations to protect the EU's financial interests. In 2021, the Hercule programme became a component of the current Union Anti-Fraud Programme (UAFP).
This article retraces the history of the Hercule programme, outlines the main features of the Hercule component in the UAFP and gives examples of the success of the programme. The article concludes that, when reviewing the ever-increasing number and quality of applications for funding under the UAFP Hercule component, it becomes evident that a financial injection would be very much necessary to allow the programme to continue to achieve its objectives.

I. Retracing the History of Hercule

2024 was a year of celebration for the European Anti-Fraud Office (OLAF) – an occasion to look back on the Office's origins as well as to contemplate its future. In addition to celebrating 25 years as a crucial actor protecting the financial interests of the EU, OLAF also marked the 20th anniversary of the only spending programme specifically dedicated to fighting fraud affecting the EU's financial interests: the Hercule programme.

In light of the constant evolution of the criminal landscape, the fight against fraud has been strongly bolstered since the establishment of the Anti-Fraud Coordination Unit (UCLAF) as a task force within the Secretariat-General of the European Commission in 1988. UCLAF had been working alongside national anti-fraud departments in Member States and coordinating and assisting efforts to tackle transnational organised fraud detrimental to the EU's financial interests. With a reinforced and independent investigative mandate, OLAF was established in 1999[1] to perform administrative investigations into fraud and irregularities affecting the EU revenue and expenditure, including cases of serious misconduct involving staff and members of the EU institutions, bodies, offices and agencies.

On 21 April 2004, following a proposal of the Commission, the European Parliament and the Council established a Community programme for the promotion of actions in the field of the protection of the financial interests of the Community: the Hercule programme,[2] in honour of the very well-known fictional Belgian detective Hercule Poirot.[3] This programme was later extended under the Financial Perspectives for 2007–2013[4], establishing the Hercule II programme[5], followed by Hercule III (covering the financial period of 2014–2020)[6]. Given the intention to facilitate a more integrated and strategic use of financial resources, including the simplification of their management, the Hercule component was integrated into the Union Anti-Fraud Programme (UAFP) in 2021.[7]

The UAFP will run for the duration of the new Multiannual Financial Framework (MFF), for the period of 2021 to 2027, and covers three components: the Protection of the Union's Financial Interests (i.e., the Hercule component), the Anti-Fraud Information System (AFIS) and the Irregularities Management System (IMS).[8]

II. Main Features of the Hercule Component

The EU is required to protect its financial interests by virtue of Art. 325(1) of the Treaty on the Functioning of the European Union (TFEU) and this obligation is shared by its Member States. The UAFP in turn helps the EU provide financial support Member States in legal, operational and material terms, so that they can deliver on their respective obligations.

The Hercule component provides financial support, mainly in the form of grants awarded to competent authorities in EU countries. Around one third of its annual budget is spent on procured services provided to Member States authorities, such as access to commercial databases and advanced IT analytical tools, strengthening their operational and technical capacity to investigate activities detrimental to the EU budget.

Financial support is, to a large extent, delivered by means of two calls for proposals:

- Technical assistance call: aimed at strengthening national authorities' investigative capability and capacity (including their digitalisation) to step up the fight against fraud, corruption and any other illegal activity affecting the EU's financial interests, on both the revenue and expenditure sides. It mostly finances the purchase of **technical equipment and tools**, such as investigation and surveillance equipment, digital forensic and crime detection tools and tools for data analysis.
- Training, conferences, staff exchanges and studies call: this arm includes, for instance, risk analysis workshops, comparative studies and the dissemination of relevant information through periodical publications. It helps national authorities, research bodies, educational institutes and NGOs to: (i) share best practices; and (ii) improve cooperation and coordination between the different actors involved in protecting the EU's financial interests. This line of financial support also promotes specialised **training** to improve and update the digital-forensic and analytical skills of law enforcement organisations and to underpin Member States' digital transition.

The calls for proposals are very popular among the Member States authorities, OLAF receiving each year many more requests for financing than the available budget.

III. The Success of Hercule

1. Success in numbers

The initial financial framework of the Hercule programme included a budget of €11.5 million for the 2004–2006 period. Thanks to the success of the first programme, the financial envelopes of the Hercule II and Hercule III programmes were considerably increased to €98.5 million for the 2007–2013 period and almost €105 million for the 2014–2020 period.

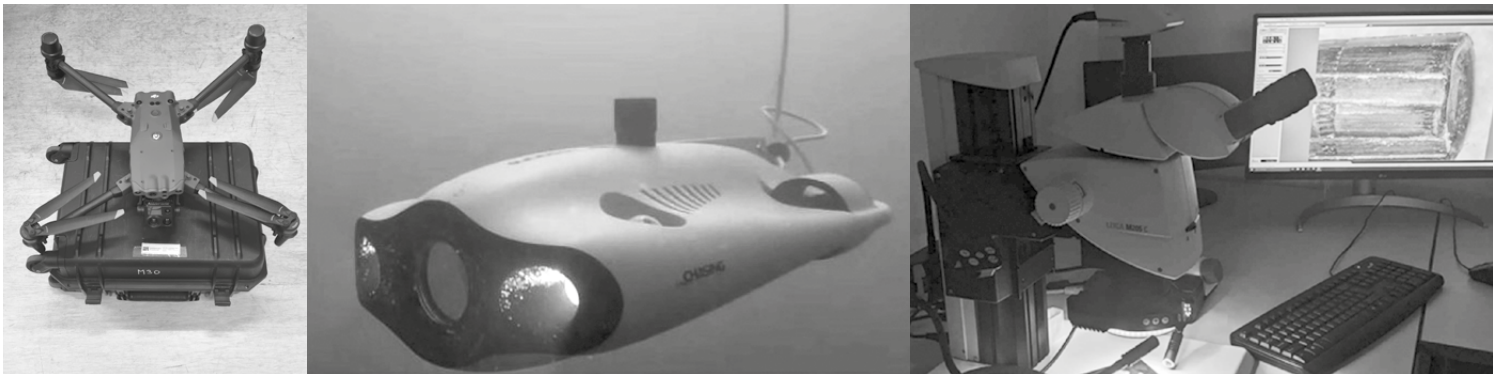
Under the current EU MFF, with a total budget volume of €1.8 trillion,[9] the UAFP will make available to beneficiaries €181 million in current prices for the period of 2021–2027, representing about 0.1% of the total MFF package. The UAFP Regulation allocates around €114 million to the Hercule component (see section II.), of which the successive Commission's Implementing Decisions have already distributed a budget of around €15 million for the years 2021, 2022 and 2023, of €16 million for 2024 and of €17.5 million for 2025.

This net increase of funding is in response to the increase in number and quality of the applications received. While OLAF received 27 grant applications and awarded 23 grants in 2006, there were 110 grant applications in 2024 (of which 88 were for technical assistance and 35 for training, conference, staff exchanges and studies), with 30 grants awarded (of which 22 were awarded for technical assistance and 8 for training, conferences, staff exchanges and studies). Given the huge uptake of the Hercule component, a budget increase for its two calls appears imperative in order to do justice to the growing number of excellent applications received by OLAF.

2. Successful projects

Over the past 20 years, OLAF has been witnessing how the Hercule funds have been put to good use. From the financing of international conferences to the purchasing of underwater drones to combat illicit traffic of counterfeit goods and smuggling, the contribution to the fight against fraud has been tangible and the funds clearly contribute to the protection of EU financial interests.

The technical assistance action has helped to finance the purchasing of specialised equipment and tools, such as forensic laboratories, unmanned aerial vehicles (drones), underwater drones, data collection and analysis tools,



photos: Audiovisual Service of the European Commission

specialised vehicles for digital forensics, spectral document analysis systems, mobile fingerprinting stations, scanner vans, Geographical Information Systems (GIS), semi-rigid boats, coast guard cutter boats and cargo containers x-ray scanners (see also photographs below).[10]

For the training, conferences, staff exchanges and studies action, the examples are more heterogeneous and include:

- Specialised training sessions, often involving different national authorities within a Member State and even those of different Member States, international partners and European organisations, on topics such as the forensic examination of mobile devices, prevention and detection of fraud in a specific context, or cooperation to combat organised fraud.
- Studies usually involve academic institutions and authorities from several Member States and often focus on the cooperation of OLAF, the European Public Prosecutor's Office (EPPO), Eurojust and Europol and their role in fighting fraud; studies have covered, for instance, an analysis of the most relevant questions of the external, internal and criminal investigation of irregularities and offences affecting the financial interests of the EU and the assessment of the effectiveness of a preventive administrative approach.
- Dissemination of relevant information through periodical specialised publications.
- Staff exchanges, e.g. from different national police forces.

IV. Concluding Remarks

20 years have passed since the Hercule programme was launched – 20 years that have seen an impressive uptake and compelling projects. However, a closer look at the numbers makes it evident that the successive budget increases lag behind the ever-growing interest and need for support and equipment of the applicants. And after all, the support and equipment of the applicants is the rationale and the essence of this programme. The uptake in number and quality of projects and the insufficient budget increases are being factored in when it comes to the European Commission planning the future of the UAFP. As it is preparing the next UAFP proposal for the upcoming MFF (2028–2034), the Commission needs to reflect on the present and, above all, the future needs of both current and future Member States.

Alicia-Luna Scala-Amez
European Commission / European Anti-Fraud Office (OLAF), Unit D1 "Legislation and Policy", Operational, administrative and legal support

* The views expressed in this article are exclusively those of the author and cannot be attributed to the institution that employs her.

1 Commission Decision 1999/352/EC, ECSC, Euratom, of 28 April 1999, establishing the European Anti-fraud Office (OLAF), OJ L 136, 31.5.1999, 20–22.

2 Decision No 804/2004/EC of the European Parliament and of the Council, of 21 April 2004, establishing a Community action programme to promote activities in the field of the protection of the Community's financial interests (Hercule programme), OJ L 143, 30.4.2004, 9–14.

3 Hercule Poirot is the most famous and long-running fictional character created by the renowned British author Agatha Christie, featured in 33 of her novels, two plays and 51 short stories published between 1920 and 1975.

4 Communication from the Commission to the Council and the European Parliament – Financial Perspectives 2007–2013, COM(2004) 487 final.

5 Decision No 878/2007/EC of the European Parliament and of the Council, of 23 July 2007, amending and extending Decision No 804/2004/EC establishing a Community action programme to promote activities in the field of the protection of the Community's financial interests (Hercule II programme), OJ L 193, 25.7.2007, 18–22.

6 Regulation (EU) No 250/2014 of the European Parliament and of the Council, of 26 February 2014, establishing a programme to promote activities in the field of the protection of the financial interests of the European Union (Hercule III programme) and repealing Decision No 804/2004/EC, OJ L 84, 20.3.2014, 6–13.

7 Regulation (EU) 2021/785 of the European Parliament and of the Council, of 29 April 2021, establishing the Union Anti-Fraud Programme and repealing Regulation (EU) No 250/2014, OJ L 172 17.5.2021, 110.

8 The support for AFIS and IMS was previously established under Council Regulation (EC) No 515/97, of 13 March 1997, on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, as amended, OJ L 82, 22.3.1997, 1–16. For details on the UAFP, see S. E. Buksa and G. Roebling, "The New Union Anti-Fraud Programme", (2021) *eucrim,* 175–177.

9 Including the Recovery and Resilience Facility, created in response to the coronavirus pandemic and established on the basis of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, OJ L 57, 18.2.2021, 17–75.

10 More information on examples for both calls can be found in the annual overview with information on the results of the UAFP for each year, available at <https://anti-fraud.ec.europa.eu/about-us/reports/annual-reports-protection-eus-financial-interests-pif-report_en> accessed 27 January 2025.

Imprint

Impressum

Published by:
Max Planck Society for the Advancement of Science
c/o Max Planck Institute for the Study of Crime, Security and Law
(formerly Max Planck Institute for Foreign and International Criminal Law), represented by Director Prof. Dr. Ralf Poscher
Guenterstalstrasse 73
79100 Freiburg i.Br., Germany

Tel: +49 (0)761 7081-0
E-mail: public-law@csl.mpg.de

Internet: https://csl.mpg.de

Official Registration Number: VR 13378 Nz
(Amtsgericht Berlin Charlottenburg)
VAT Number: DE 129517720

Editor in Chief: Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Managing Editor: Thomas Wahl, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Editors: Dr. Anna Pingen, Max Planck Institute for the Study of Crime, Security and Law, Freiburg; Cornelia Riehle, ERA, Trier
Editorial Board: Prof. Dr. Lorena Bachmaier, Complutense University Madrid, Spain; Peter Csonka, Head of Unit, DG Justice and Consumers, European Commission Belgium; Prof. Dr. Esther Herlin-Karnell, University of Gothenburg, Sweden; Mirjana Juric, Head of Service for combating irregularities and fraud, Ministry of Finance, Croatia; Philippe de Koster, Director FIU Belgium; Prof. Dr. Katalin Ligeti, University of Luxembourg; Dr. Lothar Kuhl, Former Head of Unit, European Commission (Anti-Fraud Office (OLAF) and Directorate for Audit in Cohesion (DAC)); Prof. Dr. Ralf Poscher, Director at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg, Germany; Lorenzo Salazar, Deputy Prosecutor General to the Court of Appeal of Naples (ret.), Italy; Prof. Rosaria Sicurella, University of Catania, Italy
Language Consultants: Indira Tie and Sarah Norman, Certified Translators, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Typeset and Layout: Ines Hofmann and Katharina John, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Produced in Cooperation with: Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)
Printed by: Stückle Druck und Verlag, Ettenheim, Germany

The publication is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF)

Co-funded by the European Union

ISSN: 1862-6947

Practical Information

Articles in eucrim are subject to an editorial review. The journal is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@csl.mpg.de
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@csl.mpg.de
More information at our website: https://eucrim.eu

Contact

Thomas Wahl
Max Planck Institute for the Study of Crime, Security and Law
Guenterstalstrasse 73
79100 Freiburg i.Br., Germany
Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)
E-mail: info@eucrim.eu

MAX PLANCK INSTITUTE
FOR THE STUDY OF
CRIME, SECURITY AND LAW