PRIORITIES OF COOPERATION WITH THE EU IN THE AREAS OF LAW ENFORCEMENT, FIGHT WITH ORGANISED CRIME, CYBERSECURITY AND PERSONAL DATA PROTECTION.

Expert Support to New Ukraine-EU Agenda on Justice, Freedom and Security

Civic Synergy
INTERNATIONAL RENAISSANCE FOUNDATION
UKRAINIAN NATIONAL PLATFORM OF THE EASTERN PARTNERSHIP Civil Society Forum
EUROPE WITHOUT BARRIERS civic organisation

This document is prepared by Europe Without Barriers think tank under the aegis of Ukrainian National Platform of the Eastern Partnership Civil Society Forum with the support of European Union and International Renaissance Foundation within the framework of Civic Synergy project.

The content of this publication is the sole responsibility of the Europe Without Barriers think tank.

Author:
Ruslan Minich

Project team:
Iryna Sushko, Ruslan Minich, Pavlo Kravchuk

Design:
Viktoriia Fedyna

/

1. INTRO-DUCTION

Ukraine has drafted a New Agenda on Justice, Freedom and Security within the framework of the EU-Ukraine Association Council. It has established new tasks within the realms of the implemented Visa Liberalisation Action Plan and the Association Agreement that is in the process of implementation.

The agenda was presented at the EU-Ukraine summit in summer 2018. The EU-Ukraine Association Council further discussed it and agreed to continue cooperation in justice and home affairs in December.

Anti-money laundering and countering terrorist financing, fight against serious international and organised crime are the areas of interest. Both sides emphasized a necessary cooperation to combat cyber and hybrid threats for the citizens' security.

The ministries and the Government Office for Coordination of European and Euro-Atlantic Integration, developing and implementing arrangements between Ukraine and European Union, work on these issues together with European colleagues including the EU Advisory Mission to Ukraine (EUAM).

At the same time, the New Agenda is not yet approved. Therefore, the new authorities and state institutions for European integration canl revise this document and agree new possible tasks.

/

2. CYBER-SECURITY

The International Telecommunication Union published its third Global Cybersecurity Index in 2018. Ukraine constantly improves its score: 0.353 in 2014, 0.501 in 2017, and 0.661 in 2018.

Yet Russia can show off better results, 0.836 in 2018, while the top-10 secured countries are the UK, the U.S., France, Lithuania, Estonia, Singapore, Malaysia, Canada and Norway.

Ukraine adopted the Cybersecurity Strategy on March 15, 2016, to enhance its cybersecurity. **But the latest action plan covers 2018.** Meanwhile, the Law on Cybersecurity Foundations of Ukraine was passed in July 2018. The law introduces new important definitions, the notion of critical infrastructure and public-private partnership. Moreover, it outlines major players of national cybersecurity system and their powers. They are the State Service for Special Communication and Information Protection of Ukraine, National Police of Ukraine, Security Service of Ukraine, Ministry of Defence of Ukraine and General Staff of the Armed Forces of Ukraine, intelligence, National Bank of Ukraine. **The law is not sufficient and shall be accompanied by other laws and bylaws.** Moreover, the state institutions shall have a clear guidance on their powers execution to avoid possible overlapping.

Meanwhile, the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union - NIS Directive - came into effect in the European Union in November 2018. Although Ukraine is not obliged to **transpose it into its legislation,** such a move could significantly contribute to its cybersecurity and become a further step on its European integration path.

The NIS Directive lays down obligations to adopt a national strategy on the security of network and information systems, designate national competent authorities, single points of contact, and computer security incident response team (CSIRTs or CERTs). Ukraine already comply with them. Its response team is called Computer Emergency Response Team of Ukraine, CERT-UA, which is a competent division of the Cybersecurity State Center of the State Service for Special Communication and Information Protection of Ukraine.

Moreover, Ukraine should outline requirements to be applied to the operators of essential services (critical infrastructure) and digital services suppliers. The government decree approving General requirements on critical infrastructure objects' cybersecurity no. 518 of June 19, 2019, obliges

«the owner and/or manager of the critical infrastructure object to immediately report cyberincidents and cyberattacks on its critical infrastructure object to the government computer emergency response team (sectoral computer emergency response team when applicable) as well as a functional division of national interests counterintelligence defence in the area of information security of Security Service of Ukraine (Cyber Security Situation Centre) or a specialised division of the SSU regional authority».

The critical infrastructure object can be both private and public. But **it is not yet clear which objects belong to the critical infrastructure and the procedure of their audit. Thus, this provision is not applicable. A relevant law or bylaw could fix this gap.**

Besides, it is not clear **what obligations digital services suppliers (online marketplaces, online search engines, cloud services) have.** The NIS Directive obliges them to implement appropriate and proportionate technical and organisational security measures. But in contrast to the operators of essential services, the digital services suppliers are not under a regular supervisory control by the regulator. The competent authorities will act only if there is evidence that a digital services supplier

does not meet the requirements of the NIS Directive — especially after an incident.

The **public-private cooperation** is yet another novelty. The cybersecurity law outlines the ways of such a cooperation but without a clear mechanism. Moreover, the state authorities should explain business people their benefits.

At the same time, Ukraine promised to conclude memorandum of **cooperation with the European Union Agency for Cybersecurity (ENISA) , NATO Trust Fund on Cybersecurity, the Southeast European Law Enforcement Center (SELEC)** according to the Action Plan to Implement 2020 Strategy on Enhancing Interior Ministry Institutions.

Ukraine ratified the Council of Europe Convention on Cybercrime (CETS No. 185) or the Budapest Convention. It introduced the majority provisions of substantive law to its legislation in contrast to the procedural rules. The Criminal Procedure Code of Ukraine lacks **definition of electronic evidence and its collection procedure**, for instance. Ukrainian courts cannot accept files and electronic traces as evidence without such a definition. Law enforcement officers have to collect hardware since copies are not acceptable. Often courts do not accept electronic evidence on the grounds of improper submission.

The European Union adopted the EU Cybersecurity Act in 2019 introducing **a new cybersecurity certification framework for ICT products, services and processes.** Companies have to undergo certification process only once and see their certificates recognised across the European Union. **Ukraine could introduce similar practice.**

In addition to legislative novelties, Ukrainian cybersecurity system suffers from **the limited state capacity to provide a competitive remuneration for its cybersecurity experts.**

Besides, Ukraine's international partners including the EU Advisory Mission to Ukraine conducted series of trainings for the interior ministry and its institutions to enhance the capacity of ICT experts and decision-makers.

/

3. PERSONAL DATA PROTECTION

The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) entered into force in 2018 after two years of transition period, strengthening personal data protection system in the European Union.

Since the EU-Ukraine Association Agreement was signed before the GDPR, Ukraine has no obligations regarding its incorporation into national law. The article 15 of the Agreement is quite vague: «The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards.» Nevertheless, Ukrainian authorities committed to **«improve its personal data protection legislation in accordance with the Regulation (EU) 2016/679»** in the Association Agreement Action Plan.

Ukraine established coordination working group drafting amendments to the Law of Ukraine On Personal Data Protection in accordance with the GDPR. European experts of the Twinning № UA/47b EU project called «Implementation Of The Best European Practices With The Aim Of Strengthening The Institutional Capacity Of The Apparatus Of The Ukrainian Parliament Commissioner For Human Rights To Protect Human Rights And Freedoms (Apparatus)» participate in this process.

The ombudsman and courts are the only institutions responsible for monitoring the application of the personal data protection legislation for the moment. The GDPR envisions **a special independent supervisory authority** for this purpose, instead.

Personal data means any information enabling to identify a person like name, address or even IP address. The Regulation distinguishes **special categories of personal data**, like trade union membership, political opinions, religious beliefs, racial origin and sexual orientation, requiring significantly stricter protection.

The company is obliged to obtain a **freely given consent according** to the GDPR, not by default. For instance, the data subject shall tick the consent box. The controller/company shall provide the information regarding the purposes of the processing for which the personal data are intended. The information shall be provided in writing using clear and plain language.

The controller shall implement appropriate technical and organisational measures to ensure data protection. It must explain which data and why it processes and how long these data are stored; designate a **data protection officer**; and ensure the **security** of the processing (encryption, pseudonymisation, etc).

Meanwhile, users get more control over their personal data. They can submit information request to the company/controller. The Regulation also ensures **right to erase or right to be forgotten** when the personal data are no longer necessary, the data subject withdraws consent, there are no overriding legitimate grounds for the processing, or the personal data have been unlawfully processed, just to mention a few.

The supervisory authority shall have the power to impose an **administrative fine**. If the company processes personal data not in an appropriate manner, it is fined. If it does not have data protection officer, it is fined. If the security of processing is not guaranteed, it is fined. For instance, Polish data protection authority fined 220 thousand euro from a data broker company for failure to inform individuals that their data were being processed.

France fined 50 million euro from Google for failure to provide enough information to users about how it collected data to personalise advertising. The option to personalise ads was pre-ticked when creating an account, breaching the GDPR.

At the same time, supervisory authorities of EU member states still prefer dialogue over sanctions, especially with small companies whose primary activities are not about personal data processing.

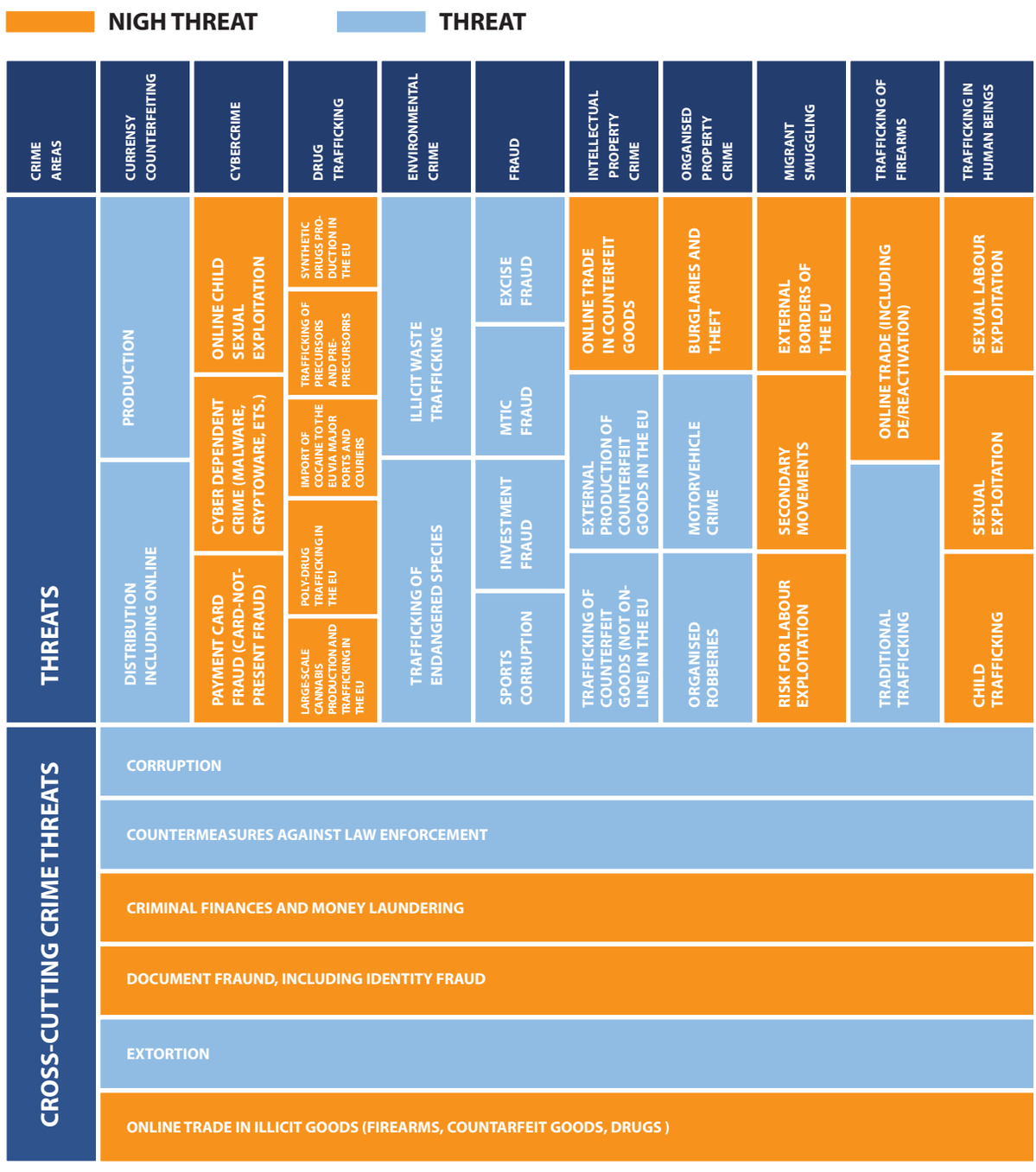
When incorporated to Ukrainian law, the Regulation would facilitate law enforcement cooperation between Ukraine and the EU countries. It would also serve Ukrainian business dealing with European citizens' personal data like IT companies.

/

4. COMBATING ORGANISED CRIME

The cooperation with the EU in combating organised crime is envisioned both by the article 22 of the Association Agreement and its Action Plan.

At the moment, Ukraine is implementing the European concept of Intelligence Led Policing (ILP). Its gist is the strategic and operational planning in the fight with organised crime. It means criminal analysis and risk assessment, among other things. The analytic component is weak in Ukraine because the national police has a limited access to the specific software and the information exchange between law enforcement agencies provide an ample space for improvement, just to mention a few. The **Europol's Serious and Organised Crime Threat Assessment (SOCTA) methodology** could significantly enhance the analytic capacities. The EU Advisory Mission to Ukraine shares this view. Ukraine committed to introduce it by 2023. The methodology foresees application of qualitative and quantitative methods to identify the biggest threats. Here is an example from the most recent Europol's report published in 2017:



Source: https://www.europol.europa.eu/socta/2017/conclusions.html

Meanwhile, Ukraine is still **drafting its Strategy on Fighting Organised Crime**. Such a strategy and its action plan shall be elaborated by 2020 and implemented by 2024 pursuant to the government plans.

The cooperation with Europol and other relevant international institutions is an important part of Ukraine's European integration. For this purpose, Ukraine completed the ratification of Memo on mutual understanding with Europol as to establishment of secure communication line.

Ukraine already has access to Interpol's databases: 157 border crossing points are connected to them. But if If Interpol focuses mainly on establishing and maintaining global databases and joint police operations, Europol provides analytic, technical, and financial assistance to prevent and fight with serious crimes and terrorism.

Another challenge is the **availability of modern equipment which could enhance Ukrainian law enforcement capacity to combat organised crime.** Such a support is provided by the European Union within the framework of Support for Rule of Law Reforms in Ukraine – in the Areas of Police and Public Prosecution and Good Governance (PRAVO-II) project. For instance, this project procured and delivered 150 personal computers and 20 printers to the Strategic Investigations Department of the National Police of Ukraine in 2018.

New legal highs constantly appear in Ukraine. They are legal since not included into the list of narcotic drugs, psychotropic substances, precursors. Ukrainian government issued the decree on monitoring drug and alcohol situation in Ukraine in 2019 introducing European rules. The monitoring is carried out by the MHE Center for Mental Health and Drug and Alcohol Monitoring of the Ministry of Healthcare of Ukraine according to the indicators defined by the European Monitoring Center for Drugs and Drug Addiction (EMCDDA), the United Nations Commission on Narcotic Drugs, and the International Committee on Drug Control. The cooperation with law enforcement agencies is part of the procedure allowing to reveal illicit trade of psychoactive substances and the related crimes. Besides, EMCDDA's experts within the EU4Monitoring Drugs project shared their experience of online monitoring and testing in lab sewage that may contain narcotic drug residues.

But Ukraine needs **to adopt Procedure for recognising drugs/substances as narcotic drugs and psychotropic substances ensuring appropriate prevention of illicit trafficking of new psychoactive substances.** The procedure shall take into account European practice of preventing new psychoactive substances from ending up in the illicit trafficking. It must guarantee prompt and efficient procedure of including new narcotics to the the list of narcotic drugs, psychotropic substances, precursors. The healthcare ministry drafted the relevant order. The main player, according to it, is the State Service of Ukraine on Drugs and Drug Control. It can summon interagency working group for the evaluation of drugs and substances to discover and recognise narcotic drugs and psychoactive substances.

Besides, Ukraine aims **to join the EU early warning system for new psychoactive substances** to get access to the information on new narcotics, trade and manufacture points, just to mention a few.[1]

Ukraine also committed **to join the Pompidou Group – Cooperation Group to Combat Drug Abuse and Illicit Trafficking in Drugs.** It aims to end illicit drug use and trafficking.

Ukraine has 2019-2020 Action Plan on Implementing State Drug Policy Strategy for the period up to 2020 that shall be implemented. The new strategy and its action plan for the period until 2025 remain pending issues in line with its European integration.

1
Examples of initial reports prepared pursuant to the early warning system: http://www.emcdda.europa.eu/publications/topic-overviews/eu-early-warning-system

The National Police is present on Ukrainian TV and social media broadcasting videos of arresting criminal suspects to prevent and combat human trafficking. An example of such a programme is the Police Wave on the Espresso TV channel. The police discovered four organised crime groups trafficking people during the first half of 2019. Ukraine is also implementing the 2016-2020 State Social Programme for Combating Trafficking in Human Beings.

The Group of Experts on Action against Trafficking in Human Beings (GRETA, the Council of Europe) notices the progress of Ukraine in the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings in its 2018 report. However, it lists **issues for immediate actions** in the brackets to the para 240. For instance, GRETA urges the Ukrainian authorities to strengthen their efforts to prevent trafficking for the purpose of labour exploitation as well as children trafficking.

Ukraine successfully fulfil its obligations to the EU regarding readmission. It **continues talks on implementing protocols to the EU-Ukraine Readmission Agreement and readmission agreements with the countries of origin/transit of irregular migrants.**

Ukraine adopted a new law on preventing and counteracting to legalisation (laundering) of the proceeds of crime, terrorist financing, and financing proliferation of weapons of mass destruction, approximating Ukrainian legislation to the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and the Regulation (EU) 2015/847 on information accompanying transfers of funds. The law streamlines financial reporting of primary financial monitoring entities (banks, insurers (reinsurers), credit unions, pawn brokers, stock market, payment organisations and other financial institutions). For instance, the threshold for mandatory financial reporting of financial transactions is increased from UAH 150 to 400 thousand, and the number of the indicators of such transactions is reduced from 17 to 4. Moreover, the law applies risk-oriented approach to the due client examination and case-by-case reporting of suspicious transactions. It introduces stricter obligations regarding the information on ultimate company beneficiaries as well as sanctions.

Besides, Ukraine is implementing **the strategy of improving the system of preventing and counteracting to legalisation (laundering) of the proceeds of crime, terrorist financing, and financing proliferation of weapons of mass destruction for the period up to 2020.**

It has t**o conclude international agreements (memorandums) on cooperation in countering legalisation (laundering) of proceeds of crime and terrorist financing by 2024.**

Ukraine plans to oblige air carriers to transfer passenger name record (PNR) data of passengers to better address serious offenses. When you book or purchase flight tickets, you get a PNR number. The data you provide are PNR. The EU already applies relevant legislation due to the Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, entered into force in May 2018. **The incorporation of this directive into national law would allow Ukrainian law enforcement to exchange the information with EU member states.**

Besides, the EU Advisory Mission to Ukraine **presented the «Cash Team» system in Ukraine** in 2018. The «cash teams» should be established in airports and ports. Their work involves the use of data and analyses from a number of different agencies like national police, border guards, security service, customs service. This could include passenger name records from flights or evidence of cross border cash flows.

/

5. SUGGESTIONS

CYBERSECURITY

- adopt the 2020 Action Plan on Cybersecurity Strategy;

- pass laws and/or bylaws to implement the Law on Cybersecurity Foundations of Ukraine;

- transpose the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, the NIS Directive, including:

- **clarify which objects belong to the critical infrastructure and the procedure of their audit. A relevant law or bylaw could fix this gap;**

- **determine obligations of digital services suppliers (online marketplaces, online search engines, cloud services);**

- **outline the mechanism of the public-private cooperation;**

- conclude memorandum of cooperation with the European Union Agency for Cybersecurity (ENISA) , NATO Trust Fund on Cybersecurity, the Southeast European Law Enforcement Center (SELEC);

- define electronic evidence and its collection procedure in the Criminal Procedure Code of Ukraine;

- introduce the rules of the EU Cybersecurity Act, in particular the new cybersecurity certification framework for ICT products, services and processes;

- improve the state capacity to provide a competitive remuneration for its cybersecurity experts.

PERSONAL DATA PROTECTION

- **improve the personal data protection legislation in accordance with the Regulation (EU) 2016/679, including:**

- establish a special independent supervisory authority for personal data protection;

- oblige companies/controllers to obtain a freely given consent;

- oblige companies/ controllers to implement appropriate technical and organisational measures to ensure data protection designating a data protection officer and guaranteeing the security of the processing (encryption, pseudonymisation, etc);

- ensure right to erase or right to be forgotten when the personal data are no longer necessary, the data subject withdraws consent, there are no overriding legitimate grounds for the processing, or the personal data have been unlawfully processed, just to mention a few;

- provide the supervisory authority with the power to impose an administrative fine.

COMBATING ORGANISED CRIME

- introduce the Europol's Serious and Organised Crime Threat Assessment (SOCTA) methodology;

- draft Strategy on Fighting Organised Crime and its Action Plan;

- provide law enforcement agencies with modern equipment enhancing their capacity to combat organised crime.

COUNTERING DRUG-RELATED CRIMES

- adopt Procedure for recognising drugs/substances as narcotic drugs and psychotropic substances ensuring appropriate prevention of illicit trafficking of new psychoactive substances;

- join the EU early warning system for new psychoactive substances;

- join the Pompidou Group – Cooperation Group to Combat Drug Abuse and Illicit Trafficking in Drugs;

- continue actions pursuant to the 2019-2020 Action Plan on Implementing Public Drug Policy Strategy for the period up to 2020 and draft new strategy and its action plan until 2025

AGAINST TRAFFICKING IN HUMAN BEINGS

- address issues for immediate actions listed in the para 240 of the 2018 report of the Group of Experts on Action against Trafficking in Human Beings (GRETA, the Council of Europe).

COMBATING IRREGULAR MIGRATION

- continue talks on implementing protocols to the EU-Ukraine Readmission Agreement and readmission agreements with the countries of origin/transit of irregular migrants.

FIGHT WITH MONEY LAUNDERING AND TERRORIST FINANCING

- continue the implementation of the strategy of improving the system of preventing and counteracting to legalisation (laundering) of the proceeds of crime, terrorist financing, and financing proliferation of weapons of mass destruction for the period up to 2020;

- conclude international agreements (memorandums) on cooperation in countering legalisation (laundering) of proceeds of crime and terrorist financing;

- incorporate the Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;

- establish the "Cash Teams" in airports and ports with the assistance of the EU Advisory Mission.