MAX PLANCK INSTITUTE
FOR THE STUDY OF
CRIME, SECURITY AND LAW

Developing Public-Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing

RECOMMENDATIONS OF THE ISF-POLICE-FUNDED RESEARCH PROJECT "PUBLIC-PRIVATE PARTNERSHIPS ON TERRORISM FINANCING"

This report was funded by the European Union's Internal Security Fund — Police.

This report builds on the work of a multinational group of legal experts that was directed by

Dr. Benjamin Vogel
Senior Researcher, Max Planck Institute
for the Study of Crime, Security and Law

and additionally comprised

Prof. Dr. Lorena Bachmaier-Winter (Universidad Complutense de Madrid)

Dr. Magdalena Brewczyńska (Tilburg University)

Dr. Ana Carolina Carlos de Oliveira (Universitat Pompeu Fabra)

Dr. Silvia De Conca (Vrije Universiteit Amsterdam)

Prof. Dr. Jonathan Fisher KC (London School of Economics)

Dr. Nandor Knust (Universitetet i Tromsø)

Prof. Dr. Eleni Kosta (Tilburg University)

Dr. Giulia Lasagni (Università di Bologna)

Dr. Maxime Lassalle (Université de Bourgogne)

Dr. Aaron Martin (Tilburg University)

Manos Roussos (Tilburg University)

Dr. Bart van der Sloot (Tilburg University)

DOI: https://doi.org/10.30709/eucrim-2023-031

Published in February 2024

Max Planck Institute for the Study of Crime, Security and Law

Günterstalstraße 73 · 79100 Freiburg i. Br., Germany

Tel.: +49 761 7081-0

www.csl.mpg.de

Developing Public-Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing

Recommendations for the European Union

Benjamin Vogel/Maxime Lassalle

https://doi.org/10.30709/eucrim-2023-031

Contents

I. Public-Private Information Sharing as One Way to Improve the Performance of AML/CFT

Questions about the performance of AML/CFT

Since the early 1990s, the Anti-Money Laundering (AML) framework (later complemented with Countering the Financing of Terrorism, CFT) has seen steady expansion, requiring an ever-growing number of financial institutions and other private businesses to conduct customer due diligence (CDD) and report suspicious transactions. While private stakeholders and public authorities have been investing considerable resources in the functioning of the regulatory framework, the results of these efforts have been criticised from various angles.

To be sure, some of the criticism of current AML/CFT must be treated with caution.[1] Though critical accounts often cite the quality of Suspicious Activity Reports (SARs) in particular as evidence, on its own this factor does not allow clear conclusions about the performance of the existing regulatory setup.[2] While only a small fraction of SARs usually lead to the initiation of criminal investigations, generally little is known about the complementary role these reports may play as information to support ongoing investigations or operational analyses by Financial Intelligence Units (FIUs). Furthermore, the usefulness of SARs depends not just on their quality but on how they are processed by FIUs and other relevant authorities. Past experiences indicate that often SARs are not adequately exploited even if they contain clear indications of financial crime. If this is the case, any criticism of the AML/CFT framework would rightly be based not so much on the quality of SARs and the underlying efforts of the private sector, as on problems at the level of the competent authorities. Furthermore, there are good reasons to believe that having a large number of unsubstantiated SARs is not in itself a sign that the reporting system is ineffective, but rather an unavoidable side effect of obliged entities' choice to err on the side of caution when deciding whether to file a SAR. Seen in this way, the large number of non-actionable SARs may not be the primary problem – instead, the focus should lie at least as much on how to distinguish between relevant and irrelevant SARs. Besides, in some jurisdictions, SARs may say little about the role of obliged entities in the investigation of crime, especially in Member States where investigative authorities traditionally enjoy great flexibility to interact with, and obtain data from, private entities directly.

Despite these caveats, the fight against financial crime can hardly be called a success story. After all, only a small fraction of criminal assets in the EU are

[1] See M Levi/P Reuter/T Halliday, "Can the AML system be evaluated without better data?", 69 *Crime, Law and Social Change* (2018), pp. 307–328.

[2] In this sense, already, Europol, "From suspicion to action, Converting financial intelligence into greater operational impact," 2017, p. 29.

detected and confiscated. Worryingly, the criminal infiltration of the legal economy, though a key element of organised crime,[3] is rarely uncovered.[4] In view of the massive revenues generated by organised crime, one can conclude that criminals are usually still able to hide their assets in the EU, indicating that current regulation largely fails in its objectives. While the AML/CFT framework forces criminals to make efforts to hide their wealth and thus imposes additional costs on them, its overall crime-reduction effect remains in doubt.[5]

Explaining current shortcomings

Of course, even a well-functioning AML/CFT framework has limits to what it can achieve while also respecting the rule of law and fundamental rights. However, several decades of experience indicate that from its start, AML/CFT has been marred by an important design flaw, namely that initial expectations were too optimistic on one particular point: the ability of obliged entities to detect crime on their own. As governmental bodies have issued financial crime typology papers more frequently, the private sector's understanding of crime risks has improved somewhat. Yet typologies alone are hardly satisfactory, in part because producing, disseminating and effectively implementing them often simply constitutes too slow a response to rapid changes in financial crime methods.

In light of these experiences, the limitations have become evident for an AML/CFT system in which information about financial crime flows almost exclusively in one direction, from the private sector to the authorities. These limitations are not simply a matter of the level of obliged entities' general understanding of financial crime. When authorities fail to share information, obliged entities will frequently be left unprotected against specific threats, and thus will ultimately be more vulnerable to infiltration by criminals. In addition, as AML/CFT is intended not only to protect the integrity of the financial system, but also to support criminal investigations, it is hardly convincing that the AML/CFT framework so far provides little guidance on operational cooperation between investigative authorities and obliged entities.

The above points do not of course offer a full explanation of the shortcomings in the fight against financial crime. Other areas of concern pertain in particular to the cooperation between FIUs, criminal justice, and supervisory authorities; to ambiguities and lacunas in the design of CDD obligations and their coordination with data protection law; to the quality of supervision; and to

[3] Europol, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, "A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime," p. 15.

[4] For an assessment of this phenomenon, see EU Savona & G Berlusconi (eds.), *Organized Crime Infiltration of Legitimate Businesses in Europe: A Pilot Project in Five European Countries*, Transcrime – Università degli Studi di Trento 2015.

[5] See PC van Duyne/JH Harvey/LY Gelemerova, The Critical Handbook of Money Laundering: Policy, Analysis and Myths, 2018, pp. 260–266.

cross-border cooperation between FIUs.[6] Above all, improvements to the regulatory system, no matter how elaborate, are unlikely to make a big difference if the relevant authorities are not suitably equipped for their respective tasks. These include not least the crucial task of supervisors and investigative authorities to uncover cases of criminal infiltration of obliged entities.

Towards more public-to-private information sharing

However, if the current AML/CFT framework suffers from the design flaw of one-sidedly relying on information flows from the private to the public sector, this is a weakness that should be addressed – particularly in light of the EU's new security environment, in which the fight against illicit financial flows has been declared crucial for defending European democracies against infiltration not only by organised crime, but also by malign State actors and their associates. It is unlikely that criminal prosecutions and the confiscation of assets alone will suffice to deal effectively with these security challenges. Beyond these traditional approaches, policy should therefore strive to strengthen the relevant institutions' resilience by improving obliged entities' understanding of general and specific threats. At the same time, such an improved understanding would benefit competent authorities by generating more meaningful information for FIUs and investigative authorities.

II. The Rise of Information-Sharing Public-Private Partnerships

Reflecting a belief that information sharing between competent authorities and obliged entities will improve the effectiveness of obliged entities' CDD, and of the fight against financial crime more broadly, recent years have seen a movement in Europe and beyond towards the creation of AML/CFT public-private partnerships. Previous research has already thoroughly documented these developments in great detail and identified operational potentials as well as challenges.[7] Furthermore, in 2022, a Commission Staff Working Document summarised main characteristics of partnerships across the EU and provided guidance for policymakers.[8] Building on these previous works and complemented by the authors' own observations of relevant practices, the

[6] For an in-depth analysis of these concerns in EU law, see B Vogel JB Maillart, National and International Anti-Money Laundering Law, Developing the Architecture of Criminal Justice, Regulation and Data Protection, 2020, p. 883–1027, downloadable at https://pure.mpg.de/rest/items/item_3262446_6/component/file_3286393/content

[7] For a comprehensive account, N Maxwell, Future of Financial Intelligence Sharing (FFIS) research programme, "Five years of growth in public–private financial information-sharing partnerships to tackle crime," 2020.

[8] European Commission, Commission Staff Working Document on the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing of 27 October 2022, SWD(2022) 347 final.

present analysis can confine itself to a brief overview of partnerships' key features insofar as they are relevant for the subsequent development of a legal framework for public-to-private information sharing.

To begin with, "public-private partnership" does not refer to a single form of public-private cooperation, but serves as an umbrella term to describe various practices that can differ in many ways from one another in the objectives they pursue and the activities they undertake. Common to all of them, however, is the idea that they provide obliged entities with more or less specific information to be used by those entities in detecting indications of financial crime. Beyond this common denominator, partnerships must be distinguished primarily according to two factors: their respective specific *objectives*, and the *types of information* they provide to obliged entities.

Objectives of public-private partnerships

As regards their aims, partnerships can essentially take two approaches, either separately or in combination. The information sharing may be intended to improve obliged entities' ability to detect financial crime, and/or to harness their data in the context of ongoing investigations.[9] While the first strategy emphasises obliged entities' role as gatekeepers of the financial system, the second involves them instead as instruments in support of law enforcement authorities.

In some cases, the sharing of particular data will ultimately serve both purposes at the same time, although priority may be given to obliged entities' gatekeeping function or the support of law enforcement, depending on the case. For example, if authorities share information about current crime trends, this will usually help obliged entities to better design their CDD policy and thereby improve their ability to protect themselves against crime; insofar as this then leads to better SARs, such an improvement can also help authorities at the same time. In contrast, if obliged entities are provided with the names of particular suspects, authorities' main aim will often be to identify additional information relevant for their ongoing investigations; in that case the use of these names by obliged entities in their CDD might be only a useful side effect.

Types of information

Public-private partnerships can entail the transfer of various types of information depending on the particular aim pursued. Information can broadly be placed in two categories: first, operational information, that is, information that usually points obliged entities to one particular criminal case; and second, strategic information, which provides obliged entities with general features of relevant criminality.[10] Going further, one can identify numerous sub-types of

[9] See the overview in the Commission Staff Working Document, pp. 4–12.

[10] Commission Staff Working Document, p. 4; N Maxwell, "Five years of growth in public–private financial information-sharing partnerships to tackle crime," p. 13.

information, although a terminology for those sub-types is not yet commonly agreed.

Partnerships will often include the collaborative production of financial crime typologies, as well as knowledge exchange on criminal trends, as such typologies and trend information constitute the most common forms of strategic information.[11] Typologies describe features of financial crime uncovered in past criminal investigations or in past CDD practice. More specifically, typologies usually explain *modi operandi* of money laundering or terrorism financing, so that obliged entities can design their risk parameters accordingly and thereby more easily recognise criminal activity. Typologies may be based on one single case (for example explaining the dissimulation practices in one past money laundering case), but also reflect experience obtained through numerous cases over a longer period of time. A collaborative production of typologies within partnerships is intended to harness synergies by bringing together strategic knowledge from both the public and the private sector.

In comparison, information about criminal trends may signify strategic information about current criminal phenomena that pose an acute threat to the financial sector. It may refer to specific financial crime methods, for example methods to dissimulate the origin of funds, or to the commission of predicate offences, for example by pointing to the activities of a particular criminal organisation that may try to abuse the financial system.

Partnerships can also serve as a means to provide obliged entities with general feedback about the quality of SARs.[12] This can in particular include information about whether obliged entities applied adequate risk parameters and whether SARs were sufficiently detailed. Even without disclosing whether the particular suspicious transaction was in fact related to crime, such feedback can help obliged entities to better tailor their SARs filings to regulatory expectations.

As they straddle the border between strategic and operational information, public-private partnerships will sometimes extend to information that goes beyond describing general features of a criminal phenomenon, but that the authorities cannot yet link to a particular person or entity. Such information will notably consist of data that proved relevant in past criminal cases, when there are reasons to believe that the same data may help uncover hitherto undetected crimes. One can think for example of postal addresses, IP addresses, virtual IBANs, or even company names that were used by criminals in the past and that the authorities provide to obliged entities in the hope that it will allow them to discover financial crimes.

When a public-private partnership involves operational information, and thus pertains to a specific case, it may also serve to provide an obliged entity with substantial feedback in response to SARs, in particular by disclosing that at

[11] Commission Staff Working Document, p. 5–8.

[12] Commission Staff Working Document, p. 8–9.

least for the time being, the FIU believes that the reported suspicion was in fact linked to criminality.[13] Such feedback might include additional details, for example an explanation of why the authorities think so, and possibly even further information about a criminal investigation already initiated in connection with the SAR. Especially if the reported customer is still with the obliged entity, that entity will usually be keen to get such information in order to protect itself, especially if it would otherwise not find out about the criminal case for a long time.

Finally, public-private partnerships can provide a setting through which the authorities inform obliged entities about ongoing criminal investigations and provide relevant details, for example the names of suspects and other persons of interest, as well as case-specific insights.[14] Such information can have a dual function. Authorities may be motivated by the hope that the information will allow the obliged entities to identify new investigative leads or produce other relevant insights. At the same time, the information may also, and sometimes even exclusively, be provided in order to warn obliged entities against particular individuals who the authorities believe constitute a financial crime threat.

Design of public-private partnerships

Existing partnerships vary in design and size, for which three factors are of particular relevance: defining the authorities involved in a partnership, deciding about the organisational structure, and choosing the obliged entities that are invited to join. Though there is no need to go deeper for the purpose of this overview, some key features are noteworthy inasmuch as they already highlight both the diversity and some of the practical challenges of partnerships.

Depending on the aims as well as the types of information to be shared, public-private partnerships in AML/CFT will usually include FIUs and/or police, though other law enforcement authorities, such as prosecutors, may also participate in some instances.[15] In addition, AML/CFT supervisors play an active role in some partnerships.[16]

The organisation of partnerships will first and foremost reflect their particular purpose. As a precondition for any long-term cooperation, they usually include a steering committee or other governance structures where participants agree on their working agenda.[17] If partnerships include a collaborative production of typologies, tasks will often be distributed among specialised working groups that include experts from relevant authorities and the private sector.[18] Where strategic information, such as typologies and notices about criminal trends, is

[13] Commission Staff Working Document, p. 11–12.

[14] Commission Staff Working Document, p. 10–11.

[15] Commission Staff Working Document, pp. 5, 6, 11.

[16] N Maxwell, "Five years of growth in public–private financial information-sharing partnerships to tackle crime," p. 15.

[17] See Commission Staff Working Document, p. 18.

[18] Commission Staff Working Document, pp. 5, 10, 12.

intended to be accessible only to a limited group of obliged entities, it can be shared both at in-person meetings and through online tools.

So far as operational information is concerned, in some partnerships confidentiality needs have led to special safeguards, such as security vetting of private-sector participants and secured locations where authorities disclose sensitive information to representatives of obliged entities.[19] Operational information will sometimes also be shared on an ad hoc basis, even in the absence of an institutionalised partnership. This can happen for example when an FIU and an obliged entity meet to discuss the substance of a particular SAR.

Similarly, an ad hoc public-private partnership can also arise if an obliged entity voluntarily collaborates with police or judicial authorities within an ongoing criminal investigation, for example when a prosecutor discloses case-specific details and asks the obliged entity to proactively support the investigation beyond what it is required to do under the applicable criminal-procedure law.

As to the selection of participating obliged entities, one must note that partnerships will necessarily be limited in scope. Collaboration requires mutual trust, and therefore excludes an open format. Selection criteria are often not clearly discernible, but are likely to focus on special expertise as well as the obliged entity's role in a particular business sector. Though strategic information can be made accessible to a large number of obliged entities or even to entire sectors, such wide dissemination can sometimes negatively impact the effectiveness of information sharing, as a wide dissemination increases the risk that the information may be obtained by criminal actors and abused by them in order to adapt their dissimulation methods. Furthermore, an overly broad number of participants can be problematic because it can invite free riders, and thereby discourage active participation. As far as the sharing of operational information is concerned, authorities will collaborate with only a handful of obliged entities, or even with only a single one, both because of confidentiality concerns and because operational information (such as substantive feedback for a SAR) is by nature often relevant only to specific obliged entities.

Legal concerns

As already pointed out by the Commission Staff Working Document, public-private partnerships do however raise a number of legal challenges. These pertain, in particular, to data protection and privacy, interference in the contractual relationship between obliged entities and their customers, and risks for the integrity of competent authorities, not least a loss of confidential or otherwise sensitive information that may compromise investigations.[20] A recent letter by the European Data Protection Board to the co-legislators and

[19] Commission Staff Working Document, pp. 17–18, 24; N Maxwell, "Five years of growth in public–private financial information-sharing partnerships to tackle crime," p. 14.

[20] Commission Staff Working Document, p. 14–16.

the European Commission has highlighted further concerns from a data protection standpoint, questioning in particular the proportionality of a monitoring of customers by obliged entities on the basis of operational information provided by law enforcement authorities.[21] As indicated by these observations, to date national legal orders are often not well prepared for enhanced public-private collaboration, especially if such collaboration would go beyond the dissemination of typologies and similar strategic information and instead also entail the sharing of operational data. In any case, the public-to-private sharing of information by competent authorities with the private sector for the purpose of preventing, detecting, and investigating crime is a topic that so far is usually only tentatively addressed by national laws. Consequently, there is an urgent need to map the various legal challenges related to public-private partnerships and develop options for legislators on how to address them.

III. Challenges and Guiding Principles for Regulating Public-to-Private Information Sharing

As explained above, public-private partnerships can take various shapes and pursue a plurality of goals. Yet despite this diversity, all these models have one feature in common: the transfer of information from public authorities to private entities. This transfer, in combination with the intended processing of this information by obliged entities, constitutes the main challenge from a legal point of view. To understand how Member States should respond to these challenges when deciding whether to introduce partnerships or other forms of public-to-private information-sharing mechanisms in AML/CFT, one must first assess the state of the law (so far rather underdeveloped) governing public-private cooperation in AML/CFT and criminal policy more generally (III.1.). Subsequently one must work out the relevant rules under EU law, as regards both the processing of customer data and the unintended consequences that information sharing could cause to customers (III.2.). This will then provide the basis for a list of principles that legislators and relevant authorities will have to address in order to respect fundamental rights (III.3.).

III.1. Public-Private Cooperation in AML/CFT and in Wider Criminal Policy

III.1.1. The Lack of an EU Framework for Public-Private Information Sharing in AML/CFT

Information sharing under EU AML/CFT law

The EU's AML/CFT framework has increasingly emphasised the role of the public sector in providing obliged entities with guidance about performing their CDD obligations. Directive 2015/849 establishes an obligation for the

[21] European Data Protection Board letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations of 28 March 2023, OUT2023-0015.

Commission, the European Supervisory Authorities (ESAs), and Member States to identify and assess money laundering and terrorism financing risks at regular intervals and to make their findings available to obliged entities.[22] Further guidance specifying risk factors is required from the European Banking Authority (EBA),[23] and Member States' authorities must provide obliged entities with up-to-date information on the practices of money launderers and financers of terrorism and on indications leading to the recognition of suspicious transactions.[24] EU law, however, specifies neither the scope of such information nor how the associated information gateways should function. Moreover, although FIUs are under a general obligation to provide feedback to obliged entities on SARs that these entities file,[25] EU law remains silent on the scope and frequency of this feedback. As a result, in most cases obliged entities at the level of the Member States have received no specific guidance beyond the EBA's risk factors[26] and the typologies provided by various supranational institutions, most importantly the FATF.[27] In short, while EU law now presupposes that public-private information sharing is a prerequisite for the effective functioning of the AML/CFT system, it does not yet provide meaningful guidance on how to put such information sharing into practice.

Given this state of affairs, the development of public-to-private information sharing ultimately comes down to national legislators. In fact, some States' laws already provide specific public-to-private information-sharing powers, not least for the benefit of police authorities. Yet especially insofar as personal data is concerned, the introduction of more extensive public-to-private information sharing necessitates far more than a legislative clarification of the types of information to be shared and the creation of appropriate sharing mechanisms. Introducing information-sharing mechanisms can heavily impact how the overall AML/CFT framework operates, especially because the more the authorities share information with obliged entities, the more the measures taken by the private sector might to a large extent be determined by the authorities, thus leading to a blurring of the responsibilities of public and private actors. As a consequence of information sharing, a process that AML/CFT law has hitherto placed under the control of obliged entities might transform into a measure that is, at least partially, attributable to the authorities.

---

[22] Art. 6(1)–6(3) and 6(5), Art. 7(1) and 7(4)(a)(e) of Directive (EU) 2015/849 of 20 May 2015, as amended by Directive (EU) 2018/843 of 30 May 2018.

[23] Arts. 17 and 18(4) of Directive (EU) 2015/849, as amended by Directive (EU) 2019/2177.

[24] Art. 46(2) of Directive (EU) 2015/849.

[25] Art. 46(3) of Directive (EU) 2015/849.

[26] European Banking Authority, "Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions" ("The ML/TF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849, 1 March 2021.

[27] See for example FATF, "Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing" of September 2020.

Public-to-private sharing as a de facto enhancement of authorities' powers

Insofar as such a blurring of responsibilities occurs, it can be highly questionable whether CDD provisions under current AML/CFT law provide obliged entities with a sufficient legal basis. Four phenomena in particular stand out that current AML/CFT law does not yet anticipate, all of which can result from the interplay of public-to-private sharing and obliged entities' obligations under AML/CFT law: first, the authorities' having access to a new form of bulk surveillance; second, a partial delegation of information-gathering to the private sector; third, a targeted surveillance of customers; fourth, the occurrence of state-induced de-risking – that is, the discontinuation of business relationships due to information provided by the authorities.

Customer screening as bulk surveillance

As regards the use of information from the authorities as a basis for screening customers' financial activities as a means of detecting crime, one must note that obliged entities are required as part of their CDD to conduct an ongoing monitoring of generally every business relationship.[28] This means that they must screen their customers' transactions for factors that indicate an enhanced risk of money laundering or terrorism financing. In the area of financial transactions, the AML/CFT framework has thereby effectively created a surveillance framework that covers virtually all electronic financial transactions performed in the EU. Up to now, however, this surveillance has been controlled not by state authorities, but by the numerous obliged entities that carry out these transactions. But if this continuous monitoring is based on information provided by the authorities, in the sense that the authorities define screening parameters that obliged entities use, these authorities can exercise effective control over the monitoring. That control will be particularly far-reaching if authorities provide obliged entities with names of specific individuals or entities, in the expectation that the obliged entities will screen all business relationships for possible connections with these targets. In this case a surveillance framework that AML/CFT law intends to be controlled by the private sector becomes a bulk surveillance tool of the authorities.

A partial delegation of information-gathering to obliged entities

As a consequence of the risk-based approach to CDD, whenever obliged entities decide about the risk profile of a customer and determine the necessary scope of CDD, they are required to consider all relevant information available to them, not least the information that a particular customer is the subject of a criminal investigation. Therefore if investigative authorities or FIUs provide an obliged entity with risk-relevant information about a specific individual or entity, the obliged entity's CDD obligations may require it to conduct a more or less far-reaching analysis of its customer data, which may include an obligation to take proactive steps on its own to produce additional information about the targeted

[28] Art. 13(1)(d) of Directive (EU) 2015/849 of 20 May 2015.

customer, for example about the origin of funds, the control structure of corporate customers, or the purpose of a business relationship. This information will then also be available to the authorities.

Enhanced CDD as an instrument of targeted surveillance

Furthermore, it must be noted that enhanced CDD obligations entail an obligation to subject specific high-risk business relationships to enhanced continuous monitoring. As a consequence, information requests by the authorities can in some cases effectively lead to a targeted monitoring of a suspected customer for the benefit of the requesting authorities – namely, where an obliged entity continues a business relationship with a customer, at least on a temporary basis, after receiving such a request targeting that customer. By potentially tracking all transactions that the targeted person makes in the future, the information thereby obtained can then provide deep insights into a person's private life. Furthermore, while such monitoring will then pertain primarily to the customer's financial conduct, in some cases it can also extend to a monitoring of a customer's physical movements, not least if the IP address used for accessing an online banking application allows the obliged entity and, ultimately, also the authorities to geolocate a suspect. Insofar as such monitoring is ultimately a result of public-to-private information sharing, it may then amount to covert surveillance, especially if the obliged entity is prohibited from disclosing its interaction with the investigative authorities to the affected customer.

State-induced de-risking

Finally, it also has to be borne in mind that the public-to-private transfer of information can lead to a termination of business relationships or other adverse measures (such as an increase in fees) to the detriment of customers, especially when the information leads the obliged entity to believe that affected customers entail a high financial crime risk that the entity is unwilling to assume. After all, obliged entities are usually required to implement additional CDD measures if they become aware of information indicating that a particular business relationship constitutes an enhanced risk. As additional CDD measures will usually necessitate additional compliance resources, obliged entities are likely to reconsider their relationship with a customer, especially if these additional costs are not compensated by the profits that the relationship generates, or if the obliged entity has reputational concerns about keeping this customer. This practice, known as de-risking,[29] is usually an autonomous decision of obliged entities and therefore is generally not attributable to the authorities. However, especially where public-to-private information sharing targets particular individuals or entities, it would appear that any resulting de-risking is partially attributable to these authorities. Insofar as authorities

[29] See European Banking Authority, Opinion of the European Banking Authority on 'de-risking' of 5 January 2022, EBA/Op/2022/01, p. 1; Department of the Treasury, *AMLA - The Department of the Treasury's De-risking Strategy*, Washington, DC, 2023, p. 1.

thereby become intimately involved in obliged entities' risk management, public-to-private sharing leads to consequences that the current design of AML/CFT laws does not anticipate.

III.1.2. The Role of the Private Sector in the Investigation and Prevention of Crime

Looking at legislative options for how to regulate public-to-private sharing in AML/CFT, one should start by broadening the perspective and inquire whether existing public-private collaboration in other areas of criminal policy may offer guidance. Efforts to fight crime have of course always relied heavily on private parties. With the rise of digitalisation in all areas of modern life, this role has expanded considerably. Nowadays more and more data is held by private companies as a result of the rise of digital services, including online market-places and social networks. In addition, as more and more human activity in the physical world is organised with the help of digital devices – for instance in transportation, the delivery of goods, or even housekeeping – day-to-day human activity leaves more and more digital traces that will be stored, to a greater or lesser extent, by private companies. As a consequence, investigators are finding this wealth of private data increasingly relevant for collecting information about crimes committed not only online, but also outside cyberspace. This is most obvious with regard to telecommunications traffic data and financial data, both of which can allow authorities to deduce information about a person's offline activities. In short, today the role of the private sector as a facilitator of criminal investigations stretches well beyond the traditional role of witnesses to report on past events they observed; instead, private businesses often automatically record information directly linked to the commission of a crime at the very moment of its commission, and this information can then be exploited retrospectively for investigative purposes. Based on the recently adopted E-Evidence Regulation, competent authorities are now even allowed to interact directly with certain providers of online services in another Member State.[30]

While authorities' reliance on the collection of data by the private sector is arguably the area where the role of such data collection as a facilitator of criminal proceedings is most directly felt, criminal-procedure laws also recognise ways in which private parties may support investigations in more proactive ways. This is the case notably when investigators rely on informers – more specifically on private individuals who are willing to collaborate with the authorities to covertly collect information.[31] In a somewhat similar vein, national criminal-procedure laws have also started to embrace private

[30] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. See in particular Art. 3(3) on the definition of service providers, which does not include financial service providers.

[31] See ECtHR, *Castro v. Portugal*, no. 44/1997/828/1034, 9 June 1998, para. 35.

investigations as a way of uncovering crimes committed within the sphere of private companies. These internal investigations are initiated by the affected company itself, but regularly conducted by a third party, such as law firms or service providers specialising in private investigations. While the law is often not conclusive about the extent to which authorities can rely on the products of internal investigations as evidence in criminal proceedings, private internal investigations can serve in any case as a lead for investigative authorities. Internal investigations can be extensive in scope – for example, in some cases they may rely on interviews of dozens or even hundreds of employees and on an analysis of millions of emails and other communications. Where the resulting findings are used as evidence at trial or as the basis of a plea agreement, the widespread acceptance of internal investigations signals that today's criminal-procedure laws allow for an exercise of investigative functions by private actors, sometimes to a significant degree.[32]

Beyond an extensive reliance of criminal investigations on private actors, laws are increasingly also allowing private parties a growing role in the prevention and detection of crime. Indeed, reliance on the private sector is particularly well-developed in the AML/CFT framework. However, similar developments can now also be observed with regard to hosting content on the internet, in that in some cases, Regulation (EU) 2021/784 requires hosting-service providers to take specific measures to prevent the dissemination of terrorist content.[33] More comprehensively, Regulation (EU) 2022/2065 (the "Digital Services Act"), while not imposing a general obligation on data transmission and data storage providers to actively monitor information, does require providers of hosting services, including online platforms, to put mechanisms in place to allow any individual or entity to notify them of illegal content so that this content can be removed or access to it can be disabled.[34] Furthermore, this regulation also requires providers of hosting services to promptly inform law enforcement or judicial authorities when they become "aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place".[35] It is also noteworthy that Regulation (EU) 2022/2065 requires providers of online platforms, when processing user complaints, to give priority to notices submitted by "trusted flaggers", meaning entities (including qualifying non-governmental organisations and private and semi-public bodies) that have "particular expertise and competence for the purposes of detecting, identifying

[32] For a transatlantic perspective see "Privatized Prosecution: The Outsourcing of White Collar Criminal Investigations to Big Law and Its Fifth Amendment Implications" (https://journals.library.columbia.edu/index.php/CBLR/announcement/view/407).

[33] Art. 5 of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

[34] Arts. 8, 6(1) and 16(1) and (3) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

[35] Art. 18(1) of Regulation (EU) 2022/2065.

and notifying illegal content".[36] Beyond requiring the providers of online platforms to remove or to disable access to illicit content they become aware of, Regulation (EU) 2022/2065 also imposes a preventive obligation on the providers of online platforms, requiring them to "suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content."[37] Elsewhere, reliance on the private sector for the purpose of preventing crime also appears outside AML/CFT and the regulation of online services, albeit to a limited extent. Air carriers, for instance, have been involved in the surveillance of their customers, although they are mainly in charge of collecting data, while the analysis is left to public authorities.[38] And economic operators who trade in specific substances that entail a risk of being used for the production of explosives are under an obligation to perform CDD and report suspicious transactions.[39]

However, comparative legal research undertaken for the present recommendations has revealed that even as legal orders rely more and more extensively on private parties in the prevention, detection and investigation of crime, national laws are only tentatively beginning to address the legal questions that result from this development.[40] It is true that, not least as a consequence of the case-law of the ECJ, national legal orders have increasingly defined limits on investigative authorities' use of telecommunications traffic data, reflecting the fact, as stressed by the ECJ, that this data allows for a very far-reaching surveillance of citizens. To some extent, especially through Regulation (EU) 2022/2065 as regards adverse measures adopted by hosting services, the law is also increasingly attentive to detrimental consequences that individuals may suffer as a result of the private sector's involvement in criminal policy. However, overall, the law is only beginning to adapt to the increasing interdependence between law enforcement and the private sector. Uncertainty is widely observable in several key respects, four of which are particularly relevant in the present context. First, while telecommunications data has been singled out by the ECJ, it remains unclear to what extent the underlying assumptions require similar limitations for other types of bulk data as well. Second, although the gathering of information is frequently delegated to private investigators, the rules applicable to them are frequently defined only sparsely

---

[36] Art. 22(1) and (2) and recital 61 of Regulation (EU) 2022/2065.

[37] Art. 23(1) of Regulation (EU) 2022/2065.

[38] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[39] Arts. 8 and 9 of Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013.

[40] For a detailed analysis of the current legal status quo, see the analysis of national legal orders in the forthcoming final report of the ParTFin project: B Vogel/E Kosta/M Lassalle (eds.), *Public-Private Information Sharing in the Fight against Money Laundering and Terrorism Financing*, Intersentia 2024.

or not at all, especially from a data protection point of view. Third, while national laws often seem to allow competent authorities to disclose information to private parties, the conditions and scope of such disclosure are seldom clearly defined. Finally, where private entities are tasked by law with preventive functions, safeguards for individuals affected by such measures remain undeveloped or quasi non-existent. In conclusion, this means that the current rules on public-private collaboration in matters of criminal policy offer only scarce guidance on how to develop public-to-private information sharing in AML/CFT.

III.1.3. Voluntary Public-Private Cooperation as Legally Uncharted Territory

III.1.3.1. Voluntary Public-Private Cooperation in Current Criminal Policy

When envisaging public-to-private information sharing within partnerships, and thus within mechanisms in which obliged entities' participation is voluntary, legislators furthermore need to be aware that this voluntary aspect adds another layer of complexity. As comparative research has shown, Member States are used to thinking about combating serious criminality like terrorism financing and money laundering by imposing obligations on individuals and entities. In contrast, in this context voluntary cooperation of the private sector is rarely part of the vocabulary of the law, which instead often focuses exclusively on coercive measures.[41] Private businesses are traditionally not seen as partners of investigative authorities, but rather as the addressees of obligations to provide information, in particular as addressees of subpoenas and production orders in criminal proceedings. Clearly, in the fight against serious crime, the law has traditionally adopted a top-down approach, in light of which the very idea of public-private partnerships can appear dubious.

However, although the law remains largely silent on this issue, informal, partially voluntary forms of public-private interaction have already developed, even in the context of criminal investigations. For example, investigative authorities will often refrain from coercive acts – especially from searching a company's offices and seizing documents – if the company agrees to provide the desired information voluntarily. Such consensual cooperation can carry benefits for both sides. For the authorities, it saves time and resources that coercive investigative measures would require. Relying on voluntary cooperation from the private sector can also be much more efficient, since the private side usually has a better understanding of its own databases and will therefore often find it easier to identity information likely to be relevant for the authorities. For their part, companies can prefer consensual cooperation in order to avoid the interference in business operations, and possibly even reputational damage, that a search of premises and a confiscation of computers would entail. Furthermore, voluntary cooperation provides companies with an opportunity to

[41] S Ruggeri, "Multiculturalism, coercive measures, human rights in EU judicial cooperation in criminal matters" in *Criminal Proceedings, Languages and the European Union*, Francesca Ruggieri (ed.), Springer, 2014, pp. 215–237.

influence how much of their data, and what data, is disclosed to the authorities. For very similar motives, companies often voluntarily conduct internal investigations to detect criminal wrongdoing committed internally, and their private investigator will then often cooperate informally with investigative authorities. Other examples of voluntary cooperation in criminal investigations can be found in the context of cross-border access to information. If authorities are unable to coerce access to private data that a company stores abroad, they will sometimes be able to procure that data voluntarily.[42]

Even within the AML/CFT framework, one can identify elements that may induce voluntary public-private cooperation. For instance, while obliged entities are of course subject to CDD obligations with regard to their business relationships, they are usually free to discontinue a suspicious business relationship even if the authorities would prefer to have that relationship continue temporarily in order to gather additional financial data. Furthermore, the quality of CDD, and thus the usefulness of SARs for authorities, will depend not least of all on the efforts that an obliged entity invests to this effect. CDD obligations will usually not rule out the possibility that for reputational or other reasons, an obliged entity may undertake extra CDD efforts beyond what the law requires. In this respect, one should not overlook that the EU AML/CFT framework still suffers from considerable legal uncertainty as regards the scope of obliged entities' powers to process personal data, thus leaving room for obliged entities to determine for themselves the acceptable extent of their CDD.[43]

III.1.3.2. A Need to Provide Rules for Voluntary Cooperation

While voluntary forms of public-private cooperation between competent authorities and the private sector in the fight against crime are rarely regulated and thus usually pursued informally, legislators must take special care that such cooperation does not lead to a circumvention of the law. The fact that national law rarely addresses voluntary interaction at present is therefore not so much an opportunity as a cause for concern, since it can prompt misguided behaviour. Legislators should turn their attention to two aspects in particular, namely the need to protect the rights of third parties targeted by the cooperation, and the need to avert potential risks for the public interest.

---

[42] TJ McIntyre, "Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, their Irish Subsidiaries and European Legal Standards" in *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, F Fabbrini, E Celeste and J Quinn (ed.), Oxford, Bloomsbury Collection, 2020, pp. 139–156.

[43] See B Vogel/JB Maillart, *National and International Anti-Money Laundering Law*, pp. 989–996; WJ Maxwell, "The GDPR and private sector measures to detect criminal activity," *Revue des Affaires européennes/Law & European Affairs*, no. 1, 2021, pp. 103–116.

The protection of individual rights

Voluntary public-private cooperation is often chosen by the authorities so as to avoid recourse to formalised procedures that would entail more demanding legal requirements, such as the need to apply for a judicial warrant. If voluntary cooperation would consequently have the effect of circumventing legal safeguards, it must of course not be endorsed by legislators. Two points are particularly relevant in this respect, namely the rights of customers under data protection law or contractual secrecy duties, and defence rights in criminal proceedings.

With respect to customers' rights under data protection law or other confidentiality duties, it must be stressed that obliged entities can voluntarily consent to interference in rights only if and insofar as they have disposition over the rights in question. As regards their customers' data, this is usually the case only if they are under a legal obligation to comply with a request from the authorities, or alternatively, if they can rely on another legal ground to process customer data in the context of a voluntary public-private cooperation. As regards the latter option, it should be noted that even if an obliged entity's contract with the customer entitles it to process data for competent authorities, there will often still be doubt whether voluntary processing is also authorised. In that case, voluntary cooperation without a clear legal framework not only entails the risk of causing unlawful interference in customer data, but can expose obliged entities and their employees to liability as a result.[44]

Similarly, voluntary cooperation can also lead to tensions with defence rights in criminal proceedings. Usually, the interaction between investigative authorities and private parties is regulated through a set of obligations, particularly obligations to respond to production orders and subpoenas, and subject to particular procedural safeguards, for example a judicial warrant. If customer data is processed and disclosed outside this framework, it might not be admissible as evidence, depending on the law of the Member State concerned. Furthermore, informal interaction between authorities and private parties can create fairness concerns, since suspects and their defence lawyers might be unable to establish how, and on the basis of what information, investigative authorities reached certain incriminating conclusions. Such concerns by themselves do not constitute a reason for legislators to forgo the possibility of

[44] By way of comparison, the need to regulate voluntary transfers of data has also been recognised in some non-EU jurisdictions. For example, in the US, the Right to Financial Privacy Act (Pub. L. 95-630) acknowledges that there should be limits to the informal relationships between public authorities and banks (see N Kirschner, "The Right to Financial Privacy Act of 1978 – The Congressional Response to United States v. Miller: A Procedural Right to Challenge Government Access to Financial Records," *University of Michigan Journal of Law Reform*, nº 1, vol. 13, 1979, pp. 10–52). More recently, the Canadian Supreme Court found that voluntary cooperation by an internet service provider, acting outside the scope of any mandatory measure, is a violation of customers' right to privacy; *R. v. Spencer* of the Supreme Court of Canada (2014 SCC 43).

voluntary public-private cooperation, but they show the need for a legal framework with appropriate safeguards.

The protection of the public interest

When public-private cooperation is based on a voluntary commitment of the private actors, legislators must furthermore accommodate the fact that the interests of both sides might not always coincide. In fact, profit-oriented businesses cannot be expected to suddenly transform into agents of the public interest.[45] However, this does not exclude that their interest may overlap with the crime-fighting objectives of competent authorities. There will especially be a shared interest when cooperating businesses themselves are directly harmed by crime. Even beyond such instances, voluntary cooperation will sometimes be in the private interest, in particular when that cooperation makes it easier to meet compliance obligations or when the private side supports authorities out of reputational motives.

In any case, voluntary public-private cooperation must not lose sight of potential conflicts of interest. Obviously, if private parties voluntarily cooperate with the authorities, they have a legitimate expectation of deriving some benefit from their contribution. In any case, such benefits must be compatible with the public interest and not entail outcomes that go against the lawful interests of the public side, including those of authorities that are not directly involved in the cooperation (but whose data might be at stake). Thus, wherever the agenda and priorities of a cooperation mechanism are defined jointly by the public and private participants, conflicts of interest must be managed accordingly. Otherwise, in some cases informal cooperation may even carry reputational risks for the authorities involved, in particular if they are perceived by relevant third parties or the wider public as maintaining an untransparent relationship with sensitive businesses.

III.2. Legal Foundations of the Regulation of Public-To-Private Information Sharing

III.2.1. The Legitimacy of the Aim of Closer Public-Private Cooperation

According to Article 52(1) of the Charter of Fundamental Rights, any limitation on the rights and freedoms the Charter recognises must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The fight against terrorism financing and against serious crime, including money laundering, is recognised as such an interest.[46]

[45] On this ambiguity, see G Favarel-Garrigues, T Godefroy and P Lascoumes, "Reluctant partners?: Banks in the fight against money laundering and terrorism financing in France," in *Security Dialogue*, nº 2, vol. 42, April 2011, pp. 179–196.

[46] ECJ (GC), *Digital Rights Ireland*, 8 April 2014, C-293/12, C-594/12, para. 42; ECJ, *Sovim SA*, 22 November 2022, C-37/20 , C-601/20, para. 58.

In order to genuinely meet these general objectives, the envisaged public-to-private information sharing must also be appropriate for its purpose.[47] EU law increasingly relies on obliged entities to prevent, detect, and investigate financial crime, imposing obligations on them for CDD, reporting and further activities. Yet throughout the EU, only a small percentage of criminal assets is ultimately detected, and therefore the effectiveness of the current framework is unsatisfactory. This situation may have multiple causes, possibly including an insufficient allocation of resources to competent authorities. But there are strong reasons to believe that public-to-private sharing of strategic and also tactical information does have the potential to improve obliged entities' understanding of relevant threats and their ability to focus their compliance efforts in a more effectiveness-oriented way.

One may of course question whether a further extension of the private sector's role is indeed in the public interest, given that extensive private involvement in criminal policy can also have significant drawbacks.[48] Not least of all, legitimate fears may arise that the authorities' increasing reliance on profit-oriented private actors might expose citizens more and more to an arrangement that already today, not least in the area of AML/CFT, effectively constitutes a far-reaching privatisation of law enforcement with no adequate legal safeguards to protect citizens against private enforcers[49] and "surveillance intermediaries".[50] This would potentially undermine core premises of the rule of law.

At the same time, one must not overlook that increasing dependence on the private sector, and therefore also the need to render public-private cooperation effective, is only partially a matter of political choice. To some extent, rather, it is the consequence of societal developments and even geopolitical realities that are not easily amenable to legislative intervention. More recently, the pivotal role of obliged entities in the enforcement of EU restrictive measures, in particular, has demonstrated the strong interdependence between globally operating businesses and competent authorities in the EU. Alternatives to a deepening of public-private cooperation, most notably a possible direct oversight of financial flows by the authorities, may be even more worrying from a fundamental-rights perspective.

As one particularly problematic aspect of a closer cooperation between competent authorities and obliged entities, legislators should in any case give

---

[47] See ECJ (GC), *Ligue des droits humains*, 21 June 2022, C-817/19, para. 123.

[48] See for instance M Valsamis, "The privatisation of mutual trust in Europe's area of criminal justice: the case of e-evidence", *Maastricht Journal of European and Comparative Law*, no. 3, vol. 25, 2018, pp. 263–265.

[49] On the public role of private actors, see J Daskal, "Speech across borders," *Virginia Law Review*, no. 8, vol. 105, 2019, pp. 1605–1666. See also S Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors," *Computer Law & Security Review*, vol. 43, 2021.

[50] AZ Rozenshtein, "Surveillance Intermediaries," *Stanford Law Review*, vol. 70, 2018, pp. 99–189.

special consideration to the question whether increasing public-to-private information sharing may negatively affect the operational abilities of competent authorities by leading to abuses of sensitive information. If this would be the case, it would call into question the very appropriateness of information sharing as a way to strengthen the fight against crime. This pertains not least of all to information whose disclosure could endanger individuals and impair the trustworthiness of authorities. Even if information does not relate to particular individuals, its disclosure to private parties may be problematic if it would alert criminals to investigative strategies and thereby obstruct investigations. Whether public-to-private information sharing genuinely meets the pursued objectives will therefore depend to a significant degree on the ability of legislators and authorities to prevent such abuse.

III.2.2. Privacy and Data Protection

III.2.2.1. The Different Kinds of Public-Private Data Processing

III.2.2.1.1. The Need to Differentiate between Various Types of Public-To-Private Sharing

As a starting point to find out the extent to which the collaboration between the authorities and obliged entities requires a special legal basis, one must start by recalling that this collaboration can take various forms that legislators may need to treat differently. Without at this point going into details, broadly speaking three different and particularly intrusive types of collaboration can be emphasised which may be enabled by public-to-private information sharing:

- First, authorities may share information about particular individuals or entities (for example by identifying a suspect) or other search criteria and induce obliged entities to use this information in the continuous monitoring of business relationships and transactions, with the aim of detecting situations that are linked to these individuals or entities or to the other search criteria.
- Second, authorities may induce an obliged entity to analyse its existing customer data in order to produce new insights, and for this purpose may share information (for example details of a suspected crime) to guide the obliged entity's analysis.
- Third, authorities may share information about a particular customer and thereby induce the obliged entity to monitor the financial activities of this customer.

All three forms of public-private cooperation can also appear in combination with one another. And all three can primarily serve to support authorities (notably an ongoing investigation), or primarily serve obliged entities' CDD (and thus improve their ability to detect and prevent crime), or aim for both at the same time.

III.2.2.1.2. Continuous Monitoring of Business Relationships and Transactions to Detect Individuals or Entities, or Situations Meeting Other Search Criteria

Where authorities share information about particular individuals or particular entities, or other search criteria not relating to particular individuals or entities, in order for it to be used in an obliged entity's continuous monitoring of multiple hitherto nonsuspicious business relationships and transactions, the public-private cooperation will usually entail a monitoring of a vast number of business relationships and transactions – possibly of all customers and all transactions that are processed by this obliged entity. If the obliged entity comes across the individual or entity in question, or a situation that satisfies the other search criteria in question, it will usually be under an obligation to report back to the authorities.

III.2.2.1.3. Analysis of Obliged Entities' Data Based on Information Provided by Public Authorities

Public-private cooperation can also take the form of an authority prompting an obliged entity to analyse available transaction data and other customer data, and providing the obliged entity with information (for example details of a suspected crime or the hallmarks of a particular type of crime) in order to guide the obliged entity's analysis. The obliged entity is thus expected to base its analysis on a more or less extensive combination of its own data and data provided by the authority. Such analyses differ from traditional production orders or subpoenas in one particular respect, namely that they aim at producing new findings that would not have been accessible by simply asking the obliged entity to screen its data stocks through some keywords.

An analysis of this type can reach various levels of complexity. At the one end of the spectrum, it may be concerned with only one specific customer (for example a particular company) and seek to find out whether, on closer scrutiny, this customer is controlled by, or otherwise linked to, a hitherto hidden individual. At the other end of the spectrum, one can think of a case where the authorities provide a globally operating obliged entity with strategic information about the activities of a specific transnational criminal group, and ask this obliged entity to analyse its data stocks in order to identify past transactions whose characteristics indicate that they might be connected to the criminal group.

III.2.2.1.4. Monitoring of the Activities of Specific Individuals or Entities

Public-private cooperation can finally also take the form of authorities sharing information with an obliged entity concerning a particular individual or entity in order to initiate monitoring of this individual's or entity's future financial activities. Unlike the first type of public-private cooperation mentioned above, this third type of cooperation is targeted, since it is aimed at specific customers who have attracted the authorities' attention, whether due to a criminal suspicion or mere anomalies.

Again, the monitoring can reach various levels of complexity. At one end of the spectrum, public-private cooperation of this type may merely entail the monitoring of transactions in a single bank account. At the other end, the monitoring might extend to an entire network of individuals and companies and include the collection of data other than transaction data, such as data obtained from an analysis of the targeted customers' online activities in social networks in order to better understand these customers' financial activities.

III.2.2.2. The Requirement of a Legal Basis

III.2.2.2.1. Distinguishing Relevant Data Processing Operations

Even though the issue of data protection has become a prominent part of the EU legal order in recent years, currently neither EU law nor the ECtHR provides clear guidance on how to regulate the above forms of public-private collaboration. To ascertain the extent to which a legal basis is necessary when public-to-private information sharing is done in order to prompt data processing by private entities, and how such a basis should look, one must start by differentiating the data processing operations involved. Such a differentiation is key, because the applicable legal framework depends on it.

To begin with, one must note that collaboration between authorities and obliged entities in the context of AML/CFT will usually entail the processing of personal data. Such processing is governed by Regulation 2016/679 (the "GDPR"),[51] as regards obliged entities (and possibly FIUs),[52] and by Directive 2016/680, as regards authorities responsible for the prevention, detection and investigation of crime.[53]

Within a public-private cooperation, at least two data processing operations can be distinguished for the present purpose:

- a processing of data by a public authority, especially the transfer of data to one or more obliged entities;
- a processing of data by these one or more obliged entities, including not only the data received from the authority but other data (in particular, the entities' own customer data).

---

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[52] Recital 42 and Art. 43 of Directive (EU) 2015/849 and recital 38 of Directive 2018/843; as to uncertainties regarding the legal status of FIUs: E Kosta, "The proposed Anti Money Laundering Authority and the Future of FIU Collaboration in Europe" in: V Mitsilegas, M Bergström (eds.), *EU Law in the Digital Age*, Hart Publishing, 2024 (in press).

[53] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Further data processing operations are conceivable after this processing of data by an obliged entity. In particular,

- the entity may for instance transfer the findings from its data processing back to an authority, such as an FIU or investigative authority;
- and if this happens, that authority may then process those findings.

However, the following analysis will focus only on the first two processing operations, as these will largely determine the feasibility of the latter two.

The question of the applicable legal framework depends not only on who is processing the data – the authority or the obliged entity – but also on who actually controls this processing. The "controller" is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data", while a natural or legal person "which processes personal data *on behalf* of the controller" is merely a "processor".[54] In the present context, this distinction can become relevant in some instances, especially when a public authority exercises a degree of control over an obliged entity's data processing, and consequently the authority, and not the obliged entity, must be deemed to be the controller of the processing. This would be an exceptional case, but if it were to happen, the authority concerned would not only transfer data to an obliged entity, but would be understood to process itself the obliged entity's data, a scenario with potentially far-reaching repercussions not least for the proportionality of the processing. In any case, an authority is not considered to control a private entity's data processing merely because that entity is legally obliged to process information at the authority's request.[55]

Finally, for the purpose of the following analysis, it should be emphasised that public-to-private information sharing can also pertain to information that is not about particular individuals, but instead about a legal entity (for example if authorities disclose that a particular company is suspected of crime). Given that as a rule, information related to legal entities does not qualify as personal data, Regulation 2016/679 and Directive 2016/680 generally do not apply. However, this does not usually mean that this kind of public-private interaction is excluded from the requirement of a legal basis, because depending on the circumstances of the case, this interaction can still involve an interference with fundamental rights.

III.2.2.2.2. A Legal Basis for the Transfer of Information by the Public Authority

The need for a sufficiently specific legal basis

According to Article 52(1) of the Charter of Fundamental Rights, any limitation imposed by a public authority on the exercise of the rights and freedoms recognized by the Charter must be provided for by law. The first prerequisite that arises in respect of public-to-private sharing is thus the availability of a

[54] Art. 4(7) and (8) of Regulation 2016/679 (emphasis added).

[55] See Art. 6(1)(c) of Regulation 2016/679.

legal basis in EU or national law. That legal basis must conform to the requirements of EU data protection law, namely Directive 2016/680 and, insofar as it is deemed to cover FIUs, Regulation 2016/679. As regards authorities covered by Directive 2016/680 (especially criminal-justice and police authorities, and depending on their design in a particular Member State, FIUs), the legal basis must, in particular, define a particular purpose, or multiple purposes, of the processing.[56] Given the current silence of EU law on public-to-private information sharing, a transfer of personal data by competent authorities to obliged entities will be lawful only if national law includes a legal basis that meets these requirements, particularly a legal basis that envisages a particular form of subsequent processing of the data by the obliged entity. If the data processing by an FIU is deemed to be covered by Regulation 2016/679, a legal basis for public-to-private sharing might not require the same level of specificity (in light of Article 6(1) sentence 2, and provided that the obliged entity is not under an obligation to participate in the sharing),[57] though in that case the sharing must still be necessary for the performance of a task of the FIU. Yet at present, EU law essentially limits the FIU's tasks to "receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing" and "disseminating the results of its analyses and any additional relevant information to the competent authorities".[58] At the moment, therefore, the collaborative processing of personal data together with obliged entities, and a public-to-private transfer of personal data to this end, does not constitute a task of the FIU, unless national law provides otherwise.

The public-to-private sharing of non-personal data

Apart from that, even if a public-to-private information transfer does not involve personal data, it can still require a legal basis, namely insofar as the transfer itself still constitutes an interference with fundamental rights. Given the particular relevance in this context, legislators must ensure that when information about commercial entities is disclosed, the public-private cooperation respects the freedom to conduct a business according to Article 16 of the Charter of Fundamental Rights. As with other rights under the Charter, the Charter's Article 52(1) requires that any limitations on the exercise of this right must be provided for by law. This particularly concerns interference in a company's business secrets.[59] The same is true for measures that damage a company's reputation insofar as that damage constitutes an interference with Article 16 or with the right to protection of private life under Article 7 of the Charter.[60]

---

[56] Article 8 of Directive 2016/680.

[57] See Art. 6(3) sentence 2 of Regulation 2016/679.

[58] Art. 32(3) sentences 2 and 3 of Directive 2015/849.

[59] ECJ, *Varec SA*, 14 February 2008, C-450/06, para. 49; ECJ, *Interseroh*, 29 March 2012, C-1/11, para. 43.

[60] In this sense GC, *Evonik*, 28 January 2015, T-341/12, para. 125.

III.2.2.2.3. A Legal Basis for the Processing of Information by the Obliged Entities

Following from Article 2 in conjunction with Article 6 of Regulation 2016/679, any processing of personal data by obliged entities must have a legal basis. Four different justifications provided by the Regulation can generally be relevant in this context:

- the data subject (in particular any affected customer) has given consent to the processing of his or her personal data, according to Article 6(1)(a);
- the processing is necessary for compliance with a legal obligation of the obliged entity, according to Article 6(1)(c);
- the processing is necessary for the performance of a task carried out by the obliged entity in the public interest, according to Article 6(1)(e);
- or processing is necessary for the purposes of the legitimate interest pursued by the obliged entity, according to Article 6(1)(f).

Consent as an insufficient legal basis

Consent, however, is unlikely to be applicable here, because it will usually not meet the validity requirements of Regulation 2016/679. According to the Regulation's Article 7(4), consent must be freely given, and "utmost account" should be taken of whether "the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". Moreover, Recital 32 of the Regulation refers to a "clear affirmative act" which is "specific" to a processing operation. It is unlikely that a general consent given by obliged entities' customers in the contractual terms and conditions for financial services would meet these standards. Such consent would not be specific to a particular operation. Moreover, the acceptance of these terms and conditions is likely to be imposed as a condition for entering into a contract with the obliged entity. Considering how important it is to clients in particular to access financial services, a free decision in the sense of Article 7 would appear to be absent.

Processing in the pursuit of a "legitimate interest" usually inadequate

In the absence of any more specific legal basis in EU or national law, the pursuit of a legitimate interest according to Article 6(1)(f) of Regulation 2016/679 would offer the only ground for the obliged entity's data processing. However, while the prevention and detection of financial crime within the entity's sphere can constitute a legitimate interest capable of outweighing the rights and interests of a customer affected by the data processing, such a general legal basis will often not seem adequate as a ground for processing that is done in response to the transfer of personal data by a public authority.[61] This is particularly so when the shared data includes sensitive information about the

[61] WJ Maxwell, "The GDPR and private sector measures to detect criminal activity", *Revue des Affaires européennes/Law & European Affairs*, no. 1, 2021, p. 103–116.

possible involvement of customers in criminal activity. Under Article 6(1)(f), the questions whether, and to what extent, to process such sensitive information would be left to the discretion of the obliged entity. Leaving such leeway would appear contradictory, as it raises the question whether the sharing of personal data by the authorities was necessary in the first place. Furthermore, the obliged entity would be required to perform the balancing of rights and interests required by this part of the Article, thereby exposing customers whose sensitive data was shared to a significant risk of disproportionate interference with their rights.

Processing based on a legal obligation or in pursuit of the public interest

It therefore seems necessary to require more specific legal bases for obliged entities' processing of personal data in the context of public-to-private information sharing. Such a legal basis can be framed as a legal obligation of the obliged entity under Article 6(1)(c), or as a task carried out by the obliged entity under Article 6(1)(e). The latter case would be preferable if legislators would like to provide collaborating obliged entities with a margin of discretion as to how to process data that was provided by the authorities. In both cases, the basis for the processing must be laid down by Union law or Member State law. Moreover, in light of Article 6(3), the law should in particular contain specific provisions as regards the types of data which are subject to processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing.

Whether current AML/CFT law provides a legal basis

The question then arises whether in some instances, the current law of Member States may already provide a sufficient legal basis in this sense. Insofar as public-to-private sharing is meant to improve the ability of obliged entities to detect relevant risks, current CDD obligations under AML/CFT laws would generally already provide a legal basis for processing customer data together with data that was shared by the authorities. The processing limits to be respected by the obliged entity would then be the same as in any other case of CDD. If obliged entities are willing to voluntarily go beyond what is required from them under their CDD obligations, out of their own interest in effectively protecting themselves from financial crime, the lawfulness of their processing may be doubtful, as it would then need to rely on Article 6(1)(f) of Regulation 2016/679 ("legitimate interest" of the obliged entity), whose inadequacies have already been mentioned above. Insofar as the public-to-private sharing is primarily meant to lead to the gathering of information for the benefit of authorities, in the sense that obliged entities' CDD infrastructure is directly used as an instrument of the authorities, the purpose of the processing goes beyond CDD, meaning that it is not authorised by current AML/CFT law.

Processing of personal data as a result of public-to-private sharing of non-personal data

Finally, it should be noted that the transfer of non-personal data, such as information related to legal entities, will often prompt processing of personal data by the obliged entities, which in this case will require compliance with Regulation 2016/679. In many cases it would be rather useless, for AML/CFT purposes, to process information about a legal entity without at the same time also processing information about individuals who are or might be connected to that entity. If the authorities have identified a particular entity as being involved in crime or as posing a high risk, obliged entities will often need to screen the customer data not only for the name of that company, but also for other companies that the tainted company might use to hide its activities. To screen their customer data effectively, obliged entities will then at least need to scrutinise the beneficial owners that control the tainted company, and thus process these individuals' personal data. Thus even the public-to-private sharing of mere company names can lead to a substantially intrusive processing of personal data by obliged entities, not least because this processing may lead to the identification of individuals connected to tainted companies, and ultimately have a stigmatising effect on such individuals.

III.2.2.3. The Intrusiveness of Data Processing in the Context of Public-Private Information Sharing

According to Article 52(1) of the Charter, any interference with fundamental rights is subject to the principle of proportionality. In order to determine what is proportionate in the context of public-to-private information sharing, one should first of all assess the degree of intrusiveness of the instances of interference entailed by such sharing. Three different considerations are particularly relevant for this purpose: the sensitivity of the information shared by the authorities; the sensitivity of the data processed by the obliged entities as a result of the sharing; and the methods by which the data is processed.

III.2.2.3.1. The Sensitivity of the Data Transferred by Public Authorities

As regards the sensitivity of the information shared by authorities, one must recall that the domain of police and criminal-justice authorities in particular usually encompasses vast amounts of personal data of great relevance for the private and professional life of affected individuals. Investigative authorities are equipped with highly intrusive powers that enable them to gather information and that are justified only if the authorities handle their data stocks with care. As recognised by EU Directive 2016/680, this means in particular that competent authorities must use the information for purposes that are always appropriate in light of the information's sensitivity and of how it was obtained. The disclosure of personal data by authorities can also be highly sensitive in itself because of the risk of abuse it entails. If information is sensitive, that does not of course mean that it cannot be disclosed under any circumstances, but authorities will need to be careful to ensure that disclosure to the private sector

constitutes a proportionate interference with the rights of affected persons. Authorities also need to be alert to the fact that interference with rights can also result from sharing information that is not attributable to a particular person and is thus not personal data (for example when a typology highlights cultural roots of a particular criminal group), because such sharing can then still have a discriminatory impact on customers and notably infringe upon their fundamental right to non-discrimination.

Interference with the rights of individuals

The disclosure of information by the authorities to private entities can raise particular concerns if that information is capable of damaging the reputation of individuals. The case-law of the ECtHR found a violation of Article 8 ECHR where statements of an authority constituted an "attack on personal honour and reputation", provided they "attain a certain level of gravity and in a manner causing prejudice to personal enjoyment of the right to respect for private life".[62] If this is the case, the interference must rely on a legal basis, pursue a legitimate aim, and be necessary in a democratic society. While, as a rule, Article 8 ECHR does not preclude authorities from expressing a suspicion about a specific individual to a third party or to the wider public, it does require them to strike a fair balance between competing public and private interests.[63] For instance, the ECtHR found a violation of Article 8 ECHR in a judgment deciding a family law dispute, where a court stated its suspicion that a particular person had committed sexual abuse, even though the court had not subjected this issue to a thorough evidentiary assessment and its statement was not relevant for resolving the case at hand.[64] The ECtHR highlighted that the portrayal of the suspect in an authoritative judicial ruling was likely to have a particularly stigmatizing effect.[65] Similarly, a violation of Article 8 was found in a liability proceeding against a public administration, in which a court's judgment identified the author of a wrongdoing (namely of workplace harassment) who was not a party to the proceedings and had not been informed about the underlying complaint of a co-worker. The violation lay in that only the culprit's wrongdoing, but not his identity, was relevant for determining the administration's liability.[66] A violation of Article 8 was also found where the police decided to drop a case on procedural grounds but nevertheless indicated their belief that the suspect was in fact guilty of criminal assault, and then disclosed this decision to a third party.[67] Here the ECtHR emphasised that in striking a fair balance between competing interests, it is important for safeguards to be available against arbitrary decisions and abuse; the Court therefore attributed particular relevance to the lack of remedies through which

[62] ECtHR, *A. v. Norway*, 9 April 2009, no. 28070/06, para. 64.

[63] ECtHR, *Mikolajová v. Slovakia*, 18 January 2011, no. 4479/03, para. 59.

[64] ECtHR, *Sanchez Cardenas v. Norway*, 4 October 2007, no. 12148/03, para. 37.

[65] *Ibid*, para. 38.

[66] ECtHR, *Vicent Del Campo v. Spain*, 6 November 2018, no. 25527/13, para. 48–51.

[67] ECtHR, *Mikolajová v. Slovakia*, 18 January 2011, no. 4479/03, para. 60–61.

the suspect could have obtained a retraction or clarification of the police decision.[68]

Interference with the rights of legal entities

So far, the ECtHR has left open whether Article 8 ECHR also protects the reputation of legal entities.[69] In any case, if inaccurate allegations damage the commercial viability of a company and are not justified by Union laws or national laws, they might constitute a violation of Article 16 of the Charter of Fundamental Rights[70] by imposing an unjustified burden on conducting the business.[71] However, as regards the appraisal of the gravity of an interference with Article 16, it must be borne in mind that according to the ECJ, the freedom to conduct a business "must be viewed in relation to its social function", and therefore "may be subject to a broad range of interventions on the part of public authorities which may limit the exercise of economic activity in the public interest".[72] As a consequence, the level of protection may be more limited than the protection afforded to an individual's reputation, especially if allegations pertain to a company whose business practices are inevitably subject to greater public scrutiny.[73] At the same time, it must be borne in mind that depending on the particular circumstances, damaging allegations directed against a legal entity can also affect the reputation of the entity's representatives (for example its directors) and of other individuals connected to it, including its shareholders, and to that extent may constitute an interference with their rights under Article 8 ECHR.[74]

III.2.2.3.2. The Sensitivity of the Data Processed by Obliged Entities

III.2.2.3.2.1. Financial Privacy as an Unresolved Question of Data Protection Law

As to the sensitivity of data processed by obliged entities, one must focus primarily on financial data, particularly transaction data, and data gathered by obliged entities in the performance of their CDD obligations, such as

---

[68] ECtHR, *Mikolajová v. Slovakia*, 18 January 2011, no. 4479/03, para. 62; similarly, in the context of statements by a court, ECtHR, *Vicent Del Campo v. Spain*, 6 November 2018, no. 25527/13, para. 53; ECtHR, *S.W. v. the United Kingdom*, 22 June 2021, no. 87/18, para. 62–63.

[69] ECtHR, *Firma EDV für Sie, EfS Elektronische Datenverarbeitung v. Germany*, 2 September 2014, no. 32783/08, para. 23; ECtHR, *Margulev v. Russia*, 8 October 2019, no. 15449/09, para. 45. See however GC, *Evonik*, 28 January 2015, T-341/12, para. 125.

[70] See ECJ, *Puškár*, 27 September 2017, C-73/16, para. 114.

[71] See ECJ, *Scarlet Extended*, 24 November 2011, C-70/10, para. 46; ECJ, *Netlog*, 16 February 2012, C-360/10, para. 44; M Everson/R Correia Goncalves, in S Peers et al. (eds.). *The EU Charter of Fundamental Rights, A Commentary*, 2nd ed. 2021, Article 16, para. 16.44–45.

[72] ECJ (GC), *Sky Österreich*, 22 January 2013, C-283/11, para. 45–46.

[73] See ECtHR, *Steel and Morris v. the United Kingdom*, 15 February 2005, no. 68416/01, para. 94.

[74] See ECtHR, *OOO Memo v. Russia*, 15 March 2022, no. 2840/10, para. 47, and also ECtHR, *Frisk and Jensen v. Denmark*, 5 December 2015, no. 19657/12, para. 49; ECJ, *Puškár*, 27 September 2017, C-73/16, para. 114.

information about the purpose of a business relationship, about the origin of funds, and about the beneficial owner. This can also include information that obliged entities gathered in order to establish those aspects, such as information gathered about the control structure of a corporate client in order to identify the beneficial owner. So far, ECJ and ECtHR case-law has not yet specified to what extent the processing of such data should be treated as sensitive and whether, in view of the proportionality principle, it requires particular limitations and safeguards. However, these questions necessarily arise when assessing the proportionality of public-to-private information sharing. To determine the sensitivity of financial data, one can begin by considering existing case-law in the area of data protection, as it offers some indications. The criteria developed there will also be relevant in the present context.

III.2.2.3.2.2. Electronic Communications Metadata as a Comparative Yardstick

ECJ jurisprudence and national legal orders have set limits for what is arguably the most prominent example of the challenges resulting from an increasing involvement of the private sector in criminal policy: the retention of electronic communications metadata by electronic communications service providers and internet access providers for the purpose of the prevention or investigation of crime. Though the ECJ has specified exceptions allowing the retention of metadata, particularly in cases of a present and specific threat to national security,[75] and quick freezes of data of suspects, victims and related contact persons during an ongoing criminal investigation,[76] in general it has prohibited legislators from imposing a general and indiscriminate obligation on the relevant service providers to retain such data for purposes of the prevention and investigation of crime. This is significant in the present context because the ECJ's jurisprudence is based on the principle that in view of the content and scope of electronic communications metadata, unlimited retrospective access to such data would provide competent authorities with excessive surveillance powers that would constitute a disproportionate interference with the right to respect for private and family life according to Article 7 and the right to the protection of personal data according to Article 8 of the EU Charter of Fundamental Rights. In other words, in limiting the retention of electronic communications metadata, the ECJ and national legal orders have emphasised that in light of the massive volume of sensitive personal data routinely recorded by electronic communications and internet access providers, the involvement of the private sector in the prevention and investigation of crime must remain limited insofar as the resulting surveillance would be disproportionate.

III.2.2.3.2.3. Criteria for Determining the Sensitivity of Data

In *La Quadrature du Net*, following and expanding on a method used for the first time in *Digital Rights Ireland,* the ECJ applies one particular criterion to assess

[75] ECJ (GC), *Commissioner of An Garda Síochána et al*., 5 April 2022, C-140/20, para. 62.

[76] ECJ (GC), *SpaceNet et al*., 20 September 2022, C-793/19, para. 118–120.

the sensitivity of data. Most of the relevant recent decisions of the ECJ were related to electronic communications traffic and location data, in respect of which the Court explains their sensitivity by stating that these metadata:

> may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.[77]

Although this criterion was used for the first time in the very specific context of electronic communications metadata, it is not limited to that context. The ECJ notably applied this criterion to PNR data, where it further differentiated its approach, starting by acknowledging that "PNR data may, in some circumstances, reveal very specific information on the private life of a person", but then observing that "the nature of that information is limited to certain aspects of a person's private life", and therefore does not "allow for a full overview of the private life of a person".[78] This indicates that as a rule, the sensitivity of data must not be assessed in the abstract, but depends on the level of detail that the data in question can reveal about a person.

III.2.2.3.2.4. The Assessment of Financial Data

As regards limits on competent authorities' powers to involve private entities in the gathering of personal data, ECJ jurisprudence has so far not comprehensively addressed whether other categories of personal data beyond electronic communications metadata could potentially reach similar levels of sensitivity, and thus impose similar limitations on the retention and further processing of such data by businesses for the prevention, detection and investigation of crime. This question seems particularly relevant with regard to financial data collected by obliged entities as part of their AML/CFT obligations, notably transaction data and CDD information retained according to Article 40(1) of Directive 2015/849 for a period of five years after the end of the relevant business relationship.[79] It seems possible that the legal limitations developed for electronic communications metadata may also be applicable by

[77] ECJ (GC), *La Quadrature du Net*, 6 October 2020, Cases C-511/18, C-512/18 and C-520/18, para. 117.

[78] ECJ (GC), *Ligue des droits humains*, 21 June 2022, C-817/19, para. 120.

[79] Directive (EU) 2015/849, as amended by Directive (EU) 2018/843 of 30 May 2018.

analogy to financial data, at least to some extent, in view of the importance of electronic transactions, which have nowadays largely replaced cash transactions and frequently reveal almost all the goods and services purchased by an individual and even the location of the purchase, thus often allowing for very detailed and comprehensive insights into the private and even intimate life. Yet so far, this question is barely considered by EU law.[80] In light of the strong role of financial services providers based in the United States and the resulting importance of transatlantic data flows for EU-based service providers, further challenges in this regard could result from recent developments in US law,[81] where the Supreme Court decided to categorically distinguish financial data from electronic communications metadata.[82]

The 2022 ECJ decision on public access to beneficial ownership information could indicate a growing willingness of the Court to scrutinise the processing of financial data. Though the decision was primarily concerned with public accessibility of the data, it also highlights that financial data can potentially make it possible to draw up wide-ranging personal profiles. In the words of the Court:

> As regards the seriousness of that interference, it is important to note that, in so far as the information made available to the general public relates to the identity of the beneficial owner as well as to the nature and extent of the beneficial interest held in corporate or other legal entities, that information is capable of enabling a profile to be drawn up concerning certain personal identifying data more or less extensive in nature depending on the configuration of national law, the state of the person's wealth and the economic sectors, countries and specific undertakings in which he or she has invested.[83]

Given that beneficial ownership information does not include transaction data, and therefore must be deemed considerably less sensitive than the amalgam of transaction data and other information processed for purposes of CDD (including, regularly, information obtained from data brokers and possibly even geolocalisation data collected on the occasion of the use of online payment services), one should expect that in the future, EU law will subject obliged entities' data processing, and even more so the use of such data by authorities, to greater scrutiny than is currently the case. However, though the AML/CFT framework requires the long-term retention of extensive amounts of largely

[80] See B Vogel/JB Maillart, National and International Anti-Money Laundering Law, p. 897–904; C Kaiser, Privacy and Identity Issues in Financial Transactions, University of Groningen, 2018, p. 491–527.

[81] This discussion is nothing new in the US; see already: The Privacy Protection Study Commission, *Personal privacy in an information society*, Washington, DC, 1977.

[82] Carpenter v. United States (2018) 585 U.S. (2018); M Gentithes, "The end of Miller's time: how sensitivity can categorize third-party data after Carpenter", *Georgia Law Review*, nº 3, vol. 53, 2019, p. 1039–1091.

[83] ECJ (GC), *WM*, *Sovim SA v Luxembourg Business Registers*, C-37/20 and C-601/20, para. 41.

sensitive data – namely, transaction and CDD data – irrespective of whether such data pertains to suspicious customers, it must also be pointed out that this retention is, in many ways, different from the retention of communications metadata that has been sharply limited by the ECJ. After all, the retention and processing of financial data by obliged entities serves not only the authorities but also obliged entities, who through this retention and processing enjoy benefits to their private commercial interests and their interest in protecting themselves from being harmed by criminals. The ECJ's limits on the retention of communications metadata can therefore not be directly applied to financial data. Yet insofar as the retained financial data is processed at the initiative of authorities, the ECJ's concerns about extensive and possibly excessive surveillance become very relevant.

III.2.2.3.3. The Intrusiveness of the Processing Operations

As already explained above, the public-to-private transfer of information can prompt various forms of data processing by obliged entities (namely the monitoring of bulk data, the targeted monitoring of individual customers, and the analysis of existing data stocks), and each of these forms requires attention when assessing the degree of intrusiveness of data processing conducted in the context of public-to-private information sharing. While ECJ and ECtHR case-law on such forms of processing of private sector data has so far primarily focused on communications data, and has not yet focused on the performance of such processing operations by the private sector entities themselves, one can nevertheless identify criteria that are likely to be relevant for the processing of financial data as well.

Targeted surveillance

According to the case-law, secret surveillance targeting particular individuals constitutes a particularly intrusive interference with Article 8 ECHR. While the relevant jurisprudence had originally been developed by the ECtHR with regard to the interception of the content of telecommunications, subsequent ECJ jurisprudence found that a comparable or even higher degree of intrusiveness can arise in monitoring a person's electronic communications metadata. In this respect, the ECJ stressed the particular intrusiveness of "real-time access by the competent authorities to such data", because "it allows for monitoring of those users that is virtually total".[84] The targeted monitoring of the financial activities of a customer is unlikely to enable a similarly detailed view into the target's private life, and even if done at the initiative of an authority, will therefore usually not attain the same level of intrusiveness as in the case of communications metadata. Yet such monitoring can nevertheless be very far-reaching and – in light of the wealth of financial data produced in a largely digitalised economy – may yield insights into a person's private life that are similar to those gleaned through the traditional interception of

[84] ECJ, *La Quadrature du Net*, 6 October 2020, Cases C 511/18, C 512/18 and C 520/18, para. 187. See also ECtHR, *Ben Faiza v. France*, 8 February 2018, no. 31446/12, para. 74.

telecommunications. Even where this is not the case, the insights into persons' private life that can be obtained through a targeted monitoring of financial activities can certainly approach or even go beyond the intrusiveness of other forms of secret surveillance (such as the use of tracking devices[85] or the secret collection of data about a person's movements by train or air[86]) for which the ECtHR requires particular, although less demanding, legal safeguards.

Bulk interception

Recent years have seen growing case-law on bulk interception, meaning the application of specific filtering parameters (usually called selectors) to large quantities of data of unsuspected persons, with the aim of identifying individuals who might be involved in criminal activity or who constitute a threat. Bulk interception typically constitutes a particular form of secret surveillance, because once a person has been identified as a "match", her data will usually be examined by an analyst who will decide whether to refer the case to law enforcement or other security authorities.[87] The ECtHR has highlighted the intrusiveness of bulk interception with regard to the interception of communications metadata, holding that such practices are not necessarily less intrusive than the interception of communication content.[88] Moving beyond communications data, in its case-law on PNR data the ECJ recognised a "serious interference" with Articles 7 and 8 of the Charter of Fundamental Rights in the introduction of "a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services".[89] In this context, the ECJ also highlighted "the margin of error inherent in the automated processing", especially insofar as this leads to a substantial number of false positives, and stressed the importance of limiting such errors so as to ensure that the data processing is strictly necessary and not discriminatory.[90] In light of these standards, and insofar as the automated monitoring of obliged entities' customer data can extend to millions of financial transactions and to thousands or even millions of unsuspected customers, it seems likely that, depending not least on the screening criteria used for the automated processing, the monitoring of financial bulk data can equally constitute a serious interference.

[85] ECtHR, *Uzun v. Germany*, 2 September 2010, no. 35623/05, para. 52.

[86] ECtHR, *Shimovolos v. Russia*, 21 June 2011, no. 30194/09, para. 66.

[87] See ECHR (GC), *Big Brother Watch and others v. The United Kin*gdom, 25 May 2021, no. 58170/13, 62322/14 and 24960/15, para. 325.

[88] ECtHR (Grand Chamber), *Big Brother Watch and others v. The United Kingdom*, 25 May 2021, no. 58170/13, 62322/14 and 24960/15, para. 363.

[89] ECJ (GC), *La ligue des droits humains*, 21 June 2022, C-817/19, para. 111.

[90] ECJ (GC), *La ligue des droits humains*, 21 June 2022, C-817/19, para. 201.

Applicability of surveillance case-law to data processing by obliged entities

In the present context, the existing case-law on state surveillance appears relevant not least in view of the fact that when obliged entities receive information from the authorities, they are usually under an obligation to conduct CDD and to report suspicious activities to the FIU. Because the public-to-private information sharing concerned is inseparably linked to these obligations, the entities' data processing can appear to be a delegation of surveillance functions. A targeted monitoring of particular customers by obliged entities, as well as the continuous monitoring of large numbers of transactions and business relationships, may therefore constitute or at least closely resemble targeted secret surveillance and bulk interception within the meaning of the ECtHR and ECJ case-law. Though the monitoring is then carried out by obliged entities, and therefore the authorities themselves are not directly processing vast amounts of customer data, this functional distinction is not necessarily very relevant for assessing the intrusiveness of the surveillance. The more obliged entities' monitoring of customer relationships and transactions is prompted by a public-to-private information sharing, the more one must conclude that this monitoring constitutes an act of state surveillance whose execution is merely delegated to the private sector.[91]

Access to bulk data

As is evident from its case-law on electronic communications metadata, the ECJ has acknowledged that access to personal data can in itself be highly intrusive, especially if the data provides detailed insights into a person's private life.[92] The extent to which these limitations may also be applicable to financial data does of course depend on the question of the comparability of communications and financial data, as addressed above. In light of the rationale of the ECJ case-law, where limitations on the access to financial bulk data are required, such limitations would apply not only to the transfer of such data to the authorities, but also to instances where the data does not leave the obliged entity, but is essentially processed by that entity for the benefit of authorities.[93] Even if sensitive data is analysed by a private party on behalf of the authorities, and only the outcome of the analysis provided to the authorities, the fact remains that the authorities might thereby obtain the detailed insights into persons' private life that the case-law intends to limit.[94]

[91] To this effect ECJ, *La Quadrature du Net*, 6 October 2020, Cases C 511/18, C 512/18 and C 520/18, para. 172–182.

[92] See in particular ECJ, *Prokuratuur*, 2 March 2021, C-746/18, para. 36–40.

[93] See ECJ, *La Quadrature du Net*, 6 October 2020, Cases C-511/18, C-512/18 and C-520/18, para. 177.

[94] To this effect ECJ, *La Quadrature du Net*, 6 October 2020, Cases C-511/18, C 512/18 and C-520/18, para. 172.

III.2.2.4. Conclusions for Designing Legal Bases for Public-To-Private Sharing

As results from the preceding observations, public-to-private information sharing can lead to very intrusive forms of data processing, even if the sharing is merely meant to inform obliged entities that specific business relationships, or specific red flags, entail a particular financial crime risk. Because of the design of the AML/CFT framework, notably CDD and reporting obligations and the resulting processing infrastructure implemented by obliged entities, information sharing cannot be assessed apart from the consequences it can bring about. This regards in particular the possibility that information sharing may unduly prejudice blameless individuals and entities and lead to disproportionate surveillance. Such consequences are not inevitable, however, not least because the law can define limits on exactly how the shared information is to be used by receiving obliged entities.

When developing public-to-private information sharing in AML/CFT, legislators must therefore define substantive standards to ensure that the resulting processing of data is proportionate, and must put in place safeguards that ensure respect for these standards. In doing so they must take into account the procedural requirements set forth by Regulation 2016/679 and Directive 2016/680 as well as by ECJ and ECtHR case-law. Three aspects should receive particular attention:

- First, the law must ensure that any stigmatising effect of public-to-private sharing is limited to what is strictly necessary and proportionate to the seriousness of the financial crime risk in question. This will also require safeguards to ensure a high level of accuracy of the relevant information and limitations on who may use the information, and for what purposes.
- Second, insofar as obliged entities are expected to use the shared information in their customer and transaction screening, and thus also within automated data processing, limitations on the reach of such processing and safeguards to avert automation errors will be essential, as will guarantees for the accuracy of the information.
- Third, insofar as public-to-private sharing is meant to prompt a targeted monitoring or extensive analysis of a particular business relationship, special regard must be given to whether, in view of the scope and content of the processed customer data, such processing leads to detailed insights into a person's private life that are proportionate in view of the crime risk concerned.

Finally, legislators will have to consider that the processing of legal entities' data will usually be considered less intrusive than the processing of personal data and that, insofar as the public-to-private sharing is limited to such data, the legal requirements for that sharing may be less demanding from a proportionality point of view. Even so, it must also be borne in mind that a public-to-private sharing of information pertaining exclusively to a legal entity (as opposed to a natural person) will nevertheless often lead to a processing of personal data by obliged entities. Where this happens, public-to-private sharing

of non-personal data is not necessarily less intrusive than the sharing of personal data, especially if it exposes representatives of a company to stigmatisation. Besides, insofar as information sharing is likely to bring about serious interference with a company's rights, for example by effectively leading to its being cut off from financial services, or at least to a risk of such a cut-off, adequate substantive and procedural safeguards will likewise be indispensable.

III.2.3. Regulating De-Risking to Address Unintended Consequences of Public-Private Sharing

III.2.3.1. The Absence of a Legal Consideration Given to De-Risking and Discriminatory CDD

Public-to-private information sharing is likely, and partially even intended, to lead to the adoption of measures to the detriment of obliged entities' customers. Such measures include de-risking, i.e. the discontinuation of business relationships deemed to pose a crime risk,[95] as well as related measures, for example raising the price that such customers are asked to pay. Obviously, when investigative authorities or the FIU disclose to an obliged entity that a particular customer has attracted their attention, that obliged entity will usually become sceptical and reassess the customer's commercial value, with particular regard to the resources the entity would need to expend on additional CDD measures,[96] as well as reputational concerns.[97] This seems problematic, especially if the customer is only of interest to the authorities but not suspected of a crime, or if a criminal suspicion is based on weak factual grounds.

Besides, public-to-private information sharing can cause de-risking and other detrimental measures even with regard to customers who were not singled out by the authorities. On the one hand, a reassessment of a customer, and the resulting de-risking, will frequently extend beyond individuals and entities that are targeted by the authorities, and affect related persons as well, such as family members of the target. On the other hand, some obliged entities might already give unfavourable treatment to customers that merely share some personal traits of targeted customers, such as their origin. Even if the authorities were to share only strategic information and did not single out customers, some obliged entities might adopt a cautious approach to entire

[95] See European Banking Authority, Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The ML/TF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849 of 31 March 2023, EBA/GL/2023/03, p. 3.

[96] See ECJ, *Safe Interenvíos SA*, 10 March 2016, C-235/14, para. 99.

[97] D Artingstall/N Dove/J Howell/M Levi, *Drivers & Impacts of Derisking, A study of representative views and data in the UK*, by John Howell & Co. Ltd. for the Financial Conduct Authority, 2016; M Brei/L Cato/R DeLisle Worrell, "Credibility, Reputation and De-Risking in Global Banking: Evidence from a Theoretical Model", 11 *Journal of Globalization and Development* (2020).

groups of customers, for example if the latter are linked to a region that a typology paper singled out as being a crime hotspot.

Currently, EU law barely addresses de-risking as a consequence of obliged entities' AML/CFT obligations. The issue is treated as a matter of obliged entities' contractual autonomy, despite the fact that it is the law itself which effectively produces strong incentives for de-risking, through CDD obligations that are often resource-intensive. Even insofar as individuals in the EU have a right to a basic payment account under Directive 2014/92/EU,[98] the relationship between this right and money laundering or terrorism financing risks is not conclusively settled.

Similarly, EU law so far provides little clarity on limitations to discriminatory de-risking,[99] though a report by the European Banking Authority has indicated major concerns about de-risking and the resulting threats to the financial inclusion of some groups of customers (particularly asylum seekers from high-risk jurisdictions, as well as not-for-profit organisations).[100] Recital 66 of the preamble of Directive (EU) 2015/849 provides that CDD must not be performed in a discriminatory manner. Yet this principle has been addressed sparsely by EU courts.[101] While an opinion of the Advocate General stated that "[w]here no risk of money laundering or terrorist financing exists, no preventive action can be taken on those grounds",[102] the ECJ so far has not extended this position to obliged entities' implementation of CDD obligations, reflecting the difficulty of reconciling such limitations with obliged entities' contractual freedom.

III.2.3.2. The Need to Address Unintended Consequences of Public-To-Private Information Sharing

While it is already unsatisfactory that EU law currently gives little consideration to AML/CFT-induced de-risking and discriminatory CDD, this lacuna becomes even more problematic when these phenomena are influenced by public-to-private information sharing and are thus at least partially caused by authorities. This refers to both the excessive use by obliged entities of information provided by the authorities, and a discriminatory CDD practice prompted by such information.

---

[98] Art. 16 para. 4 and 7 of Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

[99] Concerns to this effect also in Opinion of the European Data Protection Supervisor (EDPS) on a proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing of 4 July 2013.

[100] European Banking Authority, Opinion of the European Banking Authority on 'de-risking' of 5 January 2022, EBA/Op/2022/01.

[101] ECJ, *Jyske Finans*, 6 April 2017, C-668/15, applying Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

[102] ECJ, opinion of Advocate General Wahl, delivered on 1 December 2016 in case C-668/15, para. 82.

As regards an excessive use of information that was provided by the authorities, any regulation of public-to-private information sharing must bear in mind that such sharing will often be likely to prompt de-risking or other adverse measures to the detriment of those customers, both individuals and entities, that the authorities have implicitly or explicitly singled out as constituting a financial crime risk. Such consequences will have an impact on the proportionality of the information sharing, especially if they affect customers that are in fact not linked to financial crime. To counterbalance any unintended effects, legislation might impose strict limits on how obliged entities make use of the information they receive from authorities. Such limits might in particular include conditions regarding the circumstances under which an obliged entity is allowed to take adverse measures against a customer who was subject to a public-to-private information sharing, and against related customers. At the same time, such limitations would also need to address any burden that they may impose on obliged entities, in particular as regards restrictions of their freedom of contract. In this respect, legislators must have due regard to the fact that the freedom to conduct a business under Article 16 of the Charter of Fundamental Rights covers "in particular, the freedom to choose with whom to do business and the freedom to determine the price of a service".[103] In weighing this freedom against the public interest in enabling public-private information sharing and against the rights of affected customers, legislators can find inspiration in recent legislative developments, not least in the area of digital services, where increasing attention is being devoted to the need to balance conflicting fundamental rights between private businesses and their clients.[104]

As regards discriminatory CDD practices that could be prompted by public-to-private information sharing, as a starting point legislators must consider Article 21 of the Charter of Fundamental Rights, which prohibits direct or indirect discrimination by Member States when implementing the EU AML/CFT legislative framework.[105] The prohibition of indirect discrimination is particularly relevant in this regard, because discrimination in this sense occurs where an apparently neutral provision, criterion or practice would put persons at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary. As a result, even the sharing of mere strategic information can be discriminatory, namely if the sharing has the effect of singling out particular persons and this effect is not proportionate to the aims pursued. Such concerns can arise not least if the shared strategic information goes beyond describing methods of financial crime and also includes information about the background of unspecified

[103] ECJ (GC), *Bank Melli Iran/Telekom Deutschland GmbH*, 21 December 2021, C-124/20, para. 79; see also ECJ (GC), *Sky Österreich*, 22 January 2013, C-283/11, para. 43; ECJ, *Lidl*, 30 June 2016, C-134/15, para. 28.

[104] See Art. 17, 20, 23 and 54 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

[105] ECJ, *SIA Rodl & Partner*, 17 November 2022, C-562/20, para. 50.

perpetrators. Insofar as authorities nevertheless consider it desirable to share such information with obliged entities, limitations on de-risking can again serve as a counterweight to address such concerns. This could notably include minimum standards for CDD and de-risking with regard to customers that are seemingly affected by the information sharing. Building on recent ECJ case-law, with regard to such customers the legislator might require an obliged entity to provide reasons for de-risking in order to show that the de-risking was not the result of a discriminatory use of information supplied by the authorities,[106] provided that the resulting limitation of the obliged entity's contractual freedom constitutes a proportionate interference with its right under Article 16 of the Charter of Fundamental Rights.

III.3. Regulating the Different Stages of Public-Private Interaction

As explained above, neither Regulation 2016/679 nor Directive 2016/680 nor Directive 2015/849 provides clear guidance on public-to-private information sharing. Likewise, ECJ case-law provides only limited clarity in the context of AML/CFT, given that so far, it relates mostly to communications data. European or national legislation should therefore develop a special legal framework for such information sharing, specifying the nature and scope of the data that may be shared by authorities, the scope of the subsequent data processing by obliged entities, and the procedural safeguards and remedies to ensure compliance with these substantive limits. The following provides an overview of key aspects that legislators will need to consider in order to satisfy requirements under the ECHR and EU primary law.

III.3.1. The Transfer of Information from Public Authorities to Private Entities

III.3.1.1. The Conditions for Public-To-Private Information Sharing

In order for public authorities to be allowed to share information with obliged entities, respect for the fundamental rights of all private parties involved is pivotal. As a result, legislators – as well as authorities when exercising their powers – must ensure that information sharing pursues a legitimate aim, and is necessary and proportionate *stricto sensu*. Furthermore, the law needs to provide procedural safeguards so that those substantive requirements are actually complied with.

III.3.1.1.1. Legitimate Aim and Appropriateness

According to Article 52(1) of the Charter of Fundamental Rights, limitations on rights and freedoms must "genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." As regards the processing of personal data, Article 5(1)(b) of Regulation 2016/679 and Article 4(1)(b) of Directive 2016/680 specify that personal data must be "collected for specified, explicit and legitimate purposes

[106] See, by analogy, ECJ (GC), *Bank Melli Iran/Telekom Deutschland GmbH*, 21 December 2021, C-124/20, para. 67–68.

and not further processed in a manner that is incompatible with those purposes". In other words, any public-to-private transfer of personal data must pursue a clearly-defined, legitimate aim. Consequently, the law must define how, and for what purpose, receiving obliged entities are expected to use the transferred data. The transfer and expected use of the data must genuinely meet this purpose, meaning that the obliged entities' expected use of the data must in fact be suitable to further the pursued public interest.

III.3.1.1.2. Necessity

Article 52(1) of the Charter of Fundamental Rights furthermore requires that any interference in such rights resulting from public-to-private information sharing must be necessary. This means that "where there is a choice between several measures appropriate to meeting the legitimate objectives pursued, recourse must be had to the least onerous."[107] The necessity requirement therefore "implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal."[108]

Necessity of the scope of the transfer

A disclosure of information by public authorities to obliged entities can be narrow or broad in scope. Depending on the particular purpose of the transfer, it may be necessary to provide relevant information to only one obliged entity, or even only to selected individuals within the obliged entity, or instead to numerous obliged entities. As any reputational damage as well as the impact of de-risking and similar adverse measures will increase with the amount of prejudicial information disseminated, the scope of the information sharing – both as regards the number of addressees and the level of detail of the information – must always be necessary for achieving the pursued objective.

Necessity of the envisaged data processing by receiving obliged entities

As explained above, given the extensive scope of transaction data and CDD data retained by obliged entities, the processing of this data may constitute a serious interference with their customers' rights, particularly Articles 7 and 8 of the Charter of Fundamental Rights. This is especially so where, on the basis of the information shared by the authorities, the obliged entity would be expected to screen its data stocks to identify persons who are not yet suspected of involvement in criminal activity at this point. Furthermore, even if the processing of customer data were intended only to produce information about a particular suspect, the volume of financial data retained by obliged entities about their customers means that such processing could potentially be excessive if it were to extend to large amounts of customer data that were retained long before the targeted customer became a suspect.

---

[107] ECJ, *WM and Sovim SA*, 22 November 2022, C-37/20 and C-601/20, para. 64.

[108] European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Brussels, 2017, p. 5.

Objective criteria for targeting specific individuals

By analogy with the standards applied by the ECJ in the context of communications metadata as well as with regard to PNR data, as a rule the processing of customers' personal data due to public-to-private information sharing should aim to produce information only about customers who, at the moment of the information sharing, are "suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime."[109] In situations where "vital national security, defence or public security interests are threatened by terrorist activities", the public-to-private information sharing may also aim at other persons' data, namely when "there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities".[110]

Limits on the screening of personal data of unsuspected customers

Insofar as authorities provide information in order to protect obliged entities from criminal activity and improve their ability to detect such activities, those entities will usually have to use the received information within their CDD. In fact, such use will regularly be the whole point of initiating public-to-private information sharing. More specifically, this means that the obliged entities will use the shared information as part of their ongoing – in large part automated – monitoring of business relationships and of the transactions undertaken throughout the course of those relationships,[111] and as part of their enhanced monitoring of higher-risk business relationships,[112] in order to manage and mitigate risk adequately and detect suspicious transactions or activities. However, as the extent of the data processing thus undertaken by obliged entities partially determines the intrusiveness of the data sharing, the use of the shared information must be strictly necessary. This may for example require entities to screen transactions of only some customers, not all of them, or only transactions related to specific business types. Furthermore, given that obliged entities retain vast amounts of transaction and CDD data that can reach back many years, if the processing of such data is prompted by public-to-private information sharing, it should comply with the limits developed by the ECJ with regard to the retention of personal data of unsuspected individuals. To keep the processing of customer data from going beyond these limits, any processing of data that was retained before the moment of the public-to-private data sharing must remain limited to what is strictly necessary. In particular, insofar as the public-to-private sharing is meant to help the obliged entity in detecting relevant risks, it will usually not be necessary to screen data pertaining to past transactions.

---

[109] See ECJ (GC), *Tele2*, 21 December 2016, C-203/15 and C-698/15, para. 119; ECJ (GC), *La Ligue des droits humains*, 21 June 2022, C-817/19, para. 219.

[110] See ECJ (GC), *Tele2*, 21 December 2016, C-203/15 and C-698/15, para. 119; ECJ (GC), *La Ligue des droits humains*, 21 June 2022, C-817/19, para. 219.

[111] See Art. 13(1)(d) of Directive (EU) 2015/849.

[112] See in particular Art. 18(2) of Directive (EU) 2015/849.

Limits on the gathering of additional data

Additionally, the intrusiveness of the data processing expected from obliged entities following a public-to-private information sharing, and consequently the necessity of such sharing, will be determined not only by how the shared information is used, but equally by the extent of further data gathering that the obliged entity may sometimes be expected to undertake in connection with the sharing. For example, if the shared information is meant to prompt additional CDD measures in order to clear up a particular high-risk business relationship, these CDD measures, having been instigated by an authority, must be necessary. This regards not least the scope of personal data that the obliged entity is expected to gather from the given customer or from third parties in order to ascertain relevant facts, such as the identity of a beneficial owner, the origin of funds, or the purpose of a transaction.

Limits on the processing of data about past transactions and CDD data collected in the past

Similarly, where authorities ask an obliged entity to process data about past transactions and CDD data that the obliged entity collected in the past, the scope of data included in such processing must be necessary. This regards in particular the question of the extent to which such processing will include data of customers whom the authorities have no reason to assume are connected with criminal activity. In any case, it is unlikely that a comprehensive processing of the data of all of an obliged entity's customers would ever satisfy the necessity requirement. Instead, if an obliged entity is also expected to process personal data of customers who are not suspected of criminal involvement, the authorities will need to specify the exact extent to which such processing is necessary for preventing, detecting or investigating serious crime.

Time limits on surveillance

As a further consequence of the necessity requirement, in cases where obliged entities are asked to monitor a particular customer or to use the name of particular individuals or entities in their screening of future transactions, the law must also specify time limits for such processing,[113] given that such monitoring or screening usually constitutes a continuing interference in the rights of the targeted individuals and entities.

The quality of predetermined criteria for obliged entities' automated data processing

If the authorities expect transactions and business relationships to be screened or analysed by automated means, ECJ case-law requires the criteria they provide to this end to be reliable and up to date, and not to be discriminatory.[114]

---

[113] See ECtHR, *Shimovolos v. Russia*, 21 June 2011, 30194/09, para. 68.

[114] In the context of automated processing of traffic and location data: ECJ, *La Quadrature du Net*, 6 October 2020, Cases C-511/18, C-512/18 and C-520/18, para. 182.

Specific personal characteristics should not be used, such as a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. Those criteria that are to be used in the automated screening of customer data must be "worded in a neutral fashion", so that "their application does not place persons having the protected characteristics at a particular disadvantage."[115]

III.3.1.1.3. Proportionality Stricto Sensu

Finally, any interference with fundamental rights must also be proportionate *stricto sensu.* As the ECJ explained in the context of the processing of personal data:

> an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue, in order to ensure that the disadvantages caused by that measure are not disproportionate to the aims pursued. Thus, the question whether a limitation on the rights guaranteed in Articles 7 and 8 of the Charter may be justified must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness.[116]

This balancing of rights and interests is required with regard to interference in the rights both of obliged entities' customers and, where applicable, also of obliged entities themselves. More specifically, one can identify a number of constellations where proportionality *stricto sensu* demands particular attention.

III.3.1.1.3.1. Proportionality of Interference in Customers' Rights

As explained above, the public-to-private transfer of information can impact the rights of obliged entities' customers, particularly the right to private life under Article 7 and the freedom to conduct a business under Article 16 of the Charter of Fundamental Rights. The proportionality of any interference with these rights will essentially depend on several overarching factors – not only the importance of the pursued objective and the expected effectiveness of the measure in this regard, but also the intrusiveness of the data processing induced by the measure and the gravity of the measure's unintended consequences. The design of public-to-private information sharing needs to reflect a proper balance between these factors in such a way that the expected advantages of the measure are not outweighed by its drawbacks.

[115] ECJ, *La Ligue des droits humains*, 21 June 2022, C817/19, para. 197.

[116] ECJ, *WM and Sovim SA,* 22 November 2022, C 37/20 and C 601/20, para. 64.

The gravity of adverse measures adopted by obliged entities

Public-to-private information sharing will regularly provide more or less clear indications that particular customers, or entire groups of customers, entail an enhanced risk of financial crime, or even that the authorities believe specific customers are involved in criminal activity. Obliged entities will then be likely to cut off their relationship with such customers, abstain from transactions with them, or adopt other adverse measures, for example raising the price of services in order to compensate for higher compliance costs. Especially when stigmatising information has been disclosed to numerous obliged entities, individuals' as well as legal entities' ability to use financial services can be significantly impaired. In extreme cases, affected individuals may experience financial exclusion, possibly leading to far-reaching interference with their ability to conduct their private life, and affected legal entities may effectively be put out of business. Both the numbers of customers affected by a public-to-private sharing and the impact of adverse measures on them are therefore key for assessing proportionality. Limiting such effects as far as possible, in particular by ensuring that shared information is not used for unintended purposes, will thus usually be a crucial counterbalancing factor.

The intrusiveness of the intended data processing performed by obliged entities

Where public-to-private information sharing is meant to improve obliged entities' ability to detect and prevent financial crime, the shared information will usually be used within CDD to identify risks and trigger additional CDD measures. If this is the only intended use, the degree of intrusiveness of the processing would be limited and usually require more limited safeguards. However, the law must then ensure that the information sharing does not, in actual fact, transform into a much more intrusive form of processing for which the existing safeguards are not adequate.

There are three situations in particular where information sharing could significantly increase the intrusiveness of obliged entities' data processing beyond what would usually be expected from CDD, and would therefore require more safeguards than current AML/CFT legislation provides:

- first, if the public-to-private information sharing would effectively lead to a real-time targeted monitoring of particular customers for the benefit of the authorities;
- second, if such sharing would allow the authorities to effectively steer a bulk monitoring of the financial activities of a large number of unsuspected customers;
- third, if the information sharing is intended to have an obliged entity analyse a particular customer's financial transaction history for the authorities' benefit, thereby exploiting the data retention obligations to which obliged entities are subject under Article 40(1) of Directive 2015/849.

In all cases, legislators and authorities will need to consider the degree of interference caused by the intended data processing in order to assess whether it is still proportionate in light of the particular threat or suspicion at hand. Three considerations should receive particular attention when determining the degree of intrusiveness:

- the actual sensitivity of the data processed for the benefit of the authorities, which is determined notably by the nature of the data and by the number of individuals that may be implicated by the processing;
- the aim of the processing, especially to what extent the processing of data for the authorities is meant to produce sensitive information about a person's private life;
- finally, where the intended processing is meant to be automated, the risks of discriminatory bias or error that the processing technology may entail.[117]

In addition, one should also note the possible interrelation between the gravity of adverse measures adopted by obliged entities against customers and the extent of the intended processing of the shared information by those obliged entities, for the extent of the processing will usually impact on the scale of the entities' measures and accordingly affect proportionality. For if obliged entities are expected to use the shared information within their CDD for screening business relationships and transactions, public-to-private information sharing can potentially expose vast numbers of inconspicuous customers to the risk of reputational damage and de-risking.

III.3.1.1.3.2. Proportionality of Interference in Obliged Entities' Rights

Though public-to-private information sharing offers benefits to obliged entities, it can also lead to interference with their rights, not least their freedom to conduct a business.[118] If participation in an information-sharing mechanism is voluntary, the information that the sharing provides can trigger enhanced CDD obligations under existing AML/CFT laws. Additional interference with obliged entities' rights arises if the law would oblige them to receive and process information from the authorities and, at the same time, to respect particular requirements on how to process the information. The rights of an obliged entity can be particularly affected if the law, in the context of information sharing, would require an obliged entity to temporarily refrain from de-risking or other adverse measures vis-à-vis a customer. Insofar as such interference in obliged entities' rights arises, the interference must then equally be proportionate.[119]

---

[117] For a proportionality assessment in this sense: German Constitutional Court, judgment of the First Senate of 16 February 2023, 1 BvR 1547/19, 1 BvR 2634/20, paras. 76–77 and 90.

[118] See ECJ (GC), *Telekabel Wien,* 22 January 2013, C-283/11, para. 43; ECJ, *Scarlet Extended*, 24 November 2011, C-70/10, para. 46.

[119] See ECJ (GC), *État luxembourgeois*, 6 October 2020, C-245/19 and C-246/19, para. 57.

III.3.1.1.4. Procedural Requirements

Issuing authority

It is established case-law that investigative measures interfering with the right to privacy may be issued only by a limited number of duly empowered authorities.[120] Legislators therefore have to decide which authorities (such as courts, prosecutors, police, FIUs or supervisory authorities), and possibly even more specifically, which units or individuals within those authorities, should be tasked with public-to-private information sharing. Among other practical considerations, this choice will also depend on whether a particular authority's institutional features, as well as the legal framework by which it is governed, provide a good basis for ensuring compliance with the legal requirements below.

Independent prior authorisation

Insofar as the intrusiveness of the data processing necessitates special substantive limits, the ECJ highlights the need for procedures to ensure that the substantive conditions are respected in practice. In the context of both communications metadata and PNR data, case-law therefore usually requires that access to retained data must be "subject to a prior review carried out either by a court or by an independent administrative authority, and that the decision of that court or body be made following a reasoned request by the competent authorities".[121] ECJ or ECtHR case-law does not indicate that the requirement of an independent prior review applies to all forms of access to sensitive data. However, the ECJ implies that insofar as the retention and processing of data constitutes a serious interference with Articles 7 and 8 of the Charter of Fundamental Rights, an independent prior review will constitute an important safeguard to ensure that data processing is limited to what is strictly necessary. As results from the ECJ's case-law on PNR data, such a serious interference will be present in particular if, with the aim of creating a continuous and untargeted surveillance framework, personal data of a very large part of the population is retained and analysed irrespective of a criminal suspicion.[122]

As pointed out above, the retention of financial data cannot be explained exclusively by the aim of providing a surveillance framework for the benefit of authorities, and the procedural safeguards applied by the ECJ regarding access to communications metadata and PNR data thus cannot be comprehensively applied by analogy. After all, financial data is retained first and foremost in order to document transactions for contractual reasons, not least in the customer's own interest. Insofar as competent authorities, including tax authorities, access such data, this may be considered less intrusive in many cases, especially if the

[120] ECHR, *Huvig v. France*, 1105/84, para. 34.

[121] ECJ (GC), *La Ligue des droits humains*, 21 June 2022, C-817/19, para. 223; see also ECJ (GC), *Tele2*, 21 December 2016, C-203/15 and C-698/15, para. 120; ECJ (GC), *Prokuratuur*, 2 March 2021, C-746/18, para. 52.

[122] See ECJ (GC), *La Ligue des droits humains*, 21 June 2022, C-817/19, para. 111.

authorities do not intend to screen the entirety of a person's financial activities, but instead are merely seeking information about clearly specified transactions that provide only limited insights into affected persons' private life.[123]

A different conclusion may be reached, however, if authorities initiate processing of obliged entities' data not in order to clear up a specific dubious financial activity, but instead to draw on past financial data as a way of scrutinising a person's non-financial activities (for example whether she has particular personal preferences or whether she was at a specific location at a given time) or in order to identify past suspicious transactions through the analysis of bulk data. The same holds true if the public-to-private information sharing is meant to lead to a screening of future transactions on the basis of the shared information, especially if the shared information is targeting specific individuals or entities in order to detect suspicious transactions. In such cases, the systematic retention of customer data, and the analysis of this data on the authorities' behalf, is primarily characterised by a surveillance approach, not by the more conventional approach of retracing suspects' financial transactions. For such surveillance-style processing of customer data, ECJ case-law could be understood as demanding a prior review of the public-to-private information sharing.

Finally, an independent prior authorisation may also be required if the public-to-private information sharing is deliberately intended to impede particular individuals' or entities' access to financial services, or to exclude them from such services entirely. Of course, not every prevention-oriented disclosure of information by authorities to a private party will require these safeguards – possibly even if, at least in an emergency, the disclosure is meant to warn the addressee of a threat posed by a particular person. Yet insofar as a potentially stigmatising disclosure can have far-reaching repercussions for a natural or legal person's private life or business activities by limiting their access to financial services or their creditworthiness, the potential for error and abuse should be deemed considerable and require an authorisation process that will avert such consequences as much as possible.

Prior hearing or ex post notification of individuals and entities targeted by a measure

The Court of Justice has recognised as a general principle of EU law that by and large, every person must have "the opportunity to make known his views effectively during an administrative procedure and before the adoption of any decision liable to affect his interests adversely".[124] With regard to decisions of institutions, bodies, offices, and agencies of the EU, this right is explicitly recognised by Article 41(2)(a) of the Charter of Fundamental Rights. The purpose of the right is in particular to ensure that administrative decisions are

[123] To this effect seemingly ECJ (GC), *État luxembourgeois*, 6 October 2020, C-245/19 and C-246/19.

[124] ECJ, *Mukarubega*, 5 November 2014, C-166/13, para. 46; see also ECJ, *Ismeri Europa Srl*, 10 July 2001, C-315/99, para. 28.

not taken without hearing the affected person about the facts on which the authorities want to base their decision, thereby granting her a prior opportunity to challenge the accuracy of these facts and submit additional information that might change the envisaged decision in her favour.[125] Yet the right to be heard can be restricted, "provided that the restrictions in fact correspond to objectives of general interest pursued by the measure in question and that they do not involve, with regard to the objectives pursued, a disproportionate and intolerable interference which infringes upon the very substance of the rights guaranteed".[126]

Data protection law may also entail a requirement of an *ex post* notification of the persons affected by a public-to-private information sharing. Although Regulation 2016/679 and Directive 2016/680 do not explicitly refer to a notification of the data subject in this context, the ECJ has developed this requirement in the context of access to communications metadata:

> [T]he competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.[127]

This requirement has been developed especially in the context of authorities' access to communications metadata, but so far the ECJ has not clarified whether, or to what extent, an *ex post* notification may also apply with regard to financial data. However, the case-law indicates that Article 47(1) of the Charter of Fundamental Rights may also require an *ex post* notification in other data-processing situations. To be sure, not every access of authorities to personal data held by a private third party will require enabling the affected person to directly challenge the lawfulness of that access – that is, to challenge it independently of the subsequent use of the data thus obtained. According to the ECJ, the enabling of such a direct challenge may not be required, for example, if tax authorities order a financial institution to provide customer data, provided that the customer in question is able, at a later stage, to challenge the access indirectly – that is, as part of a challenge mounted against the tax investigation's outcome.[128] Depending on the sensitivity of the data in the particular case, ECtHR case-law does however suggest that authorities' obtaining mere access to financial data retained by a financial institution may require that an effective remedy directly against the access must already be

[125] ECJ, *Mukarubega*, 5 November 2014, C-166/13, para. 47.

[126] ECJ, *Mukarubega*, 5 November 2014, C-166/13, para. 53; see also Art. 52(1) of the Charter; see also ECJ, *Organisation des Modjahedines du peuple d'Iran*, 12 December 2006, T-228/02, para. 133–134.

[127] ECJ (GC), *Tele2 Sverige*, 21 December 2016, C 203/15 and C 698/15, para. 121.

[128] See ECJ (GC), *État luxembourgeois*, 6 October 2020, C-245/19 and C-246/19, para. 83–93.

open.[129] The ECJ stance on this issue may therefore come under pressure from the ECtHR in the future.[130] In any case, it would seem that insofar as authorities' access to financial data is concerned, the ECJ and the ECtHR both require an *ex post* notification of the targeted customer if otherwise he would likely never become aware of the access.

Even though the case-law does not provide conclusive guidance in this regard, in the present context and as long as the authorities' investigation will not be jeopardised, the jurisprudence leans towards indicating that an *ex post* notification will most likely be required, particularly if the public-to-private sharing is meant to prompt farther-reaching data processing by obliged entities so that any relevant resulting findings may be provided to the FIU or other competent authorities. This may notably be so if authorities intend to cause the obliged entity to continuously monitor the future financial activities of a particular individual,[131] or if the obliged entity is asked to analyse an individual's past financial activities. In these cases, an *ex post* notification of the targeted person (or the provision of access to the case file) will usually be required, at the latest at the moment when the person challenges the outcome of the investigation.

Furthermore, if the shared information is meant to be used to screen prima facie unsuspicious transactions and customers in order to identify threats, ECJ case-law has suggested that, depending on the degree of intrusiveness of the screening, it may be necessary to notify those individuals who were singled out by obliged entities due to the information provided by the authorities. As the ECJ stated in the *La Quadrature du Net* case:

> With regard to the notification required in the context of automated analysis of traffic and location data, the competent national authority is obliged to publish information of a general nature relating to that analysis without having to notify the persons concerned individually. However, if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually. That notification must, however, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible.[132]

While it must be recalled that this judgment referred to the processing of communications data, and therefore concerns particularly sensitive data, one

[129] See ECtHR, *M.N. and Others v. San Marino*, 7 July 2015, 28005/12, para. 80–82; ECtHR, *G.S.B. v. Switzerland*, 22 December 2015, 28601/11, para. 96.

[130] See *opinion* of Advocate General Kokott of 2 July 2020 in joined Cases C-245/19 and C-246/19.

[131] See also ECJ (GC), *La Quadrature du Net*, 6 October 2020, Cases C 511/18, C 512/18 and C 520/18, para. 190.

[132] ECJ (GC), *La Quadrature du Net*, 6 October 2020, Cases C 511/18, C 512/18 and C 520/18, para. 191.

must also bear in mind that obliged entities' screening of unsuspected customers and transactions on the basis of selectors provided by the authorities (in particular in the form of names of individuals or legal entities known or suspected to be involved in financial crime) will regularly expose blameless customers to the danger of being erroneously associated with, or even confused with, the individuals or entities named by the authorities. Such consequences can result not only from involuntary errors in obliged entities' automated customer screening, but equally from the possibility that obliged entities may consciously decide to discontinue a business relationship with customers who merely *may* be linked to named individuals or entities. Even if one were to assume that the processing of financial data is generally less sensitive than the processing of communications metadata, the danger of blameless customers being wrongly associated with targeted persons (and therefore suffering de-risking or similar adverse measures) may lead to the conclusion that the *ex post* notification requirement is applicable here as well. The same should then apply if authorities ask an obliged entity to subject a particular individual's financial transactions to additional CDD measures in order to establish whether the transactions should be reported to the FIU as suspicious, especially if that request entails a similar potential that this individual may be subjected to de-risking or other adverse measures as a consequence.

By analogy with ECJ and ECtHR case-law, an *ex post* notification may be required even with regard to third private parties who were not targeted by the authorities, but whose rights were nevertheless infringed as a consequence of a public-to-private sharing.[133] Where there are indications that a public-to-private sharing has led to de-risking or similar adverse consequences for persons other than those targeted by the authorities, the authorities may be required, in order to comply with Article 47(1) of the Charter of Fundamental Rights, to ensure that they find out whether the obliged entity in question did in fact discontinue its relationship with third parties on the basis of the shared information, and in this case to notify those third parties about the underlying information sharing.

III.3.1.2. Remedies

III.3.1.2.1. Remedies for Obliged Entities

The right to an effective remedy under Article 47 of the Charter of Fundamental Rights also applies to legal persons.[134] Consequently, insofar as an authority, in the context of an information sharing, imposes particular obligations on the receiving obliged entity, the latter is entitled to have these obligations reviewed by a court. Legislation may limit this right, provided that such limitations respect the conditions set forth by Article 52(1) of the Charter. To take one example,

[133] See ECtHR, *M.N. and Others v. San Marino*, 7 July 2015, 28005/12, para. 83; ECJ (GC), *État luxembourgeois*, 6 October 2020, C-245/19 and C-246/19, para. 96.

[134] ECJ (GC), *État luxembourgeois*, 6 October 2020, C-245/19 and C-246/19, para. 57–58.

the authorities might require an obliged entity to abstain from a particular business opportunity because they believe it would lead to criminal abuse of the obliged entity, but at the same time, by exception, they also might need to refrain from disclosing the evidence underlying their assessment to the obliged entity, even within judicial proceedings, for instance for reasons of national security.[135] In any case, legislators cannot make the remedy conditional on an obliged entity's prior violation of an order.[136] Thus, for instance, if an authority were to order an obliged entity to perform additional CDD measures vis-à-vis a specific customer, that order (and not just supervisory sanctions imposed in response to a possible violation of the order) must be subject to review by a court.

III.3.1.2.2. Remedies for Individuals and Entities Targeted by Information Sharing

In line with Article 54 of Directive 2016/680 (for most competent authorities) and Article 79(1) of Regulation 2016/679 (for FIUs covered by that regulation), individuals who have been the subject of a targeted public-to-private sharing must have a right to an effective judicial remedy against the issuing authority. Such individuals are furthermore entitled to lodge a complaint with the competent data protection supervisory authority according to Article 52(1) of Directive 2016/680 or Article 77(1) of Regulation 2016/679, if they claim that a transfer was based on erroneous facts or otherwise issued unlawfully, and they are also entitled to an effective judicial remedy against this authority in line with Article 53(1) of Directive 2016/680 or Article 78 of Regulation 2016/679.

However, in many ways the scope and actual effectiveness of these remedies are still unclear. Some Member States, for instance, consider that a sufficient remedy lies in an indirect opportunity to challenge data processing by public authorities, in the sense that individuals who have been targeted by a data processing activity of a public authority may only challenge the outcome of investigations in which the data was processed.[137] Furthermore, access to an effective remedy will usually depend on whether a targeted person is made aware of the data processing at some point. Yet even though Article 14 of Directive 2016/680 and Article 15 of Regulation 2016/679 provide that every data subject has the right to obtain from the data controller information about the data that is processed about him or her, Member States will often limit this right under Article 15 of the Directive or Article 23 of the Regulation. However, these provisions allow restrictions of the rights of data subjects only insofar as is necessary and proportionate in the interest of, e.g., the prevention, investigation, detection or prosecution of criminal offences. It is still largely

[135] See ECJ (GC), *ZZ*, 4 June 2013, C-C-300/11, para. 54; ECJ (GC), *Kadi II*, 18 July 2013, C-584/10 P, C-593/10 P and C-595/10 P, para. 126.

[136] See ECJ (GC), *État luxembourgeois*, 6 October 2020, C-245/19 and C-246/19, para. 68.

[137] Opinion of Advocate General Medina of 15 June 2023 in Case C 333/22, *Ligue des droits humains ASBL*.

unclear to what extent the limitations currently provided by Member States meet these requirements. The same is true for other restrictions on data subjects' rights under Article 13(3), Article 15, and Article 16(4) of Directive 2016/680 and a similar restriction allowed by Article 23 of the Regulation. In any case, such restrictions should be the exception, not the rule.[138]

Accordingly, there is a need for legislative clarification of the law regarding the remedies available to data subjects in the context of public-to-private information sharing. At least in some situations, and depending primarily on the gravity of the interference in the rights at stake, targeted individuals should be able to directly challenge the information sharing, in particular when the sharing is likely to directly cause material or reputational prejudice to the targeted individuals. As a rule, remedies should also be available against some forms of information sharing by judicial authorities in the context of criminal investigations, especially if the authorities ask an obliged entity to conduct particularly intrusive forms of data processing. It must be remembered that judicial supervision of a measure is not equivalent in itself to an effective remedy.

Besides, legislators should note that the remedies provided by Directive 2016/680 and Regulation 2016/679 apply only to natural persons. But given that public-to-private information sharing can also lead to serious infringements of the rights of legal entities, legislation should provide them too with effective remedies.

III.3.2. The Use of Information by Obliged Entities

III.3.2.1. Obliged Entities' Obligations

Defining the purpose for which shared information is processed by obliged entities

If public-to-private information sharing involves personal data, the authorities must define the purpose of the sharing in each case. The obliged entity's primary obligation is to process the shared information in line with this purpose, and to limit that processing to what is necessary to achieve the purpose.[139] However, considering the potential detrimental consequences that sharing even non-personal data (such as the name of a company or the subject-matter of an ongoing investigation) can have for both customers and the success of investigations, it is often important also to strictly limit the use of such information. Accordingly, any authority engaged in public-to-private information sharing must first of all define exactly how recipient obliged entities are expected to process the shared information, and to what extent it can be disseminated inside and outside these entities. Authorities must in particular

[138] Opinion of Advocate General Medina of 15 June 2023 in Case C 333/22, *Ligue des droits humains ASBL*, para. 40.

[139] See Art. 5(1)(b)(c) of Regulation (EU) 2016/679.

clarify to what extent information may be used in the customer and transaction screening processes that obliged entities usually apply.

Ensuring respect for purpose limitations

As the necessity and proportionality *stricto sensu* of public authorities' disclosure of data depend not least on the risk that the data might be abused after being transferred to the private sector, it is crucial to the overall lawfulness of public-to-private sharing that obliged entities' compliance with any purpose limitations must be ensured. The more sensitive the shared information is, the more it will be necessary to ensure that the purpose limitations that were defined by the disclosing authority are respected. In this regard, legislators must be particularly sensitive to the fact that they cannot expect private businesses' data processing to meet the same standards that they would expect public authorities' data processing to meet, given that businesses are generally established not to serve the public interest, but instead to make a profit. A realistic legislative approach to defining obliged entities' obligations must in particular bear in mind that their data processing will usually not meet the same standards of objectivity and fairness that one would expect from a public authority, and that in practice, compliance with any purpose limitations (for example that a particular set of shared data must be used solely as a trigger for enhanced CDD) may be diluted (to stay with the example, the shared data may for instance lead to de-risking or an increase in the price that affected customers are charged for financial services). Legislation may then have to take into account, not least of all, the need to precisely define the extent to which shared information may be used to justify adverse measures, such as de-risking, directed at both targeted customers and unrelated customers. To ensure that purpose limitations are in fact respected, authorities will have to ensure oversight of the recipient obliged entities' handling of the shared information, especially if the information is personal data or is related to specific legal entities.

Preventing information loss

Compliance with purpose limitations is especially threatened by intentional or negligent information losses within recipient obliged entities. To address this problem, legislators can develop mechanisms to ensure, so far as reasonably possible, that information does not fall into the wrong hands within obliged entities. Legislators could furthermore consider extending confidentiality obligations under national law to include private persons to whom the shared information is disclosed. An apparent breach of such obligations could then be investigated, and where appropriate, sanctioned through criminal or administrative proceedings. To bolster respect for purpose limitations, one might also consider appointing a central contact person within the obliged entity to take charge of determining how to disseminate the information internally.

Automated processing of personal data

Legislators should have due regard to the fact that obliged entities will use automated means to process supplied information. As already provided by Article 22 of Regulation 2016/679 and Article 11 of Directive 2016/680, individuals must not, as a rule, be subject to automated decision-making, particularly profiling. This means that if the results of automated data processing, especially of an automated screening of customer data, are not verified by humans, they must not form the basis of adverse measures against a customer, such as the filing of a SAR or de-risking.[140]

In addition, while the quality of the non-automated verification of automated processing results is of key significance, and such verification must accordingly be performed using objective and non-discriminatory criteria, the ECJ has highlighted the importance, with regard to the authorities' processing of personal data, of establishing appropriate criteria already at the automated processing stage. To this end, the ECJ requires that it must always be possible for a human analyst to understand how a given program arrived at a positive match, thereby precluding "the use of artificial intelligence technology in self-learning systems" that are "capable of modifying without human intervention or review the [automated] assessment process", in particular the criteria used in this assessment.[141] While this case-law is not directly applicable to data processing by private entities, it should be taken into account at least when obliged entities process personal data on behalf and for the benefit of authorities.[142] In a similar vein, legislators should note that the ECtHR and ECJ have increasingly emphasised the need for data processing by public authorities not to be discriminatory.[143] Again, the standards developed in this regard are generally not directly applicable to data processing by private entities, but they may become relevant when obliged entities process customer data on the basis of criteria that the authorities provided for this purpose. The law should therefore make it clear that public-to-private information sharing must not lead to a discriminatory processing of customer data.

III.3.2.2. Remedies

Remedies related to data protection

Concerning the unlawful processing of any personal data, Regulation (EU) 2016/679 already contains important safeguards that must be effectively

[140] See the opinion of Advocate General Pikamaë in case C-634/21, *SCHUFA Holding*, 16 March 2023.

[141] ECJ (GC), *La Ligue des droits humains*, 21 June 2022, C-817/19, para. 194.

[142] See W Maxwell, X Vamparys and A Bertrand, "Do AI-based anti-money laundering (AML) systems violate European fundamental rights?", *International Data Privacy Law*, no. 3, vol. 11, 2021, pp. 276-293.

[143] See notably ECtHR, *Muhammad v. Spain*, 18 October 2022, 34085/17, para. 91; ECJ (GC), *La Quadrature du Net*, 6 October 2020, C 511/18, C 512/18, C 520/18, para. 180; ECJ (GC), *La Ligue des droits humains*, 21 June 2022, C-817/19, para. 197.

implemented at the level of Member States, particularly the right of natural persons to lodge a complaint with a supervisory authority,[144] the right to an effective judicial remedy against a supervisory authority,[145] the right to an effective judicial remedy against a data controller or processor,[146] and the right to compensation for material and non-material damage suffered as a result of a violation of Regulation (EU) 2016/679.[147] Yet the practical value of these remedies is still open to question, not least because the scope of data subjects' right against the data controller to access personal data concerning them[148] is not clearly defined in the field of AML/CFT.[149] To provide individuals, in the context of public-to-private information sharing, with an effective remedy against the data processing that obliged entities undertake as a consequence of the sharing, legislators should therefore specify more precisely the conditions under which obliged entities' customers may avail themselves of the remedies under Regulation 2016/679. Furthermore, legislators should take note that the remedies under the Regulation are available only to natural persons.[150] Given that an obliged entity's data processing in the context of public-to-private sharing can also cause detrimental effects for customers that are legal entities, legislation should clarify the extent to which remedies against the obliged entity are also open to these customers.

Remedies related to de-risking

Because de-risking and other adverse measures affecting obliged entities' customers can impact the proportionality of public-to-private information sharing, legislators should furthermore consider remedies to ensure that if information sharing leads to such consequences, they will not be excessive. This primarily concerns the case that obliged entities might reassess their business relationship to particular customers or groups of customers when it appears that these customers could somehow be linked to the individuals, entities or events that were singled out by the authorities. When such a link is objectively absent, the obliged entity's reaction could constitute a violation of the purpose limitations underlying the information sharing. This is especially so if the measures adopted against certain groups of customers following a public-to-private information sharing are discriminatory and not based on a case-specific risk assessment of the particular business relationships. In this case, the above remedies under data protection could provide an avenue to address de-risking. Yet in many cases, it may seem more appropriate to approach de-risking less as a violation of purpose limitations than as a question

[144] Art. 77(1) of Regulation (EU) 2016/679

[145] Art. 79(1) of Regulation (EU) 2016/679.

[146] Art. 79(1) of Regulation (EU) 2016/679.

[147] Art. 82(1) of Regulation (EU) 2016/679.

[148] Art. 15 of Regulation (EU) 2016/679.

[149] See Art. 23 of Regulation (EU) 2016/679, which provides Member States with the power to define exceptions to the right of access.

[150] See Art. 4 (1) of Regulation (EU) 2016/679.

pertaining to obliged entities' freedom of contract, and legislators should then consider whether remedies under data protection law could really be effective, or whether more specific remedies are called for, particularly mechanisms that provide for a realistic balancing between customers' rights and the obliged entity's freedom of contract.

IV. Developing a Legal Framework for Public-to-Private Information Sharing in AML/CFT

The above analysis has demonstrated that public-to-private information sharing raises numerous complex legal questions for which national legal orders are usually not yet prepared. Currently the law of Member States often lacks adequate legal bases for the provision of information by competent authorities to the private sector, especially insofar as personal data is concerned. Even where laws sometimes explicitly authorise public-to-private transfers of information, they usually do not address the particular challenges that arise when such transfers are done within the framework, and for the purpose, of AML/CFT. This is even more true where public-to-private information sharing is done informally without any explicit legal basis, not least in the context of criminal investigations. The lack of adequate legal frameworks raises doubts not only about the conformity of some existing public-to-private sharing practices with the rule of law, but also about the coherence of their underlying policy. The EU and Member States should address these doubts through legislation defining clear policy aims and safeguards, so that public and private stakeholders can have confidence in the legal anchoring of their cooperation, and at the same time, individuals and entities whose rights are affected by the information sharing are equipped with effective remedies. To this end, the following recommendations are meant to provide policymakers with guidance on how to shape such legislation.

A need to address both voluntary partnerships and mandatory forms of cooperation

It should be highlighted that the instruments proposed in the following are not a reinvention, but rather a description and systematisation of (at least in some instances) existing forms of cooperation between competent authorities and obliged entities. However, various forms of such cooperation regularly go by confusing and blurry names at present. In particular the term "public-private partnerships" is frequently used as an umbrella term for very different types of public-private interaction and therefore does not provide meaningful orientation for a legal assessment. Furthermore, the term "partnership" conventionally refers to a voluntary endeavour, which however constitutes an overly narrow starting point for policy debates on public-private cooperation. This is so because in the area of terrorism and other forms of serious organised crime, both the authorities and the private sector usually operate in a highly regulated

legal environment where there might ultimately be only limited scope for voluntary choice. This is not to say that voluntary cooperation by obliged entities with authorities might not offer significant advantages, but it would not be wise to rule out from the start that some new forms of cooperation might better be based on legal obligations.

As a consequence, the following recommendations address both the scenario in which investigative authorities and FIUs collaborate with obliged entities on a voluntary basis – that is, in the sense of a public-private partnership – and the alternative scenario where the law might require obliged entities to collaborate with the authorities. It will be explained that, in both cases, legislators will have to specify the competent authorities' powers to share information, as well as the obliged entities' rights and obligations relating to how to process that information. In other words, public-private information sharing always requires legislators to have a double perspective: They need to provide clear rules for the involvement of both the competent authorities and the obliged entities at the same time. Merely providing authorities with information-sharing powers will not suffice. For, as shown above, current AML laws are as yet largely silent as to what obliged entities can or must do when getting involved in a collaborative mechanism.[151]

A need to coherently integrate new solutions into the existing AML/CFT architecture

The following proposals furthermore reflect the need to integrate public-private partnerships and other forms of financial-crime-oriented cooperation into the wider AML/CFT legal architecture. There are two primary reasons for this need. First, if public-to-private information sharing is meant to remedy some of the deficiencies of current AML/CFT instruments, it would be a mistake to create new public-to-private information-sharing instruments for AML/CFT without explaining exactly how these new instruments are meant to interact with, and ultimately improve, existing AML/CFT instruments. Second, a coherent integration of new public-private cooperation mechanisms into the existing legal framework is important because this framework is bound to influence whether and how obliged entities approach, and participate in, such mechanisms, in particular in view of the expectations of AML/CFT supervisory authorities and data protection supervisors. Without clear rules on the impact of new instruments on the obliged entities' existing obligations, innovation runs the risk of producing more legal uncertainty and dysfunction, not less.

Five different categories of public-private cooperation

The following analysis differentiates between, and defines, five categorically different forms of public-to-private-information-sharing-based cooperation between competent authorities and obliged entities. The authors have labelled these as threat warnings (IV.1.2.), risk notifications (IV.1.3.), risk indicators

[151] III.1.1. and III.2.2.2.3.

(IV.1.4.), financial analysis requests (IV.2.2.), and financial monitoring requests (IV.2.3.). However, this terminology is secondary and has been chosen only out of a need to categorise different possible forms of cooperation. As a starting point, the analysis distinguishes between two generally very different (albeit to some extent overlapping) aims of public-to-private sharing, namely (IV.1.) sharing to support crime detection and prevention by the private sector, and (IV.2.) sharing meant to support an ongoing investigation or analysis by competent authorities. The former is essentially about improving the performance of the AML/CFT regulatory framework, while the latter is about strengthening competent authorities.

IV.1. Public-to-Private Sharing for Preventive Purposes

IV.1.1. Possible Purposes of Preventive Public-to-Private Sharing

Oftentimes, through their own investigations or through foreign partners, the authorities come across information that could serve to protect against threats to the integrity of the financial sector. Yet at the same time, for legal or practical reasons, these authorities will often not be able to take direct coercive action against the authors of the threat. This can be the case, for example, when a criminal investigation by a Member State or a third country reveals that criminals are using a network of non-EU shell companies to funnel criminal assets into or out of the EU. Due to the network's third-country localisation, criminal or administrative proceedings against such companies will often be unfeasible. But if the authorities were to provide information about the network to relevant obliged entities, the latter could adopt measures to avert or discontinue any direct or indirect contact with these shell companies. Yet as things stand today, obliged entities in the EU will often not be informed about such threats, especially if the information available to the authorities is mainly about events outside the EU and provides no clear basis for a criminal investigation within the EU.

Even in cases where ongoing threats are uncovered through a criminal investigation in the EU, obliged entities that are affected by the threats will often not learn about them. In some cases, investigators will share information about relevant threats when they come into contact with an obliged entity as part of a criminal investigation, not least when they approach a potentially affected obliged entity with a request for the entity to hand over information. But EU law and many national frameworks do not provide a clear legal basis for such practices, let alone dedicated mechanisms for the transfer of relevant information to the private sector. The disclosure of information within the context of criminal investigations is widely accepted insofar as it serves the production of evidence, and in this way, as a collateral added value, obliged entities will frequently learn about particular threats to which they are exposed, not least when they learn that a particular customer is being investigated for financial crime. Yet such disclosure powers are rarely conceptualised as a preventive instrument, so that in practice, the authorities will not be guided by

a clear preventive policy, let alone the intention that obliged entities might have some level of a confident expectation to be informed about threats.

Special AML/CFT-dedicated public-to-private information-sharing mechanisms can (and in some Member States already do) partially overcome the state of affairs described above. To understand the legal challenges that any Member State must address when contemplating the possibility of setting up such mechanisms, it is helpful to start by explaining, in very basic terms, the different purposes that preventive public-to-private sharing may serve. These purposes may sometimes overlap in current practice (and can for example be combined in one and the same FIU or supervisory guidance), and as yet the terminological usage at the level of the EU and Member States is certainly not very coherent. Broadly speaking, one can distinguish three different purposes:

- *First*, an authority may warn obliged entities that a specific situation (in particular a certain business relationship or a specific prospective customer) entails a financial threat, so that these obliged entities can protect themselves against it. This is called a "**threat warning**" below.
- *Second*, an authority may inform obliged entities, in order to facilitate the detection of suspicious activities, that particular situations (for example specific business relationships, or transactions that are linked to particular entities) entail a high risk of financial crime, even though the authority is unable to confirm whether the situation is in fact a threat. This is termed a "**risk notification**" here.
- *Third*, without identifying particular individuals, entities or transactions, authorities may provide information about typical financial crime methods or current criminal developments with the aim of guiding obliged entities' CDD by identifying criteria for the identification of risks. This kind of information is called "**risk indicators**" below.

Threat warnings

To be more specific, *threat warnings* enable obliged entities to address a particular threat when, for whatever reasons, authorities are not, or not yet, able to tackle it through coercive action by themselves. This may be the case in particular when competent authorities have sufficient information that an obliged entity is threatened by a criminal group, but no information that would already allow them to initiate a criminal investigation and adopt preventive coercive measures under the powers provided by criminal procedure law. To allow obliged entities to identify the threat, such warnings always refer to a particular person or entity from whom the threat originates. As an example, one can think of information that a customer of an obliged entity is closely involved in the activities of a criminal group, without any evidence yet that this customer has already abused the obliged entity's services to commit financial crimes. The authorities may, at this point, have no power to directly interfere in the relationship between this customer and the obliged entity. Yet in light of the proximity between its customer and the criminal group, the obliged entity may be keenly interested in discontinuing this relationship or implementing other

measures to address the concrete danger that it may be abused by this customer for criminal purposes. Similarly, a threat warning may be desirable if the authorities have evidence that the staff of a particular obliged entity has been infiltrated by individuals who are closely tied to a criminal group, even if the authorities have no information about specific crimes already committed by the infiltrators. Threat warnings might also be of considerable preventive value even when an obliged entity has not yet come in direct contact with the criminal actor. This could for example be the case when the authorities have reliable information that a particular criminal group, with the help of a known individual or entity, is currently trying to acquire companies in a particular economic sector within a particular region. Obliged entities with a strong regional footprint in that economic sector could be alerted to these developments by a warning, and thus take measures to be sure not to onboard the individuals and entities mentioned in the warning, and other individuals and companies linked to them.

Risk notifications

For their part, risk notifications are intended not to inform obliged entities about the presence of a particular threat, but merely to offer guidance for these entities' CDD – though in a very targeted way, especially by telling obliged entities that a particular business relationship, or any business relationship or transaction having a particular feature (for example a link to a particular entity), always constitutes a high risk and must therefore be subject to additional CDD measures to clear up the situation. Risk notifications may notably be useful in cases where the authorities possess information that a particular business relationship shows characteristics that are common for financial crime, or other information about particular features that indicate a significant probability of a link to financial crime, such as postal addresses or IP addresses that have been used for purposes of financial crime in the past.

Risk indicators

Finally, *risk indicators* can take various shapes, for example information about the activities of a criminal group operating in a particular town or region. Importantly, unlike risk notifications, risk indicators will not express a view that particular individuals, entities or business relationships are linked to crime or constitute a high risk, but merely provide obliged entities with a better understanding of criminal activity, in the expectation that this understanding will be useful for those entities in identifying high-risk business relationships and transactions.

Under the above definitions, risk notifications differ from threat warnings in that risk notifications are meant to ensure that an obliged entity pays particular attention to specific high-risk situations by implementing additional CDD measures, while threat warnings are essentially meant simply to clarify that particular individuals or entities represent an unacceptable risk. At the same time, risk notifications differ from risk indicators in that risk indicators, while

providing information relevant for CDD, leave it to the obliged entities to determine whether a particular business relationship or transaction carries a high risk.

As a general observation, it is worth highlighting that public-to-private sharing can also take the form of a public authority vetting the transfer of information from non-public sources, if the authority adds further information in the process of that vetting. This is the case, for example, when an authority declares publicly available information (such as media reports) to be reliable, or when an authority authorises the transfer of information from one obliged entity to another on the grounds that the authority judges the information to be sufficiently reliable – because in both cases, the authority thereby (explicitly or implicitly) declares that it possesses additional information that confirms reliability. Public-to-private sharing can furthermore take the form of a joint production of risk indicators by authorities and obliged entities when both sides feed information into the process.

IV.1.2. Threat Warnings

Threat warnings are meant to enable the obliged entity to protect itself against being abused for purposes of financial crime. A relevant threat would be any situation or chain of events that, if not stopped, will likely lead to such abuse in the near future. In contrast, one cannot yet speak of a threat if the available information, even though indicating a risk of abuse, does not show concrete activities that are, with a considerable degree of probability, intended to abuse obliged entities. Thus what is required is not a complete certainty that the obliged entity will be abused, but the presence of facts that justify a substantiated prognosis to this effect.

On the basis of the necessity and proportionality considerations described above,[152] legislators must define the substantive conditions and procedural safeguards of threat warnings. To this end, one should distinguish two stages of the public-private interaction: first, the transfer of information from public authorities to obliged entities,[153] and then, the processing of the transferred information by the obliged entities themselves.[154] For each of these stages, conditions and safeguards must be defined.

IV.1.2.1. The Transfer of Information from Public Authorities to Obliged Entities

IV.1.2.1.1. Conditions

IV.1.2.1.1.1. Necessity

In each case, issuing the warning must be necessary. This leads to essentially four sets of questions:

[152] III.3.1.1.2. and III.3.1.1.3.

[153] III.3.1.

[154] III.3.2.

- whether, based on objective criteria, a threat is indeed present;
- whether the authorities could achieve the same preventive effect with means that would constitute a less intrusive interference in the rights of affected individuals and entities;
- to whom exactly the warning must be addressed in order to be effective, and who needs to know how much;
- to what extent the warning must contain sensitive details about the threat.

The presence of a threat

In determining the gravity of the threat, legislators and authorities must take into account that gravity depends on both the magnitude of the financial crime likely to result from the threat and the likelihood of this crime actually occurring. Neither the magnitude of the expected crime nor its likelihood is enough, on its own, to establish the gravity of the threat. For example, if the authorities have information that a particular company is playing a central role within a large transnational money laundering network, a certain degree of doubt about the reliability of the information will not necessarily inhibit the conclusion that the threat is in fact grave, in view of the magnitude of the financial crime at stake. In contrast, if authorities have information that a particular individual may be abusing a small number of bank accounts to launder some thousands of euros of criminal assets, which thus would be a financial crime of a comparatively lesser severity, similar doubts about the reliability of the underlying information may preclude the assumption that a threat is indeed present.

The availability of less intrusive, equally effective alternatives

As regards the availability of less intrusive alternatives to a warning, it could be argued in some cases that the rights of the targeted person or entity would be less affected if the authorities addressed the threat by imposing a prohibition or similar order, for example by prohibiting a tainted entity to engage in a particular business relationship, or by prohibiting a particular individual to work for an obliged entity. If such measures were to be addressed directly to the author of the threat and not to third parties, their potentially stigmatising effect, and the resulting adverse effects on affected persons' private life or economic freedom, might be less significant. Yet often such alternatives will not be as effective as issuing a warning to relevant obliged entities. Obviously, some individuals will be deterred from committing crimes once they are informed that their activities are attracting the authorities' scrutiny, for instance through an order prohibiting certain activities or even through a mere warning addressed only to them and not to third parties as well. In such cases, a warning to obliged entities is not necessary, and addressing a measure only to the author of the threat himself will usually suffice.

Oftentimes, however, the author of the threat will already be well aware that he has attracted the authorities' attention, and will nevertheless continue to engage in the activity concerned (for example, running a business in the EU

despite close links to a criminal organisation in a third country). Furthermore, measures that are directly addressed to the author of the threat will usually be much more difficult, and often even impossible, to implement if the individuals or entities in question are abroad, especially if they are located in a third country. After all, it must be remembered that individuals and entities do not need to be present in the EU in order to threaten the integrity of the EU financial sector; for example, a tainted third-country business may have accounts in the EU, or the third-country subsidiary of an EU obliged entity may have been infiltrated by tainted individuals. In these cases, it will normally not be possible to address the threat effectively without informing the relevant obliged entities in the EU. Furthermore, even if the individuals or entities in question are located in a Member State and thus in reach of its authorities, in some situations a warning might still be necessary to ensure effective prevention if there are reasons to expect efforts at circumvention through the use of stooges and front companies. To ensure effective prevention, it may sometimes even be necessary to combine a warning with coercive measures (such as freezing accounts or transactions), thereby signalling to obliged entities that they should watch out for other, yet-unknown individuals or companies that may in fact serve to hide the author of the threat.

Scope of dissemination of the threat warning

The determination of which obliged entities should be addressed by a warning depends closely on the nature of the specific threat. If the threat is only about the abuse of a particular business relationship or the infiltration of a particular obliged entity, it will usually suffice to address only the obliged entity concerned. In contrast, if the threat concerns the likely future abuse of yet-unspecified obliged entities, the selection of addressees poses more questions. The more is known about the threat, the easier it will be to identify particular obliged entities that are under threat. For example, if it is known that a tainted company plans to acquire businesses operating in a particular sector and geographical area, it may be concluded that this situation threatens especially those obliged entities that have a relevant geographical footprint in managing acquisitions of businesses in the sector concerned. The broader the market for a particular service, and thus the more numerous the obliged entities that might potentially be abused when a threat involving that service is present, the more widely disseminated the warning will need to be in order to have a preventive effect. Where a wide dissemination of a warning appears to be necessary, whether this can be done lawfully is not a matter of whether such a dissemination is necessary, but whether, in light of the gravity of the threat, such a dissemination is proportionate *stricto sensu*.[155] One should also consider the possibility that the warning may have a significant preventive effect, and therefore be necessary, even if it is addressed only to a limited number of those obliged entities that are at risk of being abused. For even if the warning can potentially be circumvented by (ab)using obliged entities that were not

[155] III.3.1.1.3.1.

addressed by it, such a selective dissemination can still significantly enhance the probability that the threat will be detected.

Dissemination of the warning within obliged entities

Besides in selecting the obliged entities to be addressed by a warning, the necessity requirement is also relevant for determining exactly who within the receiving obliged entities needs to have access to the warning's content. This can again depend on the nature of the threat. If the threat essentially relates to the activities of an individual or entity in a particular town or region, effective prevention may not require the warning to be brought to the notice of a large number of employees of the receiving obliged entity; instead it may suffice for the warning to be made accessible to only a selected number of regional branches. In contrast, if the threat is less specific, and particularly if it could potentially penetrate the obliged entity through any branch or foreign subsidiary, it may be necessary to make the warning accessible at least to those employees who have a group-wide view of the obliged entity's operations. Obviously, as will be shown next, the scope of the dissemination is important not only as regards the effectiveness of the warning, but also for assessing whether the warning is proportionate *stricto sensu*. In deciding the appropriate scope for the dissemination of a warning, one must therefore always remember that while a wider dissemination might be desirable from the point of view of effectiveness, a broad dissemination may ultimately conflict with the proportionality requirement.

Sensitivity of the information contained in the warning

Finally, the necessity requirement must also be considered in deciding the exact content of a threat warning. For a threat warning to serve its purpose, it must refer to a specific situation or chain of events that, if not stopped, will likely lead to the abuse of the addressed obliged entity in the near future. This means that the threat warning must contain enough information about the threat for the receiving obliged entities to be able to address that threat. It follows that the warning must usually specify a particular business relationship or transaction, or at least name the individual or entity that poses the threat. In addition, the warning will need, as a minimum, to provide at least some basic information about the nature of the threat, so that the receiving obliged entities can judge the gravity and urgency of the threat, and decide how best to respond to it. In contrast, if a threat warning does not contain sufficient detail about the nature of the threat, receiving obliged entities will be forced to speculate about the threat, and as a result will likely adopt preventive measures that either go too far or do not go far enough; in other words, the warning will then likely produce effects that are either disproportionate or ineffective. At the same time, it will usually not be necessary to provide obliged entities with a great amount of detail about the facts underpinning the authorities' threat assessment. Where greater detail would be useful for strengthening prevention (for example by providing obliged entities not only with the name of a particular tainted company, but also with the names of that company's employees who seem to

be related to criminal activity), the authorities will have to carefully consider whether the disclosure of such additional information is still proportionate. The available evidence may for instance be strong enough to justify a warning about a particular company and its directors, but not strong enough for the warning to emphasise responsibility of individual lower-ranking employees of the company. Beyond such considerations, a warning's level of detail will obviously also need to take account of the authorities' own confidentiality needs, and in particular the risks that a disclosure of the information may cause for ongoing investigations or any confidentiality assurances given to other domestic or foreign authorities.[156]

IV.1.2.1.1.2. Proportionality Stricto Sensu

In addition to being necessary, a warning must also be proportionate *stricto sensu*.[157] This essentially comes down to balancing the gravity of the threat, the warning's expected effectiveness to prevent the threat, and the intensity of the interference in rights to which the warning may lead. While the gravity of the threat and the expected effectiveness of the warning are rather straightforward questions, the intensity of interference in rights requires particular consideration.

Customers potentially affected by the warning

As regards interference in rights, the authorities must consider what specific consequences the warning will likely have on the targeted individual or entity. Additionally, the assessment of the potential interference in rights must also consider whether the warning may have detrimental effects on third parties who have not been identified as a threat. Such effects are possible because in response to the warning, obliged entities will usually not only abstain from business relationships with individuals and entities that are explicitly mentioned, but also scan other existing and future customers for links with these individuals and entities – and moreover they should do so, because of the possibility that warnings can be circumvented with the help of stooges and front companies. This however entails the risk that customers may be rejected by obliged entities merely because they share some characteristics with individuals and entities mentioned in warnings, even though a more thorough assessment would have shown that in fact the rejected customers had no connection with the threat.

Long-term effects of the warning

Proportionality assessments must furthermore take into account that any threat warning is likely to adversely affect targeted individuals and entities even if the prognosis underlying the warning turns out, at a later stage, to have been erroneous or exaggerated. For even if the authorities issue an official rectification, the individuals and entities in question may still remain tainted in

[156] III.2.1.

[157] III.3.1.1.3.

the eyes of obliged entities. Furthermore, authorities need to be mindful that even if a warning targets only one particular business relationship or transaction – such as the acquisition of a company by a targeted individual – unintended consequences will normally still go beyond this particular business relationship or transaction, at least insofar as the warning's addressee is likely to treat the tainted individual or entity as suspect in any future business dealings as well. Nonetheless, so long as the dissemination of the warning is effectively limited to only one particular obliged entity or a small number of obliged entities (such as the specific credit institution that is financing a tainted acquisition), such long-term stigmatising effects may still be moderate and might have no impact on the affected customers beyond future dealings with these specific obliged entities. In this case, and in any other case where significant long-term stigmatising effects are unlikely, the proportionality principle will essentially require merely a balancing of the gravity of the threat with the warning's expected direct consequences (that is, the expected cancellation of the business relationship or transaction concerned). The more severely and irreversibly the affected customer would be damaged by the expected interference in a business relationship or transaction, the higher the threshold of seriousness should be that the threat must meet.

Particular scrutiny of threat warnings addressed to large number of obliged entities

The proportionality requirement needs to be addressed with particular caution if, where authorities are considering issuing a warning at a time when it is not yet clear exactly which obliged entities are threatened, this uncertainty makes it necessary to issue the warning to a plurality of obliged entities. The dissemination of a warning to a large number of obliged entities, and even more so a public dissemination of a warning, can lead to widespread and long-lasting blacklisting of the individuals and entities concerned, thereby potentially provoking their full-scale financial exclusion. In the case of companies, a widespread warning can effectively make it impossible for them to continue operating in the EU. A threat warning that concerns a company and is disseminated across the entire financial sector will therefore be appropriate only if the available evidence leaves no doubt that the company's current operations are closely linked to serious crime or the company is systematically and severely disregarding particular crime-related compliance obligations, and that the company is therefore highly likely to constitute a permanent financial crime threat for any obliged entity that would engage in business with it. Similarly, a widespread threat warning about an individual – in particular, one disseminated across the entire financial sector – may be proportionate, if at all, only if there is strong evidence suggesting that he or she will commit financial crime in the future. If the companies and individuals in question are located inside the EU, these high thresholds are unlikely ever to be met, because in the event that the evidence pertaining to such a company or individual approaches these thresholds, one should then expect that Member States' competent

authorities will be able to avert permanent criminal threats by taking direct coercive action against the company or individual in question.

Lesser proportionality concerns if dissemination of warning limited in scope

In contrast, a lower threat threshold could apply to warnings that are not disseminated to a large number of obliged entities and will not lead to a widespread stigmatisation of the targeted individuals and entities. Such a warning may be considered when, for example, the available evidence points to an ongoing criminal endeavour aimed at infiltrating a particular business sector in a particular geographical area. In this situation, the authorities may consider warning only those obliged entities that are especially exposed to the threat, and may possibly even further limit the spread by restricting access to the warning to a limited number of employees of these obliged entities. In this case, a warning could be proportionate even if some doubts remain about whether the targeted individual or entity will engage in financial crime in the future, provided that it is still likely that they are part of the criminal endeavour concerned. In any case, such a likelihood can be established only if the available evidence about this endeavour is already sufficiently detailed. A prognosis that is unsubstantiated by specific facts cannot serve as the basis for a proportionality assessment.[158]

IV.1.2.2.1.3. Procedural Requirements

Issuing authority

The competence to issue threat warnings should lie with those authorities who are best placed to assess the threat and who, at the same time, provide a high level of objectivity. Furthermore, given that disclosing information about specific threats to the private sector will regularly entail a risk of endangering the success of ongoing investigations, the power to issue threat warnings should be in the hands of the authority best placed to know about such risks. In view of these considerations, and given that the underlying information will usually have been gathered in the course of a criminal investigation, it seems evident that the authority in charge of the case file – and consequently, in most continental jurisdictions, a prosecutor or judge – should be tasked with deciding whether to issue threat warnings. In contrast, for essentially the same reasons, FIUs are usually not well placed to issue threat warnings. Most FIUs do not have a comprehensive overview of underlying investigations, which makes them unable to get the complete picture necessary for a comprehensive assessment of a threat, and also less able to see whether the disclosure of information might endanger an investigation. Crucially, the decisions of FIUs are usually not subject to judicial scrutiny in a way that would allow FIUs to adopt highly intrusive measures such as threat warnings, not least because large parts of the analyses that FIUs conduct are based on information that has the quality not of evidence, but of mere intelligence.

[158] III.3.1.1.2.

If, by exception, the warning is issued by an authority other than a judge or prosecutor, that authority must be particularly alert to the possibility that the disclosure of information could adversely affect the work of other domestic and foreign authorities, and it should therefore install internal vetting procedures. In addition, in order to ensure respect for the substantive limits of a warning, the communication between the issuing authority and the recipient obliged entities should then be subject to adequate internal oversight, including a clear assignment of individual responsibilities and the imposition of documentation requirements.

When to issue a threat warning

The issuing of a threat warning should in particular be considered once findings of an ongoing or concluded criminal investigation point to the presence of a financial threat. The decision should be taken on the basis of the available evidence and irrespective of whether the supporting investigation has already led to a criminal conviction. Threat warnings should be available not least in investigations that were prompted by a SAR; insofar as the warning is addressed to the obliged entity that filed the SAR, it would then essentially constitute a form of feedback. Threat warnings should, however, also be available in investigations not prompted by a SAR. If legislators decide that threat warnings may also be issued outside criminal investigations (in particular based on information that is provided by a foreign authority and has no link to domestic criminal investigations), the law should define the authority or authorities responsible for issuing warnings in such cases, and it should also provide the procedure to be followed in such cases, specifying, in particular, rules to ensure that the warnings are based on sufficiently reliable evidence.

Prior hearing or ex post notification

In light of the right to be heard and the right to an effective remedy,[159] particularly stringent standards need to apply if the individuals and entities targeted by a warning are not provided with the opportunity, before the warning is issued, to comment on, and effectively challenge, the allegations that underlie it.

This is because warnings that are not disclosed to the target do effectively give rise to secret blacklists that may have considerable potential for highly damaging abuse. Furthermore, if warnings are not rendered transparent but kept secret, and the underlying allegations are not subject to effective prior challenge, they entail a considerable risk of being based on mistaken factual assumptions. Nevertheless, in some cases a pressing threat may make a warning necessary at a time when the notification of the target would likely compromise the success of an ongoing investigation, notably because the target may then destroy incriminating evidence. In this respect one might consider the example of the infiltration of an obliged entity by an individual

[159] III.3.1.1.4.

closely related to a criminal group, or a threat that tainted actors could employ a particular acquisition to get access to sensitive information. At least if the undisclosed warning is expected to have a considerable impact on targeted individuals or entities, for instance if it would exclude them from basic financial services or make them lose considerable business opportunities, the issuing of that warning should then be subject to a judicial authority that will ensure that the warning's evidentiary basis is thoroughly checked prior to the issuance. Especially if the relevant evidence is the fruit of an ongoing investigation, it would seem evident that the threat warning should be entrusted to the same judicial authority that is also tasked with authorising other secret investigative measures. In any case, in situations in which operational reasons would bar a threat warning from being disclosed for the moment to the target, warnings should be available for use only where, in addition to all other applicable legal conditions being satisfied, (a) the severity of the expected harm indeed makes it urgent for the receiving obliged entity to adopt preventive measures, and (b) at the same time, such measures by themselves (for example the exclusion of the addressee's suspect employee from sensitive information, or the cancellation of a sensitive acquisition) would not be expected to endanger the investigation. Furthermore, to keep to a minimum the restrictions on the rights of targeted individuals and entities, in particular the right to an effective remedy, the issuing authority should notify the target and grant access to the underlying evidence as soon as this is possible without compromising the ongoing investigation. Finally, the issuing authority should also consider that, where the feared endangerment of the investigation would result not directly from the notification, but from the target's access to the underlying evidence, the authorities' operational interest will sometimes be sufficiently safeguarded by temporarily limiting this access.

Issuing of threat warnings outside criminal investigations

The issuing of a threat warning entirely or partly on the basis of information that has been obtained outside a criminal investigation will usually be highly problematic if the target has not been provided with a prior opportunity to challenge the underlying allegations. If information pertaining to financial crime threats was neither gathered under judicial oversight nor opened to prior challenge, the likelihood of factual errors and deliberate abuse here is considerable. Disseminating such information can entail a high risk of severe arbitrary damage to targets' private life or commercial interests. These concerns can be limited if effective safeguards are in place to prevent such consequences, in particular by requiring prior approval from a judicial body or another authority whose decision-making process ensures a high level of scrutiny of the relevant information and respect for the substantive limits applicable to the warning. However, even then, the issuing authority must ensure, in light of the right to an effective remedy, that targeted individuals and entities are notified about the warning as soon as can be done without endangering preponderant interests. In any case, as a permanent concealment of a warning would deprive its targets of an opportunity to effectively challenge

the underlying allegations, a warning must not be issued on the basis of information which can never be disclosed to the targeted individuals or entities, for example due to a confidentiality promise given to another authority. Exemptions from this notification requirement may be provided by exception for cases where the detriment caused by the warning to the target is only minor and is clearly outbalanced by the public interest in keeping the underlying information secret, provided that such exemptions are subject to case-by-case authorisation by a judicial or other independent authority.

Threat warnings against individuals and entities located outside the EU

Particular scrutiny is necessary when a threat warning is addressed to a large number of obliged entities, or is even issued publicly. Such warnings can effectively exclude the target from financial services in the relevant Member State or in the EU altogether. As was already mentioned above,[160] it is unlikely that warnings of such a wide scope of dissemination will ever be proportionate when they concern individuals or entities that are located within the EU. However, such a warning could be proportionate if no Member States' authorities have the ability to take direct action against the source of the threat. Member States' authorities will often lack this ability with regard to actors located outside the EU, especially if they are located in third countries that are known for serious rule-of-law deficiencies and whose authorities are unlikely to enable swift and effective cooperation with their EU counterparts. Given the difficulties that Member States' authorities then confront, limitations on the procedural rights of targeted individuals and companies can be proportionate, not least if the address of the target is unknown or if it is otherwise excessively difficult to provide the target with a hearing before the warning is issued.[161] A prior opportunity to challenge the allegations underlying the warning may thus be dispensable, at least if the target is in hiding or is otherwise evading official communications. Similarly, insofar as the target is or has been subject to criminal proceedings in a third country for the allegations underlying the threat warning, and provided that the target had the opportunity to effectively challenge these allegations, a prior hearing before the issuing authority might be dispensable.[162] In such cases, the issuing of a warning still requires appropriate procedures to avoid arbitrary decisions. However, depending on the severity of the consequences that the warning is expected to have within the EU, a prior judicial approval would not always seem necessary, in particular if the targeted individual or entity currently appears not to hold significant economic interests within the EU or if such economic interests may exist but are hidden. That either the former or the latter is the case may, in the case of a targeted individual, be assumed not least if that targeted individual does not

[160] IV.1.2.1.1.2.

[161] See ECJ (GC), *People's Mojahedin Organization of Iran*, 21 December 2011, C-27/09, para. 67; ECJ (GC), *Kadi and Al Barakaat*, 3 September 2008, C-402/05 P and C-415/05 P, para. 338.

[162] Similarly, ECJ, *LTTE*, 16 October 2014, T-208/11, para. 139.

appear as a beneficial owner in Member States' central bank-account registries or beneficial-ownership registries. In any case, issuing authorities should subsequently undertake reasonable efforts to notify third-country individuals or entities targeted by a threat warning.

Revocation of threat warnings

Finally, given that any interference in fundamental rights must satisfy the necessity requirement, a warning must not be left in force once its substantive requirements are no longer met. If the available evidence indicates that a threat is no longer present, or if the warning is no longer necessary and proportionate, the issuing authority should therefore be required to withdraw the warning. To prevent, so far as reasonably possible, the revoked warning from having effects in the future, and thereby keep it from continuing to produce unnecessary stigmatising consequences, the revocation should be addressed to all addressees of the original warning. A revocation would of course not undo any effect that the warning may already have produced, not least the termination of business relationships, but it would signal to the receiving obliged entities that absent any additional information to the contrary, any individuals or entities mentioned in the warning should not be treated as representing a threat of financial crime. Therefore, as a minimum, the revocation should always include a prohibition for obliged entities to continue using the revoked warning in automated screening, and an obligation to take all necessary steps to ensure that explicit or implicit references to the revoked warning are removed from their screening tools.

As regards the issuing authority, the obligation to revoke unnecessary or disproportionate warnings should be supplemented with an obligation to continuously monitor relevant future developments pertaining to the factual basis of a warning. If the warning was based on findings from a criminal investigation which was still ongoing at the time when the warning was issued, this will usually require the authority to closely follow the outcome of the investigation, and in particular to verify whether the incriminating facts underlying the warning have been confirmed or not. However, given the differences in the nature and objectives of warnings and criminal convictions (namely, respectively, to avert threats and respond to past wrongdoing), the fate of a warning will not necessarily always be the same as that of the criminal investigation from which its supporting evidence came. The issuing authority should therefore consider the possibility that the available evidence can still support the continuing presence of a financial threat even when that same evidence did not suffice to justify the imposition of criminal sanctions.

IV.1.2.1.2. Remedies in Case of Violation of these Conditions

In view of the potentially highly detrimental impact that warnings can have on affected individuals and entities, the law should provide judicial remedies

against the issuing authority.[163] If warnings have been issued by a judicial authority before the targeted individuals or entities had the opportunity to challenge the underlying allegations, those parties should be enabled to challenge the initial judicial decision. Besides being available to the individuals and entities targeted by a warning, these remedies should also be available to individuals and entities that may not themselves be mentioned in the warning, but are closely linked to a target and can demonstrate that the warning may have directly affected them.

Burden of proof

As regards the applicable standard of proof, the issuing authority should be required to establish that the alleged financial threat was present at the time when the warning was issued, and that the warning was then necessary and proportionate. Insofar as the warning has not been revoked, it must furthermore be shown that the threat continues to be present and the warning continues to be necessary and proportionate. In line with the preventive nature of threat warnings, however, the authorities are required to demonstrate not that the individuals or entities mentioned in the warning have committed a crime, but instead merely that objective facts are present that justify the prognosis that, if the receiving obliged entities do business with these individuals or entities, they are indeed likely to be abused by them for purposes of financial crime. To prove this, the issuing authority may for example be required to show that targeted individuals or entities are closely collaborating with a particular criminal group, though it may not be necessary to establish that they are aware of the criminal character of the criminal group, that the collaboration itself is unlawful, or that the targeted parties or the criminal group are planning to abuse the obliged entity with which the targeted parties entered into a business relationship. Similarly, insofar as a warning tells obliged entities that particular individuals or entities may try (openly or under the disguise of a yet-unknown front company) to infiltrate a commercial sector in a particular region through the acquisition of businesses, the threat will usually be established by presenting evidence that these individuals or entities are pursuing a corresponding criminal strategy. However, to prove that threat, it will generally not be necessary to present evidence on when and by whom a decision was taken to pursue this criminal strategy, nor on whether the particular funds used for any acquisition of businesses are derived from criminal activity, nor on whether acquired businesses are themselves meant to engage in criminal activity.

Burden of proof regarding situations outside the EU

Insofar as the warning targets individuals and entities that are located in third countries, the law should however consider the difficulties Member States' competent authorities may encounter in gathering relevant evidence, especially in situations where the threat emanates from individuals or entities operating in a third country that suffers from instability and widespread violence, and

[163] III.3.1.2.2.

where local authorities may be unable or unwilling to support Member States in their efforts to address the threat. In such cases, courts might build by analogy on the jurisprudence of the ECJ in the area of measures adopted as part of the EU's Common Foreign and Security Policy, which allows for a nuanced distribution of the burden of proof.[164] If these evidentiary standards are applied to threat warnings pertaining to individuals and entities located in places where Member States' authorities cannot count on the cooperation of the local authorities, it may then suffice that the issuing authority provide evidence establishing that the individuals or entities in question do indeed closely interact with a particular criminal group. If these individuals or entities then seek redress against the warning, they may be asked to provide a plausible explanation why the evidence offered by the issuing authority was unreliable, or why a proven collaboration with the criminal group would nevertheless not constitute a financial crime threat to the obliged entities addressed by the warning.

IV.1.2.2. The Processing of Information by Obliged Entities

IV.1.2.2.1. Obligations of the Obliged Entities

Primary obligations resulting from the warning

In general, threat warnings do leave it up to the obliged entity how to respond to protect itself against the threat. If the obliged entity has already entered into a business or employment relationship with the individual or entity responsible for the threat, discontinuing the relationship will obviously be the easiest and most effective way to disrupt the threat. Sometimes, and especially if the obliged entity is exposed to the source of the threat only indirectly (for example when it learns that a bona fide corporate customer is exposed to criminal influence), it may suffice to subject customers linked to the threat to enhanced CDD measures. In any case, if the obliged entity does not discontinue its relationship with a given customer linked to the threat, it must treat that customer as constituting a high risk, and CDD measures must be adequate to this effect. Insofar as the obliged entity has not yet come into contact with the individual or entity named in the warning, it will usually have to screen prospective customers and prospective employees in order to protect itself.

Purpose limitation regarding the information contained in the warning

Given that the risk of unintended curtailments of rights depends to a great extent on the scope of a threat warning's dissemination, the proportionality of a warning will be partially determined by how effectively the addressees of the warning are able to prevent the warning from being used for purposes other than to repel the threat.[165] To this effect, as a rule any threat warning should be subject to a strict purpose limitation. Given that warnings are meant to serve

[164] See ECJ (GC), *Anbouba* 21 April 2015, C-630/13 P, para. 47; ECJ, *Bredenkamp et al*., 21 July 2016, T-66/14, para. 72.

[165] III.3.2.1.

the specific purpose of protecting obliged entities from particular threats, in general any use of the information contained in warnings for other purposes should be unlawful. When processing a warning, obliged entities should therefore not be allowed to adopt detrimental measures against individuals or entities (such as the discontinuation of a business relationship, or an increase in fees to compensate for higher CDD costs) unless there are at least reasonable grounds to assume that these parties are linked to the specific threat.

Two challenges, however, attend the enforcement of the prohibition on using warnings for unauthorised purposes and the consequent prohibition on adopting detrimental measures against actors insufficiently linked to the threat. First, it can be difficult in practice to limit the spread of the warning, as the warning might become accessible to numerous employees of the obliged entity, in which case there would be an increased risk that information may get into the wrong hands. Second, the boundaries of the purpose limitation can sometimes be blurred, not least of all if the content of a threat warning is used to calibrate the obliged entity's customer screening. In such cases, warnings can lead to an extensive de-risking of customers who in fact may be in no way related to the threat, but are somehow similar to the individuals or entities mentioned in the warning, for example in that they share the same national origin and business activity. In view of these challenges, threat warnings should always be accompanied by effective safeguards to prevent the unauthorised dissemination, as well as the unauthorised use, of the information disclosed by the public authorities.

Safeguards to prevent unauthorised dissemination

To prevent an unauthorised spread of threat warnings within obliged entities and thereby safeguard the warnings' proportionality, serious confidentiality breaches should be subject to criminal or other effective sanctions against the employees responsible, and in the event of systemic failings, also against the obliged entity itself. As importantly, legislators should require the creation of internal mechanisms to reduce the risk that warnings may be leaked or otherwise misused. One such mechanism might consist in an obliged entity's maintaining a central contact person to whom all threat warnings are addressed, and who then decides with which colleagues each warning should be shared internally. Other possible mechanisms include limits on how much information is shared internally, for instance a requirement that, in every obliged entity, any decision about the future treatment of a business relationship linked to a specific threat disclosed in a warning must be made exclusively within the compliance unit, and that the compliance unit must make such decisions without disclosing the underlying reasons to the customer desk that manages the relationship in question. In any case, sharing a warning with other obliged entities inside or outside a group of companies should generally be authorised only if this is strictly necessary to counter the specific threat, provided that the

resulting wider scope of the warning's dissemination is then still proportionate to the gravity of the threat.

Safeguards to ensure respect for purpose limitations

To prevent warnings from being used for illegitimate purposes, warnings should define, in each case, how the recipient obliged entities are allowed to process the information contained in them. In any case, the information contained in a warning should be used for the exclusive purpose of protecting the recipient obliged entity against the particular threat described in the warning. The issuing authority could also be required to specify in greater detail exactly how the recipient obliged entities are expected to process the information, for example whether or how the information should be used in screening customers, and whether the recipient obliged entities are allowed to forward the warning to third parties tasked with the performance of CDD measures.

Crucially, obliged entities should be required to implement mechanisms to minimise the risk that warnings will be implemented arbitrarily. Where warnings pertain to threats that go beyond a particular existing business relationship or a particular transaction, obliged entities will necessarily be expected to screen their customers for possible links with the individuals and entities that the authorities identified as tainted. In order to keep warnings from leading to unjustified stigmatisation, however, obliged entities could be required to ensure that the information contained in a threat warning is not fed into their regular CDD screening process, but is instead used as a separate screening filter whose content is accessible only to a very limited number of compliance officers. This could ensure that information that may entail a risk of illegitimate discrimination – for example the national background of a particular criminal group mentioned in a warning – does not become a parameter in obliged entities' general customer screening. Only this small group of compliance officers would have access to the content of the additional screening filter, and should then flag a particular customer to their colleagues if, and only if, there are reasonable grounds to assume that the customer is in fact related to the threat. Such a separation between obliged entities' general CDD screening parameters (which can contain red flags from all sorts of sources) on one hand and warning-induced CDD screening parameters on the other hand could ensure that customers are not de-risked on the basis of vague links with the warnings. More specifically, this separation between general CDD and the processing of warnings would provide the issuing authorities with greater confidence that any sensitive information they communicate through a warning will not lead to detrimental consequences for customers who merely share some characteristics with individuals and entities mentioned in the warning and whose link to a particular threat is not substantiated by significant additional considerations.

IV.1.2.2.2. Remedies in Case of Violation of these Conditions

As already explained, the proportionality of warnings is closely connected to how they are processed by obliged entities. Legislation therefore needs to provide remedies to address obliged entities' breaches of the applicable substantive limitations.[166] Two primary concerns stand out in this regard. First, the personal data and other sensitive information contained in warnings might be unlawfully shared within the receiving obliged entity or with third parties. Second, warnings might be applied in an excessive way – that is, an obliged entity might respond to a warning by discontinuing a business relationship with an individual or entity, or adopting other adverse measures against them, when there are no reasonable grounds to assume they are linked to the threat.

Remedies against the unlawful dissemination of information

If there are reasons to suspect that a warning was unlawfully shared by employees of a recipient obliged entity, any individual who has been targeted by the warning already has a right, under Articles 77 and 78 of Regulation (EU) 2016/679, to lodge a complaint with a supervisory authority and seek judicial redress against this authority's decision. However, legislators will need to carefully assess whether the relevant supervisory instruments are effective enough to uncover unlawful processing of warnings within obliged entities. To ensure in particular that unlawful disclosures of warnings inside and outside obliged entities are effectively investigated, legislators should ensure that such conduct is covered by criminal offences pertaining to the violation of personal or professional confidentiality, and that, where specific facts give rise to a relevant suspicion, such a suspicion is duly investigated by the criminal-justice authorities.

Furthermore, given that the unlawful processing of warnings, in particular their widespread disclosure to third parties outside the addressed obliged entity, can have highly detrimental consequences for legal entities as well, legislation should ensure that legal entities which are targeted by warnings likewise have a right, in case of a relevant suspicion, to lodge a complaint with a supervisory authority and have their complaint effectively handled by that authority.

Remedies against excessive implementation of threat warnings

Legislators should clarify that the remedies under Regulation 2016/679, in addition to applying to the unauthorised dissemination of threat warnings, apply also to the excessive, and thus unauthorised, application of threat warnings. These remedies, where applied to the excessive application of threat warnings, should be available not only to the individual or entity that was targeted by a warning, but also to individuals and entities that, although not targeted by a given warning, are subjected to adverse measures by an obliged entity, if there are reasons to suspect that these measures are the consequence of the obliged entity's excessive and thus unauthorised use of that warning. This would be the

[166] III.3.2.2.

case for example if an obliged entity discontinues a business relationship with a family member of the person targeted by a warning when there are no objective grounds to assume that this family member would abuse the obliged entity for financial crime. Given obliged entities' contractual freedom, it will usually be inadequate to require an obliged entity to continue a business relationship, but legislators should still provide for remedies to sanction such cases of the unauthorised use of warnings, through complaints to a supervisory authority and, where appropriate, sanctions against the obliged entity. In many cases, however, it will be difficult to demonstrate that the warning is causally linked to the adverse measures adopted by the obliged entity, especially if the warning may have been unlawfully shared with staff at the obliged entity who were not entitled to have knowledge of the warning. For remedies against excessive implementation of warnings to be effective, the law could therefore stipulate a presumption that the adverse measures were indeed caused by a warning when there are strong reasons to assume so, while also enabling the obliged entity to rebut this presumption by presenting persuasive grounds to the supervisory authority that the adverse measures were in fact due to a different reason.

Remedies against the unlawful rejection or discontinuation of basic payment accounts

Member States are already under an obligation to require credit institutions, where they reject a payment account with basic features within the meaning of Directive 2014/92/EU, to "advise the consumer of the procedure to submit a complaint against the refusal, and of the consumer's right to contact the relevant competent authority and designated alternative dispute resolution body".[167] Such a contract may be terminated only on the basis of a limitative list of justifications provided in Directive 2014/92.[168] Legislation should clarify that such remedies apply in particular when the rejection or discontinuation of a basic payment account may result from an excessive application of a threat warning, and clarify that a person subject to a threat warning cannot be considered to have "deliberately used the payment account for illegal purposes". [169] The remedies should be granted to individuals who are themselves targeted by a warning, if the warning has been revoked by the issuing authority; furthermore these remedies should also be available to other individuals when there are reasons to suspect that their basic payment account was rejected or discontinued due to their proximity (for example as family members or business partners) to an individual or entity targeted by a warning, provided that either the warning has been revoked or they claim there are no reasonable grounds to assume that they too constitute a threat. To ensure effectiveness of these remedies, legislation should also clarify that the

[167] Art. 16 para. 7 s. 2 of Directive 2014/92/EU.

[168] Art. 19 para. 2 of Directive 2014/92/EU.

[169] See Art. 19 para. 2 a) of Directive 2014/92/EU.

decisions of the credit institution and of the relevant authority, or if applicable the latter's failure to act, can be challenged in the courts.

IV.1.3. Risk Notifications

Risk notifications are meant to notify one or more obliged entities that a particular situation entails a high risk of financial crime and should therefore be subject to additional CDD measures. Particular situations in this sense can be specific business relationships or particular transactions, but also any as-yet unspecified business relationship or transaction that is marked by particular features (such as a link to a particular IP or postal address, or to particular individuals or particular entities). Accordingly, a risk notification must be specific enough to enable the recipient obliged entities to identify specific past or future business relationships or transactions.

As regards the level of risk required for the issuing of a risk notification, the specific situation in question must give indications, on the basis of reasonable risk-assessment standards, that it requires particular scrutiny from an AML/CFT perspective. Beyond this basic meaning, risk notifications can, as a general rule, refer to various levels of enhanced risk. Depending on the level of risk of the particular case, the extent of additional CDD measures required from obliged entities will vary. Risk notifications may of course in particular refer to cases where the crime risk is especially high, for example when the authorities have information that assets originate from a third-country entity with a history of money laundering. But risk notifications may also refer to situations where the relevant risk is simply substantial enough to require more than standard CDD measures, for example when a particular individual has opened a large number of bank accounts in a short period of time with no apparent lawful reason, or when the authorities have information that a local business with no significant international operations received investments through a chain of companies domiciled in various overseas tax havens without there being any plausible explanation for such complex arrangements.

On the basis of the necessity and proportionality considerations described above, legislators must define the substantive conditions and procedural safeguards for risk notifications. To this end, one should first define rules governing the issuing of risk notifications, then define rules for the processing of notifications by the obliged entities.

IV.1.3.1. The Transfer of Information from Public Authorities to Obliged Entities

IV.1.3.1.1. Conditions

IV.1.3.1.1.1. Necessity

The assessment of the necessity of a risk notification has to be based on objective criteria pertaining to the magnitude of the risk, the actual suitability of the risk notification to improve obliged entities' CDD, and the absence of less intrusive alternative measures; these considerations also require a careful

determination of the necessary scope of dissemination of the risk notification.[170]

The magnitude of the risk

Indicia of a high risk of financial crime, such as the use of complex opaque investment arrangements, will usually not allow the authorities to have a clear idea of what type of crime, if any, may be behind the signs, for example whether a business is being used for perfectly legal purposes, or is being used by a single individual to commit tax evasion, or is being used by a transnational criminal organisation to launder the proceeds of serious criminality. Consequently, the necessity of a risk notification cannot usually be determined by examining the seriousness of a possible crime in question. In any case, a risk notification must always be based on reliable information which justifies the conclusion that the situation in question must be assessed as high risk, and which at the same time justifies the expectation that the notification will improve the recipient obliged entities' ability to avert or detect financial crime. Not least in view of the need not to arbitrarily discriminate between customers, the nature of the risk in question must justify why the issuing authority singles out some business relationships and transactions, and not others. Accordingly, although risk notifications may, as a general rule, refer to situations of various degrees of higher risk, the imperative to avoid arbitrary notifications will usually strongly militate in favour of issuing risk notifications mainly in cases where the authority believes a financial crime risk is particularly high.

The actual effectiveness of risk notifications for improving the quality of CDD

To be necessary, risk notifications must not only concern situations that have been found by the issuing authority through a reasonable risk assessment to constitute high financial crime risk, but must also, among other things, be actually suitable to improve CDD. It is here that risk notifications can prove to be particularly problematic. For when an authority labels a particular business relationship or a particular transaction as constituting a high financial crime risk, obliged entities receiving that information will regularly lose interest in continuing to serve the affected customer in the first place. After all, keeping a high-risk customer usually entails the need to implement additional CDD measures, which implies the use of additional resources. If legislators allow risk notifications to be issued, they must therefore provide for safeguards to ensure that such notifications do in fact cause recipient obliged entities to thoroughly analyse the high-risk situation in question, and not to simply de-risk the affected customer. If risk notifications would primarily cause recipient obliged entities to offboard affected customers or adopt similar adverse measures (such as raising fees), and not to provide meaningful help in the disruption of financial crime, they would fail their purpose, meaning that they would not be necessary.

The absence of less intrusive, equally effective alternatives

[170] III.3.1.1.2.

By guiding obliged entities in their performance of CDD, risk notifications ultimately serve the purpose of facilitating the detection and disruption of as-yet unknown instances of financial crime. To pursue this purpose effectively, the issuing of a risk notification may be necessary – namely, where alternative means to detect the criminal conduct in question would be less promising or more intrusive. In particular, authorities will usually lack access to the relevant financial data and therefore cannot analyse it on their own. Insofar as it is possible to verify the risk (such as the possible criminal involvement of a particular customer) by investigative measures (in particular through covert surveillance), these measures will usually be more intrusive and will possibly even be less effective than a financial analysis by obliged entities. Alternatively, one could conceive of tasking the FIU with analysing the business relationship or transaction concerned, but this would usually require the transfer of vast amounts of data from obliged entities to the FIU; and even then, this analysis would still likely be less effective than an analysis by obliged entities themselves, because the latter will usually be able to include in their analysis vast amounts of customer and transaction data that is not directly related to the relevant business relationship or transaction.

Scope of dissemination

The competent authority will furthermore need to determine to what extent it is strictly necessary to disseminate a risk notification to multiple obliged entities. Insofar as the risk relates to a particular business relationship, the notification will be addressed only to one single obliged entity. Determining the scope of dissemination of the notification can however be more difficult when the risk relates to a situation that may involve numerous still-unidentified obliged entities – for example when the appearance of a particular name or particular IP address is taken to signal an enhanced risk. In such cases, the scope of dissemination will primarily depend on the extent to which the dissemination is proportionate *stricto sensu*.

Necessity considerations finally also apply to limitations on the level of detail that a notification provides about the risk in question. As a minimum, a notification must enable the recipient obliged entities to identify the particular situation that the issuing authority considers to constitute a risk. A notification may thus for example point an obliged entity to a particular customer account, a particular transaction, or a particular address. In order to ensure an effective follow-up by the obliged entity, it may be desirable, depending on the nature of the risk, to provide the obliged entity with additional information, in particular by explaining in some detail why the particular situation is considered a risk. In such a case, however, the authority should first inquire whether the disclosure of sensitive background information to the obliged entity can be avoided by an alternative framing. Instead of disclosing that a particular customer may be involved in criminal activity with a criminal group from a specific country, for example, the authority could alternatively just ask the obliged entity, without disclosing to the entity this customer's possible link to a criminal group, to

scrutinise the customer's transactions linked to the relevant country. If the provision of additional, potentially stigmatising information is still considered necessary, the authority must then assess whether such a disclosure would also be proportionate *stricto sensu*.

IV.1.3.1.1.2. Proportionality Stricto Sensu of Interference in the Rights of Customers

The proportionality *stricto sensu* of risk notifications essentially depends on a balancing of, on the one hand, the magnitude of the respective risk and the actual suitability of the notification to improve obliged entities' CDD in view of that risk, and, on the other hand, the gravity of the detrimental consequences that the notification may cause. Thus it is key to assess the gravity of the expected or likely detrimental consequences that a risk notification may cause to affected customers, and therefore authorities must identify the actual impact of such consequences, with particular regard to the scope of dissemination of the notification and the sensitivity of its content.[171]

The nature of interference in the rights of customers

Legislators need to give consideration to any unintended detrimental consequences that notifications may cause. In particular, even if the obliged entity that receives a risk notification does not find reasons to suspect that the high-risk situation to which the notification refers is linked to crime, it will nevertheless often be inclined to discontinue affected business relationships, so as to avoid additional compliance costs and the risk of supervisory sanctions. Obviously, obliged entities are usually free to decide whether or not to continue providing services to a particular customer, and they are therefore usually also free to implement risk-mitigation measures (such as raising fees to compensate for higher compliance costs). Nevertheless, insofar as de-risking or other adverse measures are a response to the information that an authority has provided to an obliged entity, such measures are the consequence not only of the obliged entity's freedom of contract, but also and possibly even primarily of the authority's intervention. Authorities must therefore ensure that they have a good understanding of the adverse measures that receiving obliged entities may adopt due to an envisaged risk notification, in particular the extent to which the risk notification may impede affected customers' access to financial services or make them lose business opportunities.

Scope of dissemination

Given that risk notifications may cause de-risking or other adverse measures that are not based on a thorough assessment of the risk posed by the affected customer in question, the scope of dissemination of risk notifications will be important for assessing their proportionality. The more widely a notification is disseminated among obliged entities and their employees, the more likely it is

[171] III.3.1.1.3.1.

that the issuing authority will lose control over exactly how the receiving obliged entities process the notification.

In this regard, an interference in the rights of customers will be least pronounced if a notification is addressed to only one particular obliged entity, or a small number of obliged entities, and targets only one particular business relationship or transaction. Similarly, the intrusiveness of a notification can sometimes be rather limited even if the notification is addressed to a large number of obliged entities, if it does not target particular customers – for example if, without naming specific individuals or entities, it merely highlights IP addresses that have surfaced in past financial crime investigations.

In contrast, if risk notifications point to specific individuals or entities, a widespread dissemination – that is, a dissemination among a large number of obliged entities – would usually be disproportionate, given that it may lead to a broad stigmatisation. In cases where the risk notification refers to a specific serious risk, for example that a particular customer may be involved in a transnational financial crime network, a dissemination of the notification among a large number of obliged entities may sometimes still be acceptable, in light of the public interest at stake, even if the issuing authority cannot exclude that some of the receiving obliged entities will implement adverse measures against affected customers without first adequately scrutinising the particular business relationships involved. However, in that case the issuing authority must carefully assess the concrete impact that some obliged entities' adoption of such premature adverse measures would likely have on the affected customers, particularly to what extent these measures would significantly reduce those customers' ability to access financial services. An envisaged risk notification that would likely have this or a comparable effect should be deemed disproportionate, bearing in mind that at this point it is speculative whether the customer targeted by the notification is in fact involved in financial crime.

Sensitivity of the information contained in the notification

The proportionality *stricto sensu* of a risk notification finally also depends on the nature of the information it contains. If the notification must necessarily contain potentially stigmatising details about the nature of the risk (for example that the issuing authority believes that a particular customer may be linked to a criminal group from a specific country, thereby inviting the addressed obliged entity to scrutinise any possible links to this group), proportionality will largely depend on whether this information is in fact likely to have a stigmatising effect. The more stigmatising information a notification contains, the greater, in principle, the likelihood that it will produce unintended consequences to the detriment of affected individuals and companies. The more widely a notification with potentially stigmatising assertions is shared, the more one must realistically expect that this information will also be used for purposes other than to enhance CDD, and, accordingly, that the information will lead to blacklisting or similar blanket adverse measures against affected customers.

As a consequence, insofar as it is absolutely necessary for a risk notification to contain background information about criminal activities that may be linked to a particular customer, that notification should not be communicated to more than a small number of obliged entities at most, and effective measures should be put in place to prevent the information from being used for purposes other than improving the quality of CDD.

IV.1.3.1.1.3. Proportionality of Interference in the Rights of Obliged Entities

Risk notifications are meant to serve obliged entities by strengthening their risk detection capacity. As such, the issuing of a notification in itself does not entail an interference in the rights of the receiving obliged entity. This is so at least if the notification is issued in response to the obliged entity's request to authorities for an assessment of the risk of a particular business relationship, or if the obliged entity is voluntarily participating in a cooperation mechanism and receives the notification as part of this mechanism. Yet an interference in an obliged entity's freedom to conduct a business according to Article 16 of the Charter of Fundamental Rights will arise if legislation imposes an obligation on obliged entities, in certain situations, to receive and process risk notifications while at the same time complying with limitations on their freedom of contract. It must then be asked whether, in such cases, the resulting interference is proportionate in this respect as well.[172] Legislators must take this question into account in designing the aforementioned obligation, while the issuing authority must ask this question when it considers issuing a risk notification to which this obligation applies. To this end, legislators and the issuing authority must in particular consider the weight of the interference (for example, in the case of the issuing authority, to what extent the aforementioned obligation would temporarily prevent the obliged entity in question from discontinuing business relationships affected by the envisioned notification) and the public interest in strengthening the effectiveness of obliged entities' risk management.

IV.1.3.1.1.4. Procedural Requirements

Issuing authority

As risk notifications serve the aim of helping obliged entities to improve their CDD, competence for their issuing should lie with those authorities whose task is to sustain the AML/CFT regulatory framework. Furthermore, given that the identification of financial crime risks requires an assessment of specific financial transactions, and consequently often access to investigative findings and related intelligence, FIUs are best placed to be in charge of issuing risk notifications. Unlike a supervisory assessment of the adequacy of particular compliance measures, risk notifications are primarily meant not to define abstract legal standards, but to enrich the obliged entity's risk assessment by providing relevant case-specific findings.

[172] III.3.1.1.3.2.

In contrast, usually the issuing of risk notifications should not fall under the responsibility of police or other investigative authorities. These authorities will of course often have relevant information that could help obliged entities to calibrate their CDD. However, asking investigative authorities to issue risk notifications would task them with getting deeply involved in the regulatory framework and thereby likely lead to unhelpful overlaps with FIUs and supervisory authorities.

Legislators should keep in mind, however, that the regular interaction that occurs between investigative authorities and obliged entities (by way of, among other things, prosecutors' production orders) will frequently have effects similar to a risk notification, especially prompting additional CDD measures or de-risking. For when investigators approach an obliged entity and thereby disclose that a particular customer is the suspect in a criminal investigation, the obliged entity will often respond by treating this customer with caution and even discontinuing the business relationship. Given that customers are thereby oftentimes subjected to adverse measures by obliged entities even though the latter have no sound understanding of the underlying suspicion, legislation should pay more attention to this phenomenon and provide clearer rules that harness the preventive potential of criminal investigations while providing safeguards against excessive de-risking.

Possible triggers of a risk notification

Given that the aim of risk notifications is to improve the effectiveness of CDD and at the same time support obliged entities' CDD efforts, the issuing of risk notifications should be possible both at the initiative of the authority and, alternatively, at the request of obliged entities. Though the authority should as a rule enjoy discretion, legislators should additionally consider the possibility of granting obliged entities a right, under specific conditions, to request a decision whether a specific situation should be treated as high-risk. Furthermore, though risk notification should primarily build on a voluntary commitment of obliged entities to comply with the processing conditions set by the issuing authority, legislators might consider defining situations in which an obliged entity could be obliged to receive and process risk notifications in line with specific instructions.

Discretion to issue risk notifications

The discretionary issuing of risk notifications might be done at the initiative of the competent authority – which, as stated above, should usually be the FIU – or at the request of an obliged entity. Risk notifications may in particular serve as feedback to the filing of a SAR, but in general can also be issued or requested independently of a prior SAR, for example when the FIU wants to alert an obliged entity to upcoming high-risk situations. Importantly, given that risk notifications are supposed to help obliged entities accurately understand the actual risk of a particular situation (and are thus not limited to an abstract legal assessment), a risk notification may be issued only once the issuing authority possesses

sufficient information to allow for a meaningful assessment of the actual situation. Risk notifications will therefore usually require a prior operational analysis by the FIU, or information that the FIU has received from another authority, which clearly substantiates the high-risk nature of the situation. Of course, given the large number of high-risk situations in the market, and also because of the procedural requirements that need to be respected, FIUs will likely be unable to issue a risk notification in every situation that offers appropriate substantive conditions. As FIUs are thus forced to limit the number of relevant situations where a risk notification is issued, legislation should define criteria in order to prevent an undue preferential treatment of some obliged entities and discrimination against certain customers. Following a risk-based approach, particular regard should be given to the volume of the sums in question, to the seriousness of the underlying criminality (insofar as discernible), and to whether the obliged entities that may be affected by the situation in question belong to a sector or practise a type of business that is especially vulnerable to criminal exploitation.

A right of obliged entities to receive a risk assessment of a particular business relationship

Legislators may also consider defining conditions under which obliged entities may, by exception, be entitled to have the FIU or competent supervisory authority decide whether a particular situation should be treated as constituting an enhanced risk. This possibility could be considered notably for cases in which an obliged entity has repeatedly, in good faith and over a longer period of time, reported a particular business relationship without any feedback from the FIU or from investigative authorities. Under such circumstances, the FIU, potentially in coordination with the supervisory authority, could be expected to decide whether, in the absence of major changes in the underlying facts, the obliged entity should continue to treat the reported situation as entailing a high risk.

Mandatory participation in a risk notification mechanism

Legislators should finally also consider whether, under certain conditions, an obliged entity may be required to receive and process risk notifications in line with specific instructions from the FIU or other issuing authority. Participation in a mechanism to this effect may be required in particular if the FIU's findings indicate that the obliged entity is particularly exposed to criminal abuse at a given moment, or if, according to the competent supervisory authority, it suffers from severe structural failings of its AML/CFT compliance.

Procedures to limit unintended consequences

To ensure that risk notifications are based on reliable information and a sound risk assessment, and that the confidentiality of information is adequately protected, the issuing authority should have internal procedures in place to

ensure that the notifications are vetted before being communicated to an obliged entity.

Crucially, procedures are also needed to ensure that risk notifications serve exclusively as an instrument to initiate additional CDD measures, i.e. that they have no direct effect other than causing the obliged entity to pay particular attention to specific high-risk situations. In contrast, these notifications must not be allowed to be issued with the purpose of inducing de-risking or other adverse measures against particular individuals or entities; if the authorities want to induce de-risking, they must instead rely on the threat warnings explained above,[173] which require legal safeguards that are significantly more demanding than those required in the case of a mere risk notification.

Consequently, legislation must ensure that risk notifications do not quasi-automatically trigger de-risking or similar adverse measures (such as an increase in fees). Procedures should therefore be put in place that enable the FIU and the competent supervisory authority to effectively oversee how the obliged entity deals with any risk notification. This could for example be done by appointing contact persons, duly vetted for security, within obliged entities to be responsible for ensuring the appropriate handling of risk notifications and for reporting back to the FIU or the competent supervisory authority, for a certain period of time after a notification is received, on how the obliged entity deals with business relationships affected by that notification. Following the issuing of a risk notification, the FIU or the competent supervisory authority should verify whether the recipient obliged entities are implementing adequate additional CDD measures with regard to affected business relationships, and that any adverse measures that an obliged entity adopts against an affected customer after receiving the notification are essentially the result of the obliged entity's own CDD findings and are not inappropriate in this regard.

To keep risk notifications from leading to stigmatisation of affected customers, any mechanism that facilitates the handling of risk notifications should furthermore provide effective safeguards against a loss of sensitive information and against any unlawful processing of information. To process complex cases, legislation could also provide for mechanisms in which representatives from the issuing authority (and possibly other authorities) and obliged entities interact in a single location where the obliged entities' representatives also receive background information about the high-risk situations in question. On the basis of this information, the obliged entities' representatives would then be able to provide compliance officers at their own organisation with specific guidance on what additional information to demand from a particular customer and what other additional information to procure in order to better understand a particular business relationship. By preventing the obliged entity's representative from copying sensitive information or taking notes about particular background information, such a mechanism could allow

[173] IV.1.2.

for a more robust protection against information leaks and against the unlawful processing of information.

Documentation

Though risk notifications will usually entail a considerably less intrusive interference in the rights of affected individuals and entities than the above-described threat warnings, they can still lead to significant detrimental consequences, not least the loss of business opportunities. The law should therefore provide adequate oversight over how they are issued. In this respect, one must note that the ultimate purpose of risk notifications, namely the disruption of financial crime, would usually be undermined if affected customers were to be informed about a risk notification either before or soon after it was issued. It is therefore important for risk notifications to be comprehensively documented so that they can be scrutinised, at least at a later stage. This could in particular be done by requiring the issuing authority to document all risk notifications and their full content in an electronic database which can be accessed later on by competent oversight bodies, in particular by the supervisory authority responsible for overseeing the issuing authority's processing of personal data. In any case, the law should provide effective safeguards to prevent potentially stigmatising information from being communicated to obliged entities without full documentation of that communication. To ensure accountability and public trust in the cooperation between the issuing authority and the private sector, it should always be documented who communicated what to whom. Where legislation provides for cooperation between the issuing authority (and other authorities, as the case may be) and obliged entities within a closed location, the communication within that space should also be documented (for example by an audio-video recording of the interaction of participants), and participants should generally be prohibited from communicating about the content of risk notifications outside the formalised and documented communication channels.

Notification of affected customers

Finally, given that risk notifications – whether they refer to a specific customer or not – are geared to result in the singling out of a particular customer or particular customers within obliged entities' CDD, and thus to a particularly intrusive processing of customer data at the instigation of the authorities, affected customers, at least insofar as they are natural persons, should be informed that a risk notification that has affected them was issued, once informing them is no longer likely to endanger an ongoing criminal investigation or another preponderant interest. There may be cases in which informing an affected customer is permanently precluded – a scenario in which the affected person is usually completely inhibited from seeking effective redress against the risk notification. Legislation should therefore provide for an ex officio review of the legality of the risk notification in all such cases by an independent organ, for example by the competent data protection supervisor or a judge.

IV.1.3.1.2. Remedies in Case of Violation of these Conditions

IV.1.3.1.2.1. Remedies for the Obliged Entities

If an obliged entity is put under a legal duty to receive and process risk notifications in line with instructions from the authorities, it should be able to challenge this measure in court.[174] This opportunity is meant to address those cases in particular where a risk notification is unwarranted (because the situation in question does not in fact entail an enhanced risk) or where a risk notification is combined with arbitrary or excessive additional obligations on the obliged entity, notably with limitations on its contractual freedom.

IV.1.3.1.2.2. Remedies for Targeted Customers

Legislators should clarify that the remedies under Directive 2016/680 or, where applicable, under Regulation 2016/679, should be available to individuals who were individually targeted by a risk notification.[175] Accordingly, such individuals should have a right to an effective judicial remedy against the issuing authority. Further oversight should be provided by the supervisory authority tasked with supervising the processing of personal data by the issuing authority. Targeted individuals should also be entitled to lodge a complaint with this supervisory authority, if they claim that a risk notification was based on erroneous facts or otherwise issued unlawfully, and furthermore to have an effective judicial remedy against this authority.

To ensure effectiveness of the remedies based on data protection law, the law of Member States should ensure that the competent supervisory authority and the competent judicial bodies have access to the content of all risk notifications even when paramount confidentiality concerns make it necessary to deny the affected person access to the notification. Furthermore, legislators should provide that legal entities will also have effective remedies against the issuing of a risk notification, as they are usually not covered by the remedies provided under data protection law.

IV.1.3.2. The Processing of Information by Obliged Entities

IV.1.3.2.1. Obligations of the Obliged Entities

Ensuring respect for purpose limitations

Risk notifications require the receiving obliged entity to subject the relevant business relationships and transactions to additional CDD measures that are adequate to the gravity of the risk. But they do not entail a demand for the obliged entity to discontinue such relationships or abstain from such transactions. To safeguard the proportionality of notifications, legislation must first and foremost ensure that the notifications do in fact serve the purpose of causing the receiving obliged entity to subject the relevant business relationships and transactions to additional CDD measures that are adequate

[174] III.3.1.2.1.

[175] III.3.1.2.2.

to the gravity of the risk. Obliged entities should therefore be under a strict obligation to process the information contained in risk notifications only to refine their CDD regarding the relevant business relationships and transactions, and not for other purposes. To this end, risk notifications should furthermore not be made accessible to more employees of the obliged entity than is strictly necessary in order to clear up the high-risk business relationships and transactions in question. To forestall an unnecessary dissemination of risk notifications within the obliged entity, the law should require mechanisms that would limit knowledge of the particular content of the risk notification to only a small number of the obliged entity's compliance officers, who would serve as the direct addressees of the notification and who would be expected, on the basis of information contained in the notification, to guide the implementation of compliance measures without telling their colleagues where the information comes from or any details of the notification. In any case, the unlawful disclosure of risk notifications to third parties should be subject to effective sanctions against the responsible employees and, where appropriate, against the obliged entity.

Limitations on de-risking and other adverse measures

Insofar as limitations on de-risking and other adverse measures are concerned, any mechanism for the facilitation of risk notifications must essentially reflect a fair balance between the obliged entity's interests in avoiding unnecessary risk, and the customers' interests in not being subject to risk-mitigating measures that do not reflect their actual risk profile. To this effect, legislation must always take proper account of obliged entities' freedom of contract, but at the same time recognise that risk notifications also serve those entities' own interest in being protected from criminal abuse. To keep risk notifications from automatically leading to de-risking or other adverse measures, legislation must clarify that a notification must never by itself cause adverse measures by obliged entities, but may only prompt additional CDD, and that adverse measures against an affected customer may be taken only on the basis of findings obtained through CDD. As already explained, risk notifications are not necessarily confined to cases of voluntary cooperation between authorities and obliged entities, but may also be designed as mandatory instruments, in the sense that the obliged entity is legally required to receive and process notifications. To safeguard proportionality, the aforementioned limitation on the treatment of customers affected by a risk notification must also apply in this case.

Especially if risk notifications are to be issued as part of a cooperation mechanism in which obliged entities are participating voluntarily, these entities should be expected to commit to a self-limitation on how they practise de-risking and similar adverse measures in connection with a notification. In any case, obliged entities cannot be expected to abstain from such measures if additional CDD measures implemented due to a risk notification establish a suspicion, substantiated by meaningful facts, that the affected customer is

indeed involved in financial crime. Legislation should however provide limits for the case when a risk notification is issued but the obliged entity does not establish such a suspicion. Despite the lack of a suspicion, the obliged entity may then still be inclined to discontinue the affected business relationship or to adopt other adverse measures against the affected customer simply because the customer was labelled a high risk by an authority. Of course, except in very limited circumstances (notably in the case of basic payment accounts), the law cannot require obliged entities to permanently continue a business relationship against their will. However, insofar as they receive a risk notification, obliged entities might be expected to at least temporarily continue a business relationship affected by the notification, and to verify, over an adequate period, whether de-risking or other adverse consequences are really called for. Such a waiting period would serve as a precaution to keep customers from being subjected to adverse measures without first having been thoroughly scrutinised by the obliged entity. If the obliged entity does not discover facts that give rise to a specific suspicion of crime even after an adequate waiting time (which could last from a few months up to a year, depending on the complexity of the business relationships), the entity would usually still be free to keep the customer in question or not. Especially if a risk notification is issued at the request of an obliged entity, the latter may be required to commit itself to farther-reaching limitations, in particular not to de-risk the customer in question solely on the basis of the notification, not to adopt any other adverse measures against the customer solely on this basis, and instead to adopt such measures only if it learns about facts that require it to fundamentally reassess the customer's risk profile.

Legal disincentivisation of adverse measures

To avoid undue interference in the fundamental rights of affected customers, legislation could furthermore provide incentives for obliged entities to forgo the adoption of adverse measures. To this end, the law could in particular specify that once an indicated waiting period has lapsed and the obliged entity has not yet uncovered facts that provide additional substantial reasons for assuming the presence of a high risk, the entity should no longer be required to implement enhanced CDD measures with regard to the business relationship in question. Additionally, legislation could further eliminate incentives for adverse measures by providing obliged entities with greater legal certainty about the adequacy of risk management measures implemented against customers that were affected by a risk notification. This could be achieved by empowering the FIU to provide the obliged entity with specific guidance, during the waiting period following a risk notification, on what CDD measures to undertake in order to address the high risk in question. The obliged entity should be entitled to rely on such guidance vis-à-vis the competent supervisory authority when demonstrating the adequacy of its risk management in the particular case, and the obliged entity would thus enjoy greater confidence about continuing a relationship with the customer in question.

Oversight of the handling of affected customers

Finally, in order to ensure that the aforementioned safeguards are duly applied, once the obliged entity receives the risk notification and up to the end of any waiting time, the employees tasked with handling the notification should be under a strict obligation to report to the issuing authority all relevant changes in the relationship between the obliged entity and the affected customers, and to truthfully and comprehensively answer all questions asked by this authority. To enable effective oversight and review of the implementation of risk notifications, all relevant communications between the obliged entity and the issuing authority should, like the risk notifications themselves, be fully documented.

IV.1.3.2.2. Remedies in Case of Violation of these Conditions

As the proportionality of risk notifications also depends on how they are processed by obliged entities, legislation should provide remedies if such notifications are processed unlawfully by those entities.[176] This regards both any instances of unauthorised processing of information contained in a notification, and the unauthorised treatment of customers following such processing. Concerning the unlawful processing of information, remedies should in particular address cases in which notifications were shared unlawfully within the receiving obliged entity or with third parties, or where purpose limitations set by the issuing authority were disregarded in any other way. Remedies against the obliged entity for claims of unlawful processing of risk notifications should then closely resemble those described for obliged entities' processing of threat warnings. They should in particular provide individuals and entities with a right to know whether, in the past, the obliged entity actually did receive a risk notification that targeted or otherwise affected them. Where this information cannot be disclosed due to a confidentiality obligation of the obliged entity towards the issuing authority, in any case the processing of the notification by the obliged entity should still be subject to review by the competent data protection supervisory authority, which should be given complete access to all relevant information.

Regarding remedies against de-risking and other adverse measures taken against customers affected by risk notifications, legislation should provide for the possibility of having such measures reviewed when there are reasons to suspect that the obliged entity violated applicable limitations. Such a review would best be conducted, at the customer's request, by the authority tasked with supervising obliged entities' compliance with AML/CFT obligations, and the customer should be entitled to have the outcome of this review examined by a court. Due to their freedom of contract, obliged entities generally cannot be required to continue a business relationship against their will. Yet these entities should be subject to adequate sanctions insofar as they disregard their commitment to the issuing authority not to subject an affected customer to

[176] III.3.2.2.

adverse measures essentially because of a risk notification. This applies both to risk notifications issued as part of a voluntary cooperation between the FIU and obliged entities, and to risk notifications that are designed as mandatory instruments.

Obviously, a causal link between a risk notification and adverse measures against a customer will usually be almost impossible to prove. Sanctions in case of abusive de-risking or adverse measures against customers affected by risk notifications should therefore depend on a nuanced distribution of the burden of proof. If an individual or entity presents reasons to believe that adverse measures adopted by an obliged entity against them were essentially based on a prior risk notification, that entity, to avoid being sanctioned, should be required to show that following the risk notification, it implemented adequate additional CDD measures concerning the business relationship in question; furthermore, it should present plausible reasons why the adverse measures were the result of its own CDD findings and a fundamental re-evaluation, based on these findings, of the risk profile of the customer in question.

IV.1.4. Risk Indicators

Risk indicators provide obliged entities with information meant to help them in the identification of financial crime risks. They can appear in different types of documents and even oral communications, and take various forms, such as:

- typology papers,
- case studies or red flags on specific financial crime methods,
- information about criminal activity in a particular geographical area or particular market segment, or
- information about the activities of a particular criminal group.

Unlike threat warnings and risk notifications, however, risk indicators do not identify specific individuals, specific entities or specific transactions, but instead leave it to the obliged entities to decide whether or not a particular customer or transaction constitutes a heightened financial crime risk.

As risk indicators do not refer to particular individuals or entities, they do not usually entail an infringement of rights, and thus are usually unproblematic from a legal point of view. There are exceptions to this, however, especially when these indicators, despite their abstract nature, are discriminatory against a particular group of individuals characterised by a special trait.[177] This can be the case in particular when a risk indicator refers not, or at least not only, to particular conduct, but to personal characteristics, for example of a group of persons from a particular ethnic, religious or political background. As an example, one can think of the case of a typology paper highlighting a risk emanating from customers with a particular political opinion. More often, however, risk indicators will not refer to personal characteristics only, but

[177] III.2.3.

instead contain a mixture of references to conduct and status, such as when a typology paper highlights the activities of a criminal group with a specific national or ethnic background, or when a typology points to financial crime risks emanating from unspecified financial crime enablers in a particular country. In some cases, risk indicators can be discriminatory even when they do not refer explicitly to personal characteristics of individuals, if they nevertheless have the effect of causing prejudice against a particular group of individuals who are characterised by a specific personal trait. This would be the case for example when a risk indicator highlights a risk emanating from a particular geographical area or from a specific business sector, if the individuals who live in this particular area or the individuals who engage in this particular business sector, respectively, mostly share a particular trait, for instance if they are usually from a particular ethnic or national background.

There may of course be plausible reasons for a risk indicator to make reference to personal characteristics of individuals of interest, or to have the effect in some other way of singling out individuals with a particular trait. Not least, some transnational criminal groups are closely related to a country or region of origin. Also, some foreign jurisdictions have played a key role in transnational organised crime, making it likely that many business activities related to individuals or entities domiciled in such a jurisdiction may entail a high financial crime risk. The same is true with regard to the circumvention of EU restrictive measures targeting a particular country. However, in light of the potentially discriminatory effect of such personal-characteristic-specific risk indicators, it does seem necessary to subject them to particular legal scrutiny. Legislators should therefore define adequate substantive conditions and procedural safeguards for the issuing and processing of risk indicators.

IV.1.4.1. The Transfer of Information from Public Authorities to Obliged Entities

IV.1.4.1.1. Conditions

IV.1.4.1.1.1. Necessity

As explained above, although risk indicators do not refer to particular individuals or particular entities, they may still entail an infringement of rights, especially if they are likely to cause some individuals to be singled out as financial crime risks due to discriminatory considerations. Before issuing a financial crime typology or any other form of risk indicator, the authority concerned should therefore always scrutinise whether any of the criteria contained therein might lead obliged entities to perform CDD measures in a discriminatory way. Authorities should ensure that individuals are not singled out merely because of their personal status, that any other singling out of particular groups of individuals does in fact improve the effectiveness of CDD, and that less intrusive alternative measures to achieve the same end are unavailable.

Direct discrimination

Discrimination can first and foremost appear in the form of direct discrimination, which occurs especially where an authority defines the personal status of a customer (for example his or her religion, ethnic or social background, nationality, or political views) as constituting an indicator of financial crime. This scenario may be taken to constitute direct discrimination even if the reference to a personal status is combined with more neutral factors (for example when a risk indicator points to restaurants whose owners are of a particular national origin), for even in case of such a combination, individuals would ultimately still be singled out because of their personal status (in the example: because of their national origin), while the great majority of other people with the same activity (to stay with the example: all other restaurant owners) would remain unaffected. Referring to status as a risk factor will usually be unlawful, as such a differentiation violates the very essence of the prohibition of discrimination as enshrined in Article 21 of the EU Charter.

Indirect discrimination

Risk indicators will however also fall afoul of the prohibition of discrimination if they would lead to indirect discrimination.[178] Such discrimination occurs where an apparently neutral risk indicator puts a particular group of individuals at a particular disadvantage when compared to other individuals, unless this risk indicator provides factually valid criteria for the detection of financial crime. Obviously, CDD serves the specific purpose of identifying problematic transactions and business relationships, and thus particular problematic customers. Many financial crime risk indicators are likely to put a particular group of individuals at a particular disadvantage. For example, if authorities label a particular third country as constituting an enhanced AML/CFT risk, obliged entities will have to conduct enhanced CDD measures, thus usually rendering access to financial services considerably more difficult for individuals who engage in business with this third country. Article 21 of the Charter does not prohibit the singling out of individuals, but merely a singling out in ways that are objectively not justified. This is the case in particular if risk indicators are based on erroneous factual assumptions or if they are otherwise unlikely to improve the effectiveness of CDD. If the application of a risk indicator does not significantly improve obliged entities' ability to detect financial crime and file meaningful SARs, the singling out of a particular group of individuals cannot be considered necessary. In this regard, it is important to note that the effectiveness of a risk indicator cannot be determined from the number of SARs filed by obliged entities on its basis, because by themselves, such filings are not yet proof that the reported activity is linked to crime. Moreover, given that risk indicators require obliged entities to treat affected customers and transactions with particular care, it is even possible that related SARs will often constitute mere defensive reporting, i.e. reporting that is motivated more by an obliged entity's desire to defend itself against possible supervisory criticism

[178] III.2.3.2.

than by a genuine suspicion. Risk indicators' effectiveness can therefore be determined only by looking at the actual quality of SARs, which proceeds primarily from whether they are actually useful for the work of investigative authorities and FIUs.

Availability of less intrusive, equally effective alternatives

Insofar as a typology or any other communication of risk factors is likely to lead to a singling out of a particular group of individuals (for example of business owners with a particular national or ethnic background), it must furthermore be asked whether it is necessary to produce this effect in order to enable the detection of the financial crime that the risk indicator aims to address. More specifically, it must be asked whether the risk indicator could alternatively be framed in a way that would be less likely to single out particular groups of individuals while still remaining effective as an instrument to detect relevant risks. Authorities will however also have to consider whether a narrower wording of the risk indicator would be too limited and thereby weaken the indicator's effectiveness. The necessity requirement thus ultimately comes down to an assessment of the likely effectiveness of a risk indicator, for example whether it should extend to all businesses conducting transactions between country A and country B, or instead only to those businesses active in particular commercial sectors.

IV.1.4.1.1.2. Proportionality Stricto Sensu of Interference in the Rights of Customers

If it is determined that the singling out of a particular group of individuals is necessary, it must then be determined whether this effect is also proportionate *stricto sensu*. This requires balancing the risk indicator's expected added value for improving CDD effectiveness against any unintended detrimental consequences. The less a risk indicator leads to the detection of financial crime by obliged entities, the more unacceptable would be any disadvantages caused by its singling out of particular groups of customers. Besides the actual effectiveness of the risk indicator, two further factors are of particular relevance in this regard, namely the sensitivity of the characteristics of the group that is put under particular scrutiny and the gravity of the detrimental consequences caused by the risk indicator.

Sensitivity of the characteristics of the affected group

As regards the gravity of unintended consequences, consideration must be given to the defining characteristics of the group that is singled out, and to the consequences that the singling out entails for them. The defining characteristics of the group are relevant because they determine to what extent the singling out must be deemed sensitive. For example, if a risk indicator is likely to affect primarily individuals of a particular ethnic or religious background (such as business owners with a similar migration background), this implies a high level of intrusiveness that may be proportionate only in very exceptional cases, if at all. In contrast, if a risk indicator primarily affects

individuals who are engaged in a particular type of business (for example conducting a certain type of trade between two specific countries) and does not to any substantial degree single out individuals who share a particular nationality or other status feature, this would as a rule raise far fewer concerns about discrimination.

Gravity of risk indicators' actual impact on customers

The gravity of risk indicators' unintended consequences, and thus their proportionality, also depends on the consequences that the singling out actually entails for affected customers. Insofar as risk indicators regularly lead obliged entities to de-risk or adopt other adverse measures against customers without first performing a thorough CDD assessment of the customers' activities and without establishing specific facts pointing towards criminal activity, a singling out of individuals due to their personal characteristics would increase concerns regarding discrimination. In contrast, if risk indicators are used by obliged entities merely to focus their enhanced CDD, rather than serving as a quasi-automatic trigger of adverse measures, the actual negative consequences would be limited, especially if, where obliged entities do adopt adverse measures as a consequence of such CDD, their adoption of these measures does not evidence a bias to the detriment of individuals with certain sensitive characteristics.

Particular concerns about indicators pertaining to the origin of a criminal group

Particular proportionality concerns may arise when risk indicators are meant to address risks emanating from particular criminal groups whose members share a common national or ethnic origin and who are embedded within a wider community of people of the same origin. Such indicators can raise serious proportionality concerns because of the danger that the information about the criminals' specific origin, provided by the authorities and thereby rendered particularly trustworthy, may lead to a singling out of customers of the same origin. While the sharing of such risk indicators with a large number of obliged entities would therefore likely be disproportionate, in such cases the authorities could instead consider issuing risk notifications, thereby adopting a more targeted approach that would limit the danger that large parts of the relevant community might be stigmatised and put at risk of adverse measures from obliged entities.

IV.1.4.1.1.3. Procedural Requirements

Insofar as the FIU or the competent supervisory authority considers issuing a typology paper or any other form of risk indicator, they should pay attention to a potentially discriminatory effect, and ensure that, if the singling out of a particular group of individuals is likely to result, releasing the indicator is necessary and proportionate. Risk indicators should be subject to particular scrutiny if they aim at criminal activity whose perpetrators are known frequently to be of a particular national or ethnic origin, even if this origin is not explicitly mentioned in the indicator. Before being issued, potentially discriminatory risk

indicators should be submitted to the competent data protection supervisory authority.

Once a risk indicator is considered potentially discriminatory, the competent supervisory authority should continuously monitor its implementation by obliged entities and identify the resulting impact on customers. To this end, legislators may consider requiring large obliged entities in particular to regularly produce statistics on their de-risking practices and other instances where they implemented adverse measures against customers partially or entirely as the result of considerations linked to their CDD obligations. At the same time, the FIU should continuously monitor the extent to which potentially discriminatory risk indicators are effective. To facilitate monitoring of the effectiveness of risk indicators, obliged entities that file a SAR could be required to state whether they believe the reported activity is related to a particular risk indicator.

IV.1.4.1.2. Remedies in Case of Violation of these Conditions

In view of the potentially discriminatory effect of risk indicators, legislators should consider providing remedies against their issuance. Importantly, given that the information underlying a risk indicator will often be at least partially confidential, the remedy could be designed as a complaint mechanism to a supervisory authority – one in charge of either AML/CFT or data protection. Such a mechanism would allow individuals to trigger a review of existing risk indicators if they have reason to believe that they suffered discrimination from obliged entities due to a typology or any other form of risk indicator.

IV.1.4.2. The Processing of Information by Obliged Entities

IV.1.4.2.1. Obligations of the Obliged Entities

Given that the proportionality of the authorities' issuing risk indicators depends in part on such indicators' not being used for discrimination, legislators should clarify how obliged entities are expected to ensure such a non-discriminatory use. However, obliged entities' CDD builds on information from a plurality of sources, of which the authorities will usually be only one, and therefore it would seem unfeasible to impose special non-discrimination rules for the use of risk indicators. Instead, legislators should consider defining rules for non-discrimination in CDD that apply irrespective of the source of the information that may have led a particular group of individuals to be singled out. While this would essentially constitute a partial limitation of obliged entities' freedom of contract, legislators also have to recognise that today's shape of the AML/CFT framework can sometimes produce economic incentives to discriminate. This is not a small concern, given that systematic discrimination by businesses – in particular those with a large market share – might arguably have a detrimental impact on social cohesion. It is of course primarily a political question to decide to what extent de-risking and similar decisions should be subject to anti-discrimination rules. Yet especially if authorities are increasingly expected to share strategic information with the private sector, and as consequently they are more and more assuming partial responsibility for the performance of CDD,

the law should address the danger that discrimination may result. In defining the limits of what should be considered appropriate, legislators will, on the one hand, have to recognise that CDD can be costly to perform, and that cost considerations are therefore a legitimate part of obliged entities' decision on whether to continue, or abstain from, a business relationship. On the other hand, legislators should also recognise the need to make sure that the fight against financial crime does not give rise to another social ill, namely discrimination.

IV.1.4.2.2. Remedies in Case of Violation of these Conditions

If legislators were to introduce anti-discrimination rules governing CDD, then similarly to the remedies proposed above for the processing of threat warnings and risk notifications, they could consider providing a complaint avenue to the competent supervisory authority when there are reasons to believe that an individual has suffered from discriminatory risk management. Such a remedy would set a more frequent use of risk indicators on a more solid legal foundation. The supervisory authority could then in particular be entitled to scrutinise an obliged entity's risk management when there are reasons to believe that the discrimination in which that obliged entity is alleged to have engaged might be linked to a particular risk indicator.

IV.2. Public-to-Private Sharing to Assist Authorities

IV.2.1. Possible Purposes of Public-to-Private Sharing in Support of Authorities

Besides public-to-private information sharing in support of obliged entities' CDD, public-to-private sharing can also directly assist the work of competent authorities. Usually, such assistance takes the form of responding to information requests and producing documents and other data carriers, in particular in the context of criminal investigations. However, the laws so far, especially those relating to criminal procedure, deal only tentatively (if at all) with the case where a competent authority requests a private entity not merely to hand over information, but to produce information proactively for that authority. Under existing laws, most of the time, responding to a production order or similar request from a competent authority will of course require the recipient private entity to undertake some efforts (for example automated screening or the decryption of documents) in order to make relevant data available. Yet beyond such efforts, such private entities are usually not under an obligation to gather additional information for the authorities, or to analyse existing data stocks in a way that goes beyond the filtering of information.

Financial analysis request

Competent authorities may find it useful to ask obliged entities to analyse available data, because some obliged entities – especially those with large numbers of customers and with an international footprint – may be able to generate information that otherwise would be inaccessible to the authorities. Information can be out of the authorities' reach not least of all because the

authorities might lack the technology necessary for sufficiently complex processing. At least as importantly, information can also be out of reach because authorities might often not have access to the large data volumes required for a fruitful analysis, especially insofar as the use of automated analytical tools for the detection of hidden cross-border transaction patterns is concerned.

Legislators should therefore consider providing a legal basis for formal requests that authorise and, in some situations, even require obliged entities to analyse their data stocks for the purpose of supporting competent authorities ("financial analysis requests"). Though such proactive analysis may to some extent be legal under existing laws, and may occasionally already be practised by authorities and obliged entities in some Member States, the lack of a clear legal framework likely discourages such practice. Furthermore, even if an obliged entity were to comply voluntarily with such requests from investigative authorities, it is not clear to what extent such analyses would be lawful at the moment, given that data protection law, and in particular Regulation (EU) 2016/679, usually provides rather little specific guidance.[179] In light of the proportionality considerations described above,[180] and in particular the need for procedural safeguards to prevent an arbitrary singling-out of individuals and entities, it seems indeed unlikely that under the current laws, informal, unregulated forms of cooperation between obliged entities and investigative authorities would always be lawful.

Financial analysis requests are ultimately meant to prompt an analysis of customer data by the receiving obliged entity. This will however usually require the requesting authority to first provide the obliged entity with some details about the particular investigation or at least about the suspicion at hand. Such details may include personal data of specific persons of interest, or mere strategic information about particular situations of interest or about typical features of criminal phenomena. The more information the authority provides, the better the obliged entity might be able to conduct a fruitful analysis. Obviously, however, the authority will also have to consider legal and operational reasons that militate against disclosing the information to the obliged entity.

Financial monitoring requests

In what is essentially a particular form of financial analysis request, an authority may also ask an obliged entity to subject a specific business relationship, transaction, or entire business segment to particular scrutiny by collecting information for the benefit of the authorities ("financial monitoring requests"). Such requests are different from mere financial analysis requests in that the obliged entity is supposed to gather and analyse information that the entity does not yet have available at the time of the request. This would also cover the

[179] III.2.2.2.3.

[180] III.2.2.1.

case when the obliged entity is expected to monitor future transactions of a customer (and therefore continue a business relationship to collect such information) or is required to produce new information (about past or future events) from third parties (including, possibly, directly from customers). In order to provide a meaningful starting point for the requested monitoring, the authority will usually need to provide the obliged entity with more or less specific information about the suspicion or investigation at hand.

In complying with the monitoring request, the obliged entity may be required to take various measures and produce various types of information, depending on the particular purpose intended by the authority. A monitoring request may in particular ask the obliged entity to spontaneously inform the requesting authority about certain developments that transaction data allows one to observe, for example that a targeted customer is sending or receiving money to or from a particular third person, that a payment card or online service is being used outside a particular geographical area, or that a particular person (for example a person targeted by EU restrictive measures) seems to be establishing commercial links with a particular company. Depending on the sophistication of the transaction screening, the monitoring of a customer can go beyond the detection of rather obvious events (in particular, events that will subsequently be evident from the customer's account statement, for example that money was sent to a particular third person) and instead extend to events that become visible only through a more complex analysis of numerous transactions (for example that a customer indirectly received money from a particular third party hidden through a chain of front companies). Also, a monitoring request might not necessarily be aimed at a particular individual or entity; for instance, it may instead require the obliged entity to signal any phenomena with certain characteristics, such as any transactions carried out in a particular business sector with a destination in a particular foreign country.

Insofar as monitoring requests ask an obliged entity to signal particular events, they ultimately serve the purpose of providing the requesting authority with timely or even real-time information about the conduct of a particular individual or entity, or about developments in a particular market segment. Alternatively, or in addition to just signalling particular events, a monitoring request can also require an obliged entity to gather information about past or future events when the obliged entity would otherwise not gather this information if it were not for the request. In this variant, the obliged entity is essentially asked to collect and retain additional information about a particular customer or a particular market segment for the benefit of the requesting authority. This may potentially even involve mapping a customer's future physical movements through an analysis of the use of online financial services and related communications traffic data. Though some of the preceding forms of data processing may already be lawful when necessary for the performance of an obliged entity's CDD, current laws will seldom require obliged entities to conduct such extensive proactive monitoring on behalf of an authority. In the absence of a legal obligation or explicit legislative authorisation, it seems unlikely that obliged entities will

currently be allowed to voluntarily undertake monitoring of individual customers if doing so does not also entail an added value for the obliged entity itself at the same time. In particular, in that case the obliged entity cannot rely on a legal basis under EU data protection law, especially Regulation 2016/679.[181]

IV.2.2. Financial Analysis Requests

IV.2.2.1. The Transfer of Information from Public Authorities to Obliged Entities

IV.2.2.1.1. Conditions

IV.2.2.1.1.1. Necessity

Given that financial analysis requests usually constitute an interference in the rights of individuals and entities whose data is processed and, if the request is mandatory, also in the rights of the receiving obliged entity, such a request needs to be necessary. Authorities need to ask, in each individual case, whether they have alternatives available that are less intrusive and, at the same time, at least as effective in achieving the pursued objective.[182]

The necessary scope of a public-to-private transfer of information depends on the extent to which the obliged entity needs the information in order to conduct a meaningful analysis that corresponds to the objective defined by the authority. Regarding the intended data processing by the obliged entity, authorities will have to consider the intrusiveness of the processing, and in particular whether a less far-reaching analysis would be as effective, in light of the scope and sensitivity of the data to be processed and the intrusiveness of the processing method. Necessity considerations can then lead for example to the conclusion that the requested analysis should not extend to all of the entity's customer data, but only to certain categories of customers. Authorities should also take into account that the need to limit an interference in affected customers' rights can militate for a greater interference in the obliged entity's rights. In particular, requesting a financial analysis by the obliged entity may eliminate the need to require the transfer of large amounts of customer data to the authorities, thereby possibly reducing the overall intrusiveness of the investigation.

IV.2.2.1.1.2. Proportionality Stricto Sensu of Interference in the Rights of Customers

The proportionality *stricto sensu* of a financial analysis request vis-à-vis the rights of affected customers essentially depends on balancing the public interest at stake (i.e. the gravity of the suspected crime or threat investigated by the authorities) against the intrusiveness of the data processing for those affected by it and against the gravity of any unintended consequences that may be brought about by the disclosure of information to the obliged entity. The

[181] III.2.2.2.3.

[182] III.3.1.1.2.

intrusiveness of the data processing essentially depends primarily on the sensitivity of the information that the analysis is meant to produce, the sensitivity of the data that is processed to this effect, and the risk of errors that the processing method might entail.[183]

Sensitivity of the sought-after information

As regards the information that the analysis is meant to produce, various degrees of sensitivity are conceivable. At the lower end, the analysis may aim for information of a merely strategic nature – information that does not relate to specific individuals or specific entities. This would be the case for example when the authority requests the obliged entity to provide information about the volume of all cross-border transactions destined to a particular third country and about the main purposes of these transactions. Even if such an analysis leads to a singling-out of a small number of individuals of interest, the analysis would still be of limited intrusiveness. A similar conclusion may be reached if the analysis aims to produce information about the situation of specific entities (for example whether a company is controlled by particular individuals), because and insofar as entities are usually not entitled (for instance, in the case of information about a beneficial owner) to keep this information confidential. In contrast, the financial analysis will usually be more intrusive if it seeks to inquire into the situation of specific individuals. Given that individuals nowadays enjoy only a rather limited protection of information pertaining to their status as beneficial owner of a payment account, a financial analysis cannot be said to be intrusive merely because it aims to establish whether a specific individual controls particular accounts. Considerably more important proportionality concerns may be raised, however, if the financial analysis ultimately produces information about sensitive non-financial aspects of individuals' private life, such as the customer's personal preferences or intimate relationships.

Sensitivity of the processed data

As regards the nature of the processed data, legislators and authorities will need to consider that the obliged entity's analysis may possibly extend well beyond transaction data in the narrow sense. In fact, obliged entities regularly use various kinds of non-financial data for their CDD, and may also use this data to process customer data in response to a financial analysis request. This could for example include IP addresses used by customers to access online services, thereby potentially allowing the geolocalisation of the customer, as well as information that the obliged entity collected from the customers themselves, and information from third parties, in particular from data brokers – including, in some cases, data stemming from an analysis of customers' online activities. Such information can enable the obliged entity that receives the request, and thereby indirectly the requesting authority, to gain very deep insights into customers' private life. Depending on the seriousness of the suspicion or threat,

[183] III.3.1.1.3.1.

the processing of highly sensitive information about a customer may still be proportionate, but legislators should consider providing guidance on the acceptable scope of data, and on the conditions under which it may be analysed. In any case, the type and volume of personal data to be included in a financial analysis request must be subject to adequate limits, especially insofar as this data processing might effectively even lead to a fusion of transaction data and data about a customer's non-finance-related online activities.

Risk of processing errors

Crucially, the sensitivity of the financial analysis will also be determined by the method by which the data is processed, and in particular by the risks of errors that the method may entail. Obviously, financial analyses can sometimes be particularly fruitful if they include the data from thousands or even millions of transactions and customers that are seemingly unrelated to the subject matter of the analysis request. Especially advanced automated analytical tools may then be able to identify relevant transactions and accounts by detecting patterns that are invisible to a human analyst. Legislators and authorities must be aware, however, that such processing of mass data can entail considerable risks for innocent customers. Ostensible correlations might be established between a particular person and certain transactions purely on the basis of erroneous factual assumptions that result from a misinterpretation of certain information (for example if an incomplete picture of a person's social network activities, or a simple misspelling of a name, leads to a false conclusion that the person is the beneficial owner of a particular company). The obliged entity's analysis can potentially also be misguided by overreliance on customers' risk profiles, because such profiles may induce the obliged entity to focus its attention unduly on some customers. The more data from large numbers of customers is included in an automated analysis, the more likely it is that innocent customers will be mistakenly labelled as persons of interest for authorities. This will particularly pose a problem when the automated data processing method does not allow its human users to trace retrospectively how a result was reached.

Gravity of unintended consequences

The intrusiveness of a financial analysis request, and accordingly its proportionality, also depends on the gravity of de-risking and similar unintended consequences that the related transfer of information to the obliged entity may cause to individuals and entities. The fact that a competent authority shows interest in a particular customer in connection with a criminal investigation will frequently prompt an obliged entity to reassess its relationship with that customer, which will in turn frequently lead to de-risking or other adverse measures. Such consequences are likely to become more and more probable the more closely the authorities involve obliged entities in the investigation of crime; the more operational information these authorities make available to the private sector, the more the private parties may be able to learn about the identity of persons whom the authorities consider to be of interest, possibly still

at a very early stage of the investigation or even before it begins. In this regard, the more an increasingly close cooperation between authorities and obliged entities is likely to cause an adverse treatment of customers, the more that cooperation must be deemed intrusive. Of course, to some extent, stigmatising consequences are an unavoidable side effect of criminal investigations, at least from the moment the charges are made public by the authorities. One must be mindful, however, that criminal investigations usually operate within a tightly regulated legal framework that is supposed to ensure a high level of scrutiny of the underlying facts, while the same level of scrutiny (and thus the resulting protection from arbitrary infringements of rights) will often be lacking within other types of proceedings. Particular proportionality concerns will thus arise not least if the financial analysis request targets individuals or entities who are not themselves the subject of a criminal investigation, or against whom the incriminating evidence is not strong. To justify the probable unintended consequences, such a financial analysis request should be permissible only if, in addition to all other applicable legal conditions being satisfied, the nature of this customer's business dealings indicates at least that the customer entails a high financial crime risk.

IV.2.2.1.1.3. Proportionality of Interference in the Rights of Obliged Entities

Insofar as legislators and authorities choose to impose an obligation to comply with the financial analysis request, they must also give consideration to the obliged entities' rights, not least of all their freedom to conduct a business.[184] In this respect, the gravity of the interference will largely depend on the scope of the analysis and on the resources that the obliged entity needs to allocate for the purpose, minus, of course, any indemnification to which it may be entitled for complying with the request. Insofar as the financial analysis request is combined with an order temporarily not to cut off the relationship with the customer or adopt any other adverse measures against her, in order to keep from tipping off suspects, account must also be taken of the additional compliance costs that could become necessary during the non-voluntary continuation of a business relationship. Nevertheless, in balancing the public interest against the interests of the obliged entity, authorities must also bear in mind that obliged entities are subject to CDD obligations in any case, and therefore must anyway maintain the technological infrastructure and appropriately trained compliance staff necessary for the performance of a financial analysis request, irrespective of whether such a request has actually been made.

Legislators may also decide to provide for voluntary financial analysis requests, meaning requests that would leave it up to the obliged entities to decide whether or not to comply. Important public-interest considerations may however militate in favour of a mandatory approach. Since the provision of financial services often entails considerable risks of criminal abuse, the imposition of an obligation to conduct financial analyses on behalf of

[184] III.3.1.1.3.2.

competent authorities does not appear to be disproportionate in principle, especially if the technical complexity of the requested analysis does not go beyond the processing methods that the obliged entity is already required to apply in performance of its CDD obligations. Mandatory financial analysis requests especially seem to be a proportionate interference in the rights of obliged entities when the requested financial analysis addresses a particular vulnerability of the addressed entity to financial crime, for example the provision of cross-border financial services in connection with third-country jurisdictions known for a strong exposure to transnational organised crime. Depending on the seriousness of the criminality involved, legislators may then potentially even consider requiring obliged entities to implement specific analytical methods whose complexity goes beyond what is required by current CDD obligations.

Legislators should also consider whether private actors would gain an undue influence on criminal investigations if they were free to choose whether to comply with an analysis request. In some cases, a voluntary approach to public-private cooperation may offer advantages for the authorities, especially if legal reasons render the authorities unable to compel cooperation. This can in particular be the case if the requesting authority wants an obliged entity's analysis to include customer data that is located in a foreign subsidiary of the entity; for even if the laws of the foreign jurisdiction allow this subsidiary to make the relevant data available to obliged entities from its corporate group in other countries, the foreign country's sovereignty will still normally leave the requesting authority unable to compel such intra-group transfers. However, in other cases, a voluntary approach could lead instead to a curtailment of the public interest, because it might make the success of a criminal investigation contingent on private-interest considerations.

IV.2.2.1.1.4. Procedural Requirements

Authorising authority

The power to issue financial analysis requests should be available to investigative authorities and FIUs, and might be made available even to other authorities, in particular those that are tasked with the enforcement of EU restrictive measures. In empowering authorities other than criminal-justice authorities to issue such requests, legislators should take particular care that the applicable legal framework provides adequate procedural safeguards. The issuing of financial analysis requests, given their potentially highly intrusive nature, should usually be subject to prior authorisation by a judicial or other independent body, especially when such requests aim at producing information about an individual.

Ensuring proportionality of the requested data processing

To ensure that the requested financial analysis is proportionate, in each case the requesting authority should define the exact purpose of the analysis, i.e. specify the information that it seeks, along with what categories of customer

data should be processed and what processing methods should be used by the obliged entity. If the obliged entity is asked to conduct the analysis through automated processing techniques, and given that the processing method is of considerable relevance for assessing the proportionality of the analysis, the requesting authority should ensure that it understands the technology used by the obliged entity, and also verify that the types and scope of customer data included in the analysis are in line with its demands. In particular, the requesting authority should require the obliged entity to explain how personalised statistical values (as opposed to facts pertaining to a particular person) may affect the outcome of its analysis, and closely related to this question, to identify potential causes that might lead to unintentionally discriminatory results. In working with the obliged entity on these questions, it will usually be useful for the requesting authority to coordinate with the authority competent for supervising the obliged entity's data processing.

Limiting unintended consequences

The requesting authority should furthermore have internal procedures in place to ensure that it discloses to the obliged entity only such information as is strictly necessary for the purpose of conducting the requested financial analysis, and at the same time that this disclosure does not compromise preponderant confidentiality interests of the authority itself or of any third party. To prevent particularly sensitive information from falling into unauthorised hands, the requesting authority could provide a secure location where information is disclosed to employees of the obliged entity who have been duly vetted for security, and where these employees will be able to access the obliged entity's data infrastructure without having the possibility to produce written or digital records of disclosed information.

The law should also require requesting authorities to ensure that the gravity of unintended consequences is always proportionate to the seriousness of the suspicion concerned. To prevent the obliged entity that receives the request from speculating about a possible threat posed by the targeted customer, legislators may consider authorising the investigative authority to declare to the obliged entity whether there are reasons to believe, in the specific case and in light of the information known to the authority, that the targeted customer entails a significant probability of involvement in financial crime. If the investigative authority denies there is a threat of financial crime, the obliged entity should be entitled to rely on this assessment vis-à-vis the competent supervisory authority.

Insofar as a financial analysis request is not authorised as part of an ongoing criminal investigation, yet is still likely to cause the obliged entity to adopt adverse measures against the targeted customer, the law should provide alternative safeguards to protect customers from the excessive unintended consequences. To safeguard proportionality, the law could then, as a minimum, require that any customers targeted by a financial analysis request outside a criminal investigation must, in view of the available information, constitute a

high financial crime risk. Accordingly, in such cases the financial analysis request should always be treated as a risk notification, and therefore respect the procedural safeguards described above to ensure that it does not quasi-automatically trigger adverse measures.

Further measures to protect the integrity of criminal proceedings

Financial analysis requests essentially ask an obliged entity to support investigative authorities or FIUs by proactively analysing customer data and handing over the results to the requesting authority. Where the obliged entity enjoys a certain margin of discretion in selecting the processing methods (for example by determining how particular search queries are framed) and, at least as importantly, in selecting the data that is included in the analysis, the employee in charge of the analysis may have considerable influence over the result of the analysis. Given that to a greater or lesser extent, the outcome of a financial analysis is determined by choices made within the obliged entity dealing with a request, it is important to keep in mind that the analysis can, and often will, take place against the background of a conflict of interest on the part of the same obliged entity. For although the obliged entity may be required, or volunteer, to help the authorities, it may at the same time have an interest in avoiding the revelation of facts that, while related to the case at hand, would shed a bad light on its commercial activities or the quality of its AML/CFT compliance. Such conflicts of interest are potentially a serious problem for a criminal proceeding, not least because innocent individuals might be put under suspicion or even be convicted due to selective, misleading, or, in extreme cases, outright false information provided by the obliged entity. In the criminal-justice system, such concerns are usually addressed by procedures that are meant to ensure a high degree of accuracy and transparency of how evidence is obtained, and by subjecting witnesses or other private sources of evidence to the threat of criminal sanctions should they provide untruthful or incomplete testimony or obstruct justice in other ways. Those existing safeguards may however be inapplicable if a financial analysis request is authorised outside the confines of an ongoing criminal investigation and issued by an FIU, i.e. by a body that is not a criminal-justice authority. Legislation should therefore ensure that safeguards are in place so that obliged entities' responses to financial analysis requests are accurate and complete and do not withhold any potentially relevant information even where the request is not issued by a judicial authority – including, if necessary, by extending the scope of relevant criminal offences. In this respect, particular consideration should be given to financial analysis requests by FIUs in cases where the findings of the analysis may be expected to be used as evidence in judicial proceedings at a later stage.

Notification of targeted customers and keep-open requests

Finally, given that financial analysis requests can entail quite an intrusive processing of personal data, and can also incentivise adverse measures by the recipient obliged entity, targeted individuals should usually be notified that a request has been issued once disclosing this fact will no longer endanger the

outcome of ongoing investigations.[185] In a similar vein, legislators should consider establishing powers to issue temporary keep-open requests that would require the obliged entity not to adopt adverse measures against a targeted customer for a limited period of time, in order to protect investigations and strengthen the effectiveness of any tip-off prohibitions. To enable courts and supervisory authorities to scrutinise obliged entities' processing of financial analysis requests, these requests and their specific content should furthermore always be comprehensively documented in a single database, in the same way as the risk notifications described above.

IV.2.2.1.2. *Remedies in Case of Violation of these Conditions*

IV.2.2.1.2.1. Remedies for the Obliged Entities

To the extent that a financial analysis request is designed as an obligation of obliged entities, those entities should be able to challenge this measure in court, especially if the request is deemed arbitrary or disproportionate.[186]

IV.2.2.1.2.2. Remedies for Targeted Customers

Issuing a financial analysis request can constitute a significant interference in the rights of targeted individuals. It should therefore be subject to an effective judicial remedy in line with Article 54 of Directive (EU) 2016/680 or Article 79(1) of Regulation (EU) 2016/679.[187] This would proceed by way of investigations by the supervisory authority competent for overseeing the issuing authority's processing of personal data, following a complaint lodged according to Article 52(1) of Directive (EU) 2016/680 or Article 77(1) of Regulation (EU) 2016/679. Furthermore, legislators should also establish effective remedies for legal entities against the issuing of a financial analysis request, as in general these entities are not covered by the remedies provided by Directive (EU) 2016/680 and Regulation (EU) 2016/679.

IV.2.2.2. The Processing of Information by Obliged Entities

IV.2.2.2.1. Obligations of the Obliged Entities

Compliance with conditions set by the requesting authority

If the obliged entity has received information from the requesting authority as part of the financial analysis request, the entity should always comply with any processing conditions set by the authority.[188] This regards in particular the specific purpose of the analysis, the methods to be used, and the data to be included in the analysis. Furthermore, unless it has explicit prior authorisation, the obliged entity must not use the provided information from the authority for any other purpose. In the same vein, the results of the analysis may

[185] III.3.1.1.4.

[186] III.3.1.2.1.

[187] III.3.1.2.2.

[188] III.3.2.1.

subsequently be used for the obliged entity's own purposes only insofar as authorised by the requesting authority. However, the requesting authority should usually grant this authorisation if the findings of the analysis are objectively relevant in identifying financial crime threats that may affect the obliged entity.

Internal procedures to safeguard information contained in the request

To ensure compliance with the purpose limitation attached to the information provided by the authorities in the request, obliged entities should furthermore implement internal procedures to prevent the information from falling into the hands of unauthorised employees or third parties, or from being used for unauthorised purposes. Therefore, financial analysis requests should be accessible only to a small number of employees, and as a rule the information they contain should not be incorporated into the obliged entity's CDD screening. Individuals responsible for the unauthorised sharing or unlawful use of the information should be subject to effective sanctions; in case of structural failings, such liability should extend to the obliged entity itself.

Clarifying how obliged entities are to manage targeted customers

Close cooperation between authorities and obliged entities in the context of criminal investigations can, and seemingly often already does, lead to de-risking and other adverse measures against affected customers, even when there are no specific reasons to believe that these customers constitute a significant crime risk. More frequent public-to-private cooperation is likely to escalate this problem further and thus raise doubts about the proportionality of such cooperation, even if the authorities do not intend to cause adverse measures. Legislators should therefore consider imposing a prohibition: If obliged entities receive a request – that is, a financial analysis request, production order, or similar investigative measure – within a criminal investigation, they must not adopt adverse measures against a customer primarily or exclusively due to the mere fact that this customer, or a third person closely related to this customer, has been mentioned in the request. But this prohibition should apply only if, when the requesting authority issued the request, it also explicitly clarified that, in view of the available information and at least for the time being, the customer or third person in question does not entail an enhanced financial crime risk. Similarly to the procedure proposed above for risk notifications, such a prohibition could be supplemented by an obligation of recipient obliged entities to inform the requesting authority or the competent supervisory authority about any adverse measures (such as a discontinuation of the business relationship or an increase of fees) that the obliged entity has adopted against a targeted customer within a certain period of time after the request. Owing to the obliged entity's contractual autonomy, such a prohibition would usually not impede the entity from discontinuing a business relationship or from adopting similar adverse measures. However, if resulting data were to indicate a strong correlation between the issuing of financial analysis requests or other investigative measures and the adoption of adverse measures by a particular

obliged entity, even in cases when the requesting authority had explicitly denied the presence of an enhanced risk, this would be relevant for assessing the proportionality of continuing a close cooperation between authorities and the obliged entity concerned. Similarly, if financial analysis requests were to be issued by an authority outside a criminal investigation, the procedure described above for risk notifications should, as already stated, also apply to such requests and thereby curtail excessive adverse measures.

Keep-open requests

Lastly, the obliged entity receiving a request must comply with any tip-off obligation that may be added to a financial analysis request in order to protect an ongoing investigation. However, if legislation provides for a keep-open request in order to avoid an implicit tipping-off, such an obligation must be subject to stringent time limits, especially in cases where the available information does in fact point to an involvement of the targeted customer in financial crime, given that keeping the customer may entail both reputational and regulatory risks for the obliged entity. Besides providing temporal limits to a keep-open request, legislators may also consider further options to alleviate such concerns, in particular by clarifying an exemption from supervisory sanctions for dealing with the targeted customer while a keep-open request is in force, and where appropriate, by communicating clearly to the public that the obliged entity was asked to retain the customer temporarily in order to assist an investigation.

IV.2.2.2.2. Remedies in Case of Violation of these Conditions

Given that the proportionality of financial analysis requests is largely dependent on how the requests are actually processed by the obliged entity, legislation should provide for effective review and oversight mechanisms against unlawful processing by such entities.[189] These mechanisms must ensure in particular that the obliged entity respects the conditions (especially as regards the nature and scope of the processed data and the processing methods) defined by the requesting authority, and in particular the purpose limitations attached to the information contained in the request, including the prohibition on unauthorised sharing of such information within the obliged entity and with third parties. Remedies against the obliged entity in case of an alleged unlawful processing of a financial analysis request should then closely resemble those described above for obliged entities' processing of threat warnings and risk notifications.

As the proportionality of financial analysis requests depends partially on whether customers suffer de-risking and other adverse measures as a consequence, such measures should be subject to independent oversight. If a financial analysis request simultaneously entails a risk notification, the review and oversight mechanisms described above for risk notifications should apply. For financial analysis requests that were issued as part of a criminal

[189] III.3.2.2.

investigation, the authority tasked with supervising obliged entities' compliance with AML/CFT obligations or with data protection obligations should give special attention to the policy those entities adopt vis-à-vis customers who were the subject of such requests. At least if there is a strong statistical correlation between financial analysis requests and the de-risking of customers, this authority should scrutinise whether the obliged entity in question violated the above prohibition against adopting adverse measures following a financial analysis request when the requesting authority explicitly specified that the customer did not entail an enhanced financial crime risk. If the adverse measures were not plausibly based on other reasons, legislators should consider the imposition of sanctions.

IV.2.2.3. The Processing of Analysis Results by the Public Authorities

Legal safeguards should also be provided for how the findings of a financial analysis request are used as evidence at trial and in the context of the judicial authorisation of asset freezes and other preliminary preventive measures. While financial analysis requests can produce useful leads for further investigative measures, judicial authorities should be aware that the results of such analyses will often be prone to error. This is not least because financial analyses, especially complex ones, regularly rely on a multitude of different sources of information (not just transaction data but also information from third parties, possibly including information about the customer's online activities) whose accuracy the obliged entity addressed by a request will often not be able to verify. Especially if an analysis establishes a connection among numerous accounts that are held by different companies, this finding will usually rely on (more or less fact-based) hypotheses about the individuals who ultimately control these companies, and to that extent will sometimes have a rather speculative basis. The automated analysis of transaction patterns can often produce helpful clues about the origin and destination of funds, and about the beneficial owner of accounts, but such findings should be treated with caution. Unless the judicial body using the results of a financial analysis request can in fact establish exactly how, and on the basis of what information, the analysis reached certain conclusions, or alternatively, the conclusions are corroborated by additional evidence, the evidentiary value of the findings of the analysis will be limited and in this regard resemble mere hearsay evidence.

IV.2.3. Financial Monitoring Requests

Financial monitoring requests are essentially a particular form of financial analysis request, and differ from the latter in that the obliged entity is asked not only to analyse its data stocks, but also to collect or retain additional information for the authorities. Consequently, the above recommendations on financial analysis requests are relevant here as well. However, given that the obliged entity is expected to collect information on behalf of the requesting authority, some additional considerations apply.

IV.2.3.1. Necessity

As regards the necessity of a financial monitoring request, two additional factors must be considered in each particular case. Both of them pertain to whether investigative alternatives are available that would be less intrusive for both affected customers and the receiving obliged entity.

First, the issuing authority should always ask itself whether it is really necessary to task an obliged entity with collecting prospective information. In many cases the authority can obtain the desired information simply by waiting for a while and then requesting the information from the obliged entity. Obviously, this alternative is available only if the obliged entity, notably due to its accounting needs or CDD obligations, is going to collect the relevant information in any case and irrespective of the request. However, such retrospective requests will obviously not allow for a monitoring and real-time signalling of relevant events (for example a real-time signalling that the targeted customer uses his payment card in a particular geographical area).

Second, the authority should also consider whether it can by itself obtain the desired information without the help of the obliged entity, and thus without exposing the targeted individual or entity to the risk of possible de-risking or other unintended consequences. Yet depending on the circumstances, alternative monitoring techniques (for example the use of special technical tools to geolocate the customer) would sometimes lead to an even more comprehensive collection of data and would then not constitute less intrusive alternatives.

IV.2.3.2. Proportionality of Interference in the Rights of Customers

In the same way as for financial analysis requests, the proportionality of the monitoring of customers and transactions will first and foremost depend on:

- the purpose of the data processing (for example whether the monitoring is merely meant to identify the beneficial owner of a legal entity, or instead to yield sensitive insights into a customer's private life);
- the nature and scope of the processed data (for example whether the monitoring is limited to simply observing transactions on a specific account, or instead also entails processing sensitive non-financial personal data);
- and the methods of the processing (for example whether the monitoring is limited to alerts triggered by transactions above a certain amount, or instead entails an automated analysis to reveal hidden links between individuals).

As with financial analysis requests, the authority will furthermore have to consider the likelihood of unintended detrimental consequences, in particular the de-risking of affected customers.[190]

In addition to these factors, authorities need to give particular attention to the fact that financial monitoring requests are not limited to an analysis of data, but effectively also ask the obliged entity to collect information on behalf of the authorities. The proportionality assessment should therefore take into account two further considerations, namely a possible circumvention of the legal limitations to authorities' data gathering, and a particular intrusiveness of the monitoring.

A possible circumvention of the legal limitations to authorities' data gathering

The requesting authority should always ask whether it would be allowed to gather the sought-after information directly on its own. If not, then the associated prohibition, and its underlying reasons, can point towards the monitoring request being disproportionate, because the authority is effectively steering the data collection. For example, if the requesting authority is not allowed, for the purpose of the particular investigation in question, to gather telecommunications traffic data or user profiles generated by an online service provider, asking an obliged entity instead to obtain such data for the benefit of the investigation could appear to amount to a circumvention of the relevant prohibition. Even if such data is subsequently not handed over to the authority, but merely used by the obliged entity to produce certain findings (for example to geolocate a customer), the data is still being processed for the benefit of the requesting authority.

Intrusiveness of the monitoring

The proportionality of financial monitoring requests will also be influenced by the methods by which the obliged entity addressed by the request is supposed to gather information. This concerns first of all the scope of the information gathering, particularly the extent to which the measure would cover affected customers' private life, but also whether the gathering is covert, or instead is disclosed to the individuals whose data is sought. Monitoring requests must usually be considered highly intrusive if they essentially instrumentalise the obliged entity to subject a customer's private life to continuous covert monitoring, not least if the monitoring is expected to covertly produce, through an analysis of transaction and geolocalisation data, a detailed image of the customer's movements and social interactions.

IV.2.3.3. Proportionality of Interference in the Rights of Obliged Entities

If a financial monitoring request is designed as an obligation, it can as a rule be considerably more intrusive into the obliged entity's rights than a mere financial analysis request. For while the latter is limited to analysing information that is

[190] III.3.1.1.3.1.

already available to the entity, a monitoring request requires the entity to gather or retain information for the authorities. If (as in the case of the monitoring of an account) this means that the obliged entity is required to continue a business relationship against its will, this could amount to transforming the obliged entity's services into an instrument that would then primarily or exclusively serve the purpose of keeping the customer under surveillance. Depending on the circumstances of the particular case, such a transformation – essentially forcing the obliged entity to provide surveillance as a service – can constitute an excessive interference in the obliged entity's freedom to conduct a business.

As this is a key aspect for legislating mandatory financial monitoring requests, legislators will need to decide whether, and if so, for how long, an obliged entity that receives a request may be required, against its will, to keep an account open or continue a particular business relationship in order to allow for the monitoring. This will depend in particular on whether such an obligation would constitute a proportionate interference in the obliged entity's rights, which will in turn depend in particular on the seriousness of the suspected criminality involved and whether a premature closing of the account or discontinuation of the business relationship would endanger an ongoing investigation.

IV.2.3.4. Procedural Requirements

Legislation should ensure that the monitoring of customers by obliged entities does not lead to a circumvention of the privilege against self-incrimination. This privilege will generally not apply to communications between the obliged entity receiving a request and a targeted customer, but there may be cases where queries addressed by the obliged entity to a targeted customer could be seen as oppressive or in other ways as unduly limiting the customer's freedom not to incriminate herself, and if they result from a solicitation from an authority, they would amount to a violation of this freedom. Legislation should therefore clarify that an obliged entity that receives a request must not threaten the targeted customer with unlawful consequences or purposely mislead her when trying to obtain additional information for the purpose of a monitoring request.

Finally, legislators must be aware that financial monitoring requests will usually amount to a covert surveillance tool, and moreover a surveillance tool that may provide detailed insights into individuals' private life. Given the intrusiveness of such requests, in general they should only ever be issued subject to prior authorisation and continuous supervision by a judge or another independent body. Furthermore, targeted individuals must be notified about the request as soon as this can be done without endangering a criminal investigation or other preponderant interests, so that they will have the opportunity to retrospectively challenge the request and the manner in which it was executed. Where a notification is unfeasible for an indefinite time, the decision not to notify the target should be reviewed by a judge or another independent body.

IV.3. Overarching Considerations for Legislative Reform

Whether a particular Member State requires new legislation in order to allow for the above forms of public-private cooperation depends of course on whether current general laws already provide a legal basis. However, even where existing laws may be interpreted as already allowing cooperation between competent authorities and obliged entities through public-to-private information sharing, there will still often be a strong case for enacting special legislation for this purpose. Otherwise, the law is unlikely to accommodate the numerous legal challenges that result from a partial transformation of the AML/CFT regulatory system into a system in which personal data does not unilaterally flow from the private to the public sector, and instead obliged entities' AML/CFT tools are increasingly steered and utilised by authorities.

Just as importantly, before policymakers move towards authorising public-to-private information sharing within the AML/CFT framework, there must be a transparent debate on the root causes of the unsatisfactory results of current anti-financial-crime efforts. While information sharing can improve obliged entities' ability to detect financial crime, other factors are at least as important for the effectiveness of the framework. Not least of all, there is a need for the judiciary, police, FIUs and supervisory authorities to be equipped with sufficient personnel and technical resources to investigate financial crime and enforce the regulatory framework. Policy discussions about the introduction of information-sharing mechanisms must therefore not be allowed to distract from the fact that often the underperformance of the current framework is likely due not least to an under-resourcing of competent authorities, a root cause that information sharing will certainly not remedy. Far from it: as the present recommendations indicate, meaningful public-to-private sharing requires more, not less, involvement of competent authorities. Given that public-to-private information sharing implies substantial interference in the fundamental rights of citizens, the very necessity of such interference can be in doubt if public-to-private information-sharing powers are not combined with an appropriate commitment to supplying the relevant authorities with adequate resources.

Finally, legislators should be aware that more frequent and potentially extensive public-to-private sharing of personal data by competent authorities necessarily leads to a further expansion of the role of private businesses in the fight against crime. While the nature of today's criminal policy challenges makes this seem to some extent necessary and desirable, policymakers should not lose sight of any structural and longer-term consequences that may result from increasing dependence on private support. To provide only one example, one may highlight the rather high probability that frequent interaction between competent authorities and obliged entities will prompt these entities to take a growing interest in hiring compliance professionals with a law enforcement background. While such recruitment also comes with advantages for authorities (not least, a facilitation of trust between both sides), it can lead to growing competition between the public side and the private side in the search for law-enforcement-minded professionals, and in extreme cases may even

raise integrity issues. Such considerations are not in themselves arguments against closer cooperation, but they may require legislators and competent authorities to think creatively about ways to reduce detrimental effects. Member States should take such considerations into account especially if their competent authorities' institutional culture, traditional career paths, salary structure, and retirement schemes do not usually anticipate career changes between authorities and private entities. In some cases, staff-planning security as well as integrity considerations may then suggest introducing mechanisms such as waiting periods in the case of some career track changes.