Council of the
European Union

Brussels, 20 March 2023
(OR. en)

7184/23

LIMITE

COSI 43
ENFOPOL 106
IXIM 45
CATS 17
COPEN 66
CYBER 53

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	5601/23
Subject:	Proposal to establish a High-Level Expert Group on Access to Data - Compilation of replies by delegations

Following the request for written contributions on the above-mentioned proposal (CM 1815/23), delegations will find in Annex a compilation of the replies as received by the General Secretariat.

ANNEX

WRITTEN REPLIES SUBMITTED BY DELEGATIONS on doc. 5601/23

Table of contents

BELGIUM

Speaking notes COSI 22/02/2023

3. Going Dark: access to data for judicial and law enforcement purposes – the way forward

- Belgium welcomes the Presidency's initiative to organise a debate on how we should best prepare our joint efforts in further identifying a (legally) well-balanced, concise and operationally feasible way forward.

- In the meantime we confirm our firm belief that it is crucial for our law enforcement services to secure a continued lawful access to digital data in order to fight serious and organised crime.

- However, it is a challenging, broad and very complex issue, not only because digital technology and its application possibilities are evolving at lightning speed, but also because we need to strike the right balances at different levels. Not only with regard to data protection and fundamental rights, but also with regard to commercial interests and business models that guide the industry.

- A lot of work – both formally and informally – has already been done. We agree that we should take stock of those efforts and need to take this into account when deciding on the scope of the subjects we would like to focus on, in order to avoid future overlap.

Belgium believes it would probably be best to limit the subjects to what is most pressing. In that respect we believe that further work on encryption and data retention should be prioritized.

Once we undertook the aforementioned stock-taking exercise, we can than consider the exact scope and definition of the most pressing problems our judicial and law enforcement services are confronted with today and find appropriate solutions to resolve them.

- Subsequently, we can decide if and how the concept of a new High Level Expert Group is the best way to proceed. Involve technical experts its our experience that you have to have a profound knowledge of the involved digital technologies.

Specifically with regard to the future activities addressed in the Multiannual Plan, Belgium believes that most of the activities should be directed to a "transversal" support of the Agencies and Member states. In order to be complementary to the work that is already ongoing in the Innovation Lab of Europol, we believe it should involve four core tasks:

- Horizon scanning and technology foresight, for the benefit of all agencies, whether or not in cooperation with, or through, the Europol Innovation Lab,. This activity should also provide the requested "Technology radar".

- Connecting the various networks working in specific domains, e.g. around AI, Encryption, Drones and Biometrics, rather than starting additional projects in these domains themselves since a lot is already happening in expert networks.

- (Support for) building an EU infrastructure useful for innovation. This concerns cross-cutting needs such as 2) data space for internal security, 3) Mapping of innovation initiatives within the EU, ...

- Identification of possible - financial - EU support for the initiatives in the different networks; thus strengthening existing networks/initiatives rather than starting new ones.

CZECH REPUBLIC

Going Dark

CZ comments on ST 5601/23

Pursuant to request by the Presidency, CZ focuses its comments on the main areas and challenges that should form remit of HLEG.

Focus Areas / Challenges Explicitly Mentioned by the Presidency

CZ understands that SE Presidency does not identify the areas and challenges in exhaustive manner. The examples explicitly mentioned by the Presidency document 6501/23 include:

- access to encrypted communications
- improved international cooperation to ensure (cross-border) access to evidence
- clear legal framework for data retention
- measures to address volatility of electronic communication
- jurisdictional issues related to loss of location

CZ considers these focus areas to be relevant and supports the HLEG to focus on them.

Additional Focus Areas / Challenges of Concern to CZ

CZ believes that HLEG should also focus on:

- access to encryption of static (stored) data
    - even if the information was not subject to lawfully intercepted communication and was found using other lawful measures (e.g. house search) stored on data carrier (eg. data stored on HDD encrypted with TPM chip), the encryption still poses serious challenges
- unreliable registration of internet domains
    - true owners of illicit internet domains can effectively evade law enforcement by using false identities.
- misuse of anonymization measures on the internet
    - measures that increase anonymity (such as VPN or TOR networks) are frequently misused by criminals in the course of illicit activities.

Prioritization of Focus Areas / Challenges in the View of CZ

CZ proposes following prioritization of the above-mentioned issues:

1. access to encrypted communication
2. access to encrypted static data
3. improved international cooperation to ensure (cross-border) access to evidence
4. clear legal framework for data retention (of growing importance e.g. to distinguish legitimate calls from fakes using combination of contact number spoofing with AI voice manipulation)
5. jurisdictional issues related to loss of location
6. unreliable registration of internet domains
7. misuse of anonymization measures on the internet

ESTONIA

Dear Presidency,

First of all, as I also stated at the last COSI meeting on Feb 22, let me emphasise again that we are very grateful that the Swedish Presidency has taken this topic as one of the priorities of their presidency period. I hope the decisions made during the following months will carry on with next presidencies as well. The issue with the data retention and access to data is already a fundamental issue when we're talking about fighting against serious crime and national security activities. If we don't find solutions now, we can only expect the situation to get exponentially worse.

I did express our standpoint at the COSI meeting as well, but I was relatively general in my wording there. Therefore, I will now outline in a little more detail what, in our opinion, should be taken into account when planning the future HLEG activities:

1) Data retention – Data retention is the basis of this whole topic. Simply put: if there is no data retained, there is no point in talking about access to data. At least historical data. But as we know, regarding criminal investigation, in majority of cases we're talking about data that was created before the investigation even started. This is a broad problem that concerns traditional electronic communication data, alternative electronic communication data, passenger data but also the data about material shared online in general. For example, child sexual abuse material and the CSAM proposal, criminal activity online and the DSA regulation and even terrorist content and the TCO regulation. The common keyword for all these and probably several more topics is data retention.

The European Court of Justice (ECJ) has made numerous decisions on data retention. As a result, general data retention is currently essentially prohibited in EU Member States. Having represented Estonia in ECJ proceedings more than a few times, I can say that a lot of the interventions in the hearings bring out that it is not possible to implement the solutions proposed by the ECJ. Person-specific, geographic and/or post-investigation data retention rules do not serve its purposes. The for us negative ECJ rulings are mainly based on violating the principles set in the Charter of Fundamental Rights. Mainly the fundamental right to privacy. Having said that, I'm really glad that after the informal JHA meeting in January, where the Swedish National Police Commissioner gave a presentation and emphasised the importance of the rights of the victims, that several Member States have taken that exact rhetoric to their next interventions in several working party meetings. Finally the understanding begins to emerge that there are other fundamental rights as well that must be guaranteed: the safety and security of everyone, everyone's right to life and health, etc.

On the other hand, it is also possible to understand the logic of ECJ. They have virtually no other EU legislation to base their decisions on. Therefore, they are forced to always refer to the Charter of Fundamental Rights. In the current situation, it's fair to say that the ECJs hands are a little bit tied until the EU comes up with a solution that would allow them to reassess the principles and approach to this. It is clear that right now this is not a sustainable solution.

We therefore propose that first we should map the legislation of the Member States in order to clarify what is the situation all around. After that we could take into consideration the various analyses and case studies that have been made by different (including non-EU) countries (for example Australia has brought EU experience as a bad example when justifying their position). Thereupon a regulation should be developed for data retention, which is not necessarily field- or sector-specific, but then applies to all concerned regulations like an umbrella.

2) Access to data - Although there are also several issues with access to data as well, compared to data retention, it is a slightly different problem. The ECJ has said that the data can be accessed for the purpose of fighting against serious crime, for the purpose of internal security or if the only possible way to detect a crime is based on the concrete data (for example IP-address). The latter is usually referred to as crime with a clear cyber element.

Therefore, it is important to assess whether, in the light of such rules, it is possible to actually investigate some of the easier crimes for which the data is inevitably necessary. The same question concerns national security. Whereas Article 4 paragraph 2 of the Treaty on the European Union states that national security of a Member State remains the sole responsibility of each Member State. Can the ECJ intervene in the national security of a Member State, and if so, do the rules of data access impair the capabilities of security agencies?

3) Encryption – And now, on top of the previous two problem areas, we also have to deal with encryptions. Due to the development of technology, we are faced with a situation where encrypted communication, data and content can lead to a situation where regardless of the solution of the previous two problems, we could still be *going dark*.

Coming back to my initial remark, where I said that law enforcement agencies usually react after the deed is done, it is important to definitely deal with the topic of data retention before or at least in parallel to the encryption issue. Otherwise, it doesn't matter much if the content is encrypted if the data simply isn't there. Since the problem of data retention has existed for many years, we are probably forced to deal with these things at the same time. Especially considering the rapid development of technology.

Since it is just one element of a wider problem, the recommendations of the previous points are also applied here. In order to activate the discussions in informal COSI and other working groups (including HLEG) in the future, I will share some thoughts. Several Member States have said that end-to-end encryption (E2E) systems should not be weakened. This is also the official position of Estonia. But what is exactly meant by weakening the E2E? If the service provider, court or some other institution has the key, is the E2E weaker? Perhaps we are talking about the reluctance to technical weakening of the system? In other sense, is the door weaker if someone has the key?

In conclusion, these are the main problem areas that would need immediate discussions. Whereas they are in order of importance. Of course, there are still problems in defining service providers, for example to whom the obligations apply. Today, virtually anyone can offer a service almost without realizing it. It is clear that not everyone is able to follow the rules set for service providers. There are also questions arising from introduction of 5G services. But these are all details that can be discussed during the main discussions. Also, Member States would need to coordinate the inputs to ECJ proceedings as said at the COSI meeting as well.

It is important to set a clear scope and proceed step by step. Otherwise, we could find ourselves in a position where we are at awe of the size of this issue and cannot make necessary progress.

So, maybe it’s not a lot but I hope you get some ideas from this. If you have any questions or you want to discuss this topic in the future, I’m always willing to do that.

GREECE

Athens, 01.03.2023

HELLENIC REPUBLIC
MINISTRY OF CITIZEN PROTECTION
HELLENIC POLICE HEADQUARTERS
SECURITY BRANCH
INTERNATIONAL POLICE COOPERATION DIVISION

EL WRITTEN COMMENTS

Subject: Proposal to establish a High-Level Expert Group on Access to Data

- What is important is to further strengthen law enforcement authorities with innovative tools and initiatives aimed at making the most of the opportunities of the digital era, as well as at preventing and tackling organised crime. The extent and the method to be used in developing such new support tools require us to closely analyse all the specific aspects of the matter.
- In light of this, the Presidency's proposal to establish a High-Level Expert Group on Access to Data clearly moves in the right direction.
- Consideration should be given to developing cooperation between the new structure and existing structures within the Union with relevant experience in data access, so as to draw upon the experience accumulated so far and avoid any overlapping.
- The main areas and challenges that should be the primary focus of the HLEG are the following:
    - the possibility of gaining access to encrypted communications,
    - the need for enhanced international cooperation with a view to ensuring access to evidence, given the inherent cross-border nature of today's digital services and criminal activities,
    - the need for a clear legal framework on data retention, etc.

- We certainly agree that the High-Level Expert Group (HLEG) should be co-chaired by the Commission and the Presidency.

- As regards the involvement of non-institutional actors, as appropriate, we see it in a positive light, as it envisages the invitation of a wider range of competent bodies with specialised knowledge; we are, however, reserved with regard to the legal framework of their participation, especially when it comes to private bodies. We suggest that the terms of the invitation, participation and utilisation of the input of non-institutional actors should be more clearly detailed and agreed upon.

FRANCE

NOTE DE COMMENTAIRES DES AUTORITES FRANCAISES

Objet: Note de commentaires - Appel à contributions au sujet de la mise en place d'un groupe d'experts de haut niveau (HLEG) sur l'accès aux données, discutée à l'occasion du COSI du 22 février 2023

Références: 5601/23

Pour faire suite au COSI du 22 février 2023, un appel à contribution a été lancé à l'intention des Etats-Membres au sujet de la mise en place d'un groupe d'experts de haut niveau (HLEG) sur l'accès aux données, décrit dans le document de travail de la Présidence 5601/23.

Cet appel à contribution concerne les principaux domaines et défis qui devraient être au centre des préoccupations du groupe d'experts et / ou de ses sous-groupes.

En réponse à cette demande, les autorités françaises remercient la présidence suédoise d'avoir mis ce sujet d'intérêt majeur dans son programme de travail. La France, qui avait déjà cherché à signaler l'importance du sujet sous sa présidence du Conseil, au premier semestre de l'année dernière, souscrit pleinement à l'approche pluridisciplinaire et transversale proposée par la présidence et partage la nécessité d'associer tant la filière JAI que les autres filières du Conseil, compte tenu des nombreuses initiatives législatives pouvant avoir des implications importantes pour les autorités policières et judiciaires qui y sont discutées. A cet égard, les autorités françaises suggèrent d'organiser un COSI-CATS qui permettrait utilement de faciliter les convergences indispensables entre instances pour traiter ce sujet à fort enjeu. En tout état de cause, le sujet des données doit être abordé de manière globale et cohérente, et ne pas se limiter aux questions d'accès, mais également de conservation et d'exploitation.

Principe du groupe d'experts de haut niveau:

Les autorités françaises soutiennent la mise en place d'un groupe d'expert de haut niveau sur le sujet de l'accès aux données et soulignent l'importance d'une forte implication des instances du Conseil dans le pilotage de ces travaux. Une co-présidence par la Commission et la présidence tournante du Conseil, ainsi qu'un suivi régulier de l'avancement des travaux par le COSI, en lien avec la filière justice, semble acceptable.

Les autorités françaises rappellent que la plupart des enquêtes ont maintenant une dimension numérique, dès lors que la criminalité recourant aux outils numériques prend une dimension massive. Non seulement les criminels et terroristes utilisent les outils numériques comme tout un chacun, mais les organisations criminelles et terroristes y ont recours pour développer leurs activités à une vitesse et à une échelle inconnues jusqu'ici. L'exemple le plus frappant, ces dernières années, est les centaines de millions de messages à exploiter dans les affaires Encrochat et Sky ECC. Or, alors que la disponibilité et l'accès aux données numériques sont essentiels dans la lutte contre la criminalité et le terrorisme, les autorités investies des missions de prévention et de répression de ces actes accumulent des retards préoccupants face à des groupes criminels et terroristes de plus en plus innovants. Les défis auxquels sont confrontés les services compétents sont multiples, qu'il s'agisse de la généralisation – qui n'est pas contestée dans son principe – du chiffrement des communications électroniques, de l'accès aux preuves numériques conservées dans des entrepôts de données hors de l'Union européenne, de la complexité des compétences juridictionnelles pour traiter de phénomènes ou encore de la nécessité de disposer d'un cadre juridique clair en matière de conservation des données de connexion et de préserver l'efficacité des outils d'enquête.

Priorités du groupe d'experts de haut niveau:

Parmi les principaux domaines et défis qui devraient être au centre des préoccupations du groupe d'experts, les autorités françaises souhaitent, que celui-ci effectue un travail de recensement des différents textes européens, toutes filières confondues, existants ou en cours de discussion, ayant un lien avec le sujet de l'accès aux données. Ce travail devra être fait en lien avec le SGC. Il pourrait également être opportun de dresser un état des lieux des évolutions technologiques en cours et à venir, qui pourraient avoir des conséquences pour les services enquêteurs. En tout état de cause, le groupe d'experts de haut niveau ne devra pas être un outil de transposition de la jurisprudence désormais constante de la CJUE en matière de conservation et d'accès aux données dans un cadre répressif, mais devra être une instance qui proposera des orientations concrètes face aux défis et difficultés auxquels les forces de sécurité intérieure font face dans ce domaine. Il sera donc nécessaire de définir un mandat clair et une méthodologie précise qui incombera au groupe d'experts pour dégager un cadre commun de conservation et d'accès aux données qui soit équilibré au regard des impératifs préventifs et répressifs que poursuivent les États membres.

Composition du groupe d'experts de haut niveau:

Les autorités françaises soutiennent dans son principe la proposition de la présidence d'impliquer tous les acteurs concernés, y compris non institutionnels, afin de travailler à un consensus européen sur le sujet de l'accès aux données. Il convient néanmoins d'identifier les modalités de cette association (probablement en fonction des sous-groupes), de manière notamment à ce que les échanges entre praticiens des États membres ou les discussions entre acteurs législatifs puissent se dérouler si nécessaires en respectant les impératifs de confidentialité. Les autorités françaises souscrivent également à la proposition de la présidence de créer des synergies avec les structures et forums existants, tels que l'EU Internet Forum ou l'Hub d'innovation de l'UE. D'une manière générale, nous devons tous travailler à rétablir la confiance sur l'accès aux données. Entre les forces de sécurité intérieure, les magistrats, les juristes, les entreprises, il est essentiel de se parler pour lever les malentendus. C'est pourquoi la présidence française a tenté en avril 2022 d'instaurer un cadre de dialogue décloisonné, avec les États membres mais aussi la société civile, les autorités de protection des données, des magistrats, des parlementaires ou encore des opérateurs d'Internet et de l'industrie du numérique. Elle invite les futures présidences à pérenniser cette initiative, afin d'inscrire ce dialogue dans le long terme, au-delà des travaux qui pourront être menés par le groupe d'experts de haut niveau.

Courtesy translation:

NOTE OF COMMENTS FROM THE FRENCH AUTHORITIES

Subject: Comment note - Call for contributions on the establishment of a High Level Expert Group (HLEG) on data access, discussed at the COSI on February 22, 2023

References: 5601/23

As a follow-up to the COSI of 22 February 2023, a call for input has been issued to Member States on the establishment of a High Level Expert Group (HLEG) on Data Access, as described in Presidency Working Document 5601/23.

This call for contributions concerns the main areas and challenges that should be the focus of the expert group and/or its subgroups.

In response to this request, the French authorities thank the Swedish Presidency for having included this subject of major interest in its work program. France, which had already sought to highlight the importance of the subject during its Presidency of the Council in the first half of last year, fully endorses the multidisciplinary and cross-cutting approach proposed by the Presidency and shares the need to involve both the JHA channel and the other channels of the Council, given the many legislative initiatives that may have significant implications for the police and judicial authorities that are being discussed there. In this respect, the French authorities suggest the organization of a COSI-CATS which would be a useful way to facilitate the convergence that is indispensable between bodies in order to deal with this high-stakes subject. In any case, the subject of data must be approached in a global and coherent manner, and not be limited to questions of access, but also to questions of conservation and exploitation.

Principle of the high-level expert group:

The French authorities support the establishment of a high-level expert group on the subject of access to data and stress the importance of a strong involvement of the Council bodies in the steering of this work. A co-presidency by the Commission and the rotating presidency of the Council, as well as regular monitoring of the progress of the work by the COSI, in conjunction with the justice sector, seems acceptable.

The French authorities remind us that most investigations now have a digital dimension, as crime using digital tools takes on a massive dimension. Not only do criminals and terrorists use digital tools like everyone else, but criminal and terrorist organizations are using them to develop their activities at a speed and scale never seen before. The most striking example in recent years is the hundreds of millions of messages to exploit in the Encrochat and Sky ECC cases. Yet, while the availability of and access to digital data is critical in the fight against crime and terrorism, the authorities tasked with the prevention and suppression of these acts are falling alarmingly behind in the face of increasingly innovative criminal and terrorist groups. The challenges faced by the competent services are multiple, whether it is the generalization - which is not contested in principle - of the encryption of electronic communications, access to digital evidence stored in data warehouses outside the European Union, the complexity of jurisdictional competences to deal with phenomena, or the need to have a clear legal framework for the conservation of connection data and to preserve the effectiveness of investigation tools.

Priorities of the high-level group of experts:

Among the main areas and challenges that should be at the center of the expert group's concerns, the French authorities would like the group to carry out a survey of the various European texts, all sectors included, that exist or are under discussion, and that are related to the subject of access to data. This work should be done in conjunction with the GSC. It might also be appropriate to draw up an inventory of current and future technological developments that could have consequences for the investigating departments. In any case, the high-level group of experts should not be a tool for transposing the now constant case law of the CJEU on data retention and access in a law enforcement context, but should be a body that will propose concrete orientations to face the challenges and difficulties that internal security forces are facing in this area. It will therefore be necessary to define a clear mandate and a precise methodology for the group of experts in order to find a common framework for data retention and access that is balanced with the preventive and repressive imperatives of the Member States.

Composition of the high-level group of experts:

The French authorities support in principle the Presidency's proposal to involve all the actors concerned, including non-institutional ones, in order to work towards a European consensus on the subject of access to data. However, the modalities of this involvement (probably depending on the sub-groups) should be identified, in particular so that exchanges between practitioners in the Member States or discussions between legislative actors can take place, if necessary, while respecting confidentiality requirements. The French authorities also agree with the Presidency's proposal to create synergies with existing structures and forums, such as the EU Internet Forum or the EU Innovation Hub. In general, we must all work to restore confidence in data access. It is essential that we talk to each other to remove misunderstandings between the internal security forces, the judiciary, legal experts and companies. This is why the French presidency attempted in April 2022 to establish a framework for open dialogue with Member States, but also with civil society, data protection authorities, judges, parliamentarians, and Internet and digital industry operators. It invites future presidencies to make this initiative permanent, in order to make this dialogue long-term, beyond the work that may be carried out by the high-level group of experts.

CYPRUS

As regards the main areas and challenges that the HLEG should primarily focus on, we believe that these should be:

- the decryption of stored content and live communication

- The gaps created by the Decisions of the ECJ on the issue of data retention

Providing always the appropriate safeguards for the fundamental rights protection, including of course the victims' protection.

LATVIA

Please find below LV contribution on HLEG.

HLEG as an "umbrella format"

LV supports the establishment of HLEG and sees it as a comprehensive umbrella format. Thus, discussions regarding lawful access to data for judicial and law enforcement purposes should be maximally concentrated within the HLEG and – from the moment the HLEG is established – parallel discussions in other formats (in particular, in the relevant Council and Commission formats) should be avoided as much as possible (to avoid fragmentation and duplication of efforts).

In case certain (specific) issues related to "going dark" are not covered by the HLEG mandate (for instance, pilot projects of the EU Innovation Hub for Internal Security), HLEG should be regularly informed about them since discussions held in other formats might possibly feed-in in the work of the HLEG (LV sees that a clear mapping of such formats and the issues covered in these formats would be of an added value).

Mandate (substance)

LV agrees that HLEG mandate should be precisely defined; it shall also be limited in its nature by covering such core issues at stake as data retention, data acquisition and encrypted data. LV also finds it important that HLEG work results in very concrete legislative and non-legislative (incl. practical) short-, medium- and long-term recommendations.

Organisational set-up

LV believes that the High-Level Expert Group on Information Systems and Interoperability should serve as a role model for organisational matters (for instance, regarding the involvement of non-institutional actors).

At the same time, LV agrees that HLEG (unlike High-Level Expert Group on Information Systems and Interoperability) should be co-chaired by the Commission and the Presidency (this model would ensure both continuity and a clear link to the relevant Council formats). In addition, LV considers that impartiality should be maintained throughout the process, therefore – in case HLEG subgroups are created – LV tends to believe that they also should be co-chaired by the Commission and the Presidency.

Monitoring

LV considers that COSI should be responsible for monitoring (for the sake of effectiveness, one central "owner" at the Council level would be desirable); other relevant Council's committees and working parties (for instance, CATS) should be regularly briefed on HLEG work.

LITHUANIA

In accordance to the last COSI meeting scheduled on 21st February 2023, we would like to provide you with the following insights from delegation of Lithuania for the document no. 5601/23 "Proposal to establish a High-Level Expert Group on Access to Data":

We think that the expert group approach is suitable in this complex situation, to break the gridlock.

First of all, because it offers the opportunity to change the narrative, and build trust among stakeholders, because now it seems the narrative is more about suspicions and conflicting views than working together. Secondly, Law enforcement deserves to be trusted, because it safeguards our essential values

Results of the work of the expert group should break and turn around the wrong impression that law enforcement is the main source of risk to the fundamental rights. However, we see one challenge – matching this ambition with the commitment. Therefore, we think it is important:

- To set very precise and concrete the goals and deliverables for the group, so that outcomes are actionable, and we are not bogged down in discussions without results. This set of deliverables could be endorsed by COSI

- To make sure that every participating stakeholder is bound by the set of goals and directly contributes to the outcomes. We would favor wide representation, including data protection and industry representives

- To avoid duplication with other already existing formats, rather to absorb their observations

- to explore the legal basis and it's adequacy, possiblitity -considering of creating of new legal regime

Also, one more idea to explore – besides legislative and practical proposals expert group might also evaluate the necessity to develop relevant tools for law enforcement needs and recommend for Innovation Hub or relevant agencies to explore it further on.

The main areas of primary focus could be – data retention, data encryption (*end-to end encryption*), cooperation between law enforcement and judicial authorities.

POLAND

Please find below PL position concerning the proposal to establish a High-level expert group on access to data:

PL would like to thank the Swedish Presidency for a proposal of establishing high level working expert group to deal with security challenges in digital era, especially in terms of a lawful access to communications data for the law enforcement and judicial authorities. It is of our great interest to share experiences and join efforts in this area of significant importance for effective prevention, detection, investigation and prosecution of criminal offences.

PL supports the suggested format: co-chairing by the Presidency and the Commission, expert-level subgroups as well as involvement of all relevant stakeholders in order to break the silo approach and take steps toward a joint understanding of the issue of access to data. As regards involvement of non-institutional actors, we are positive about cooperation with academia and industry, especially due to their technical knowledge of providing internet services and connections.

The primary focus of the HLEG and its sub-groups should be data retention, data encryption and decryption and localisation data.

SLOVENIA

Written comments of Slovenia regarding the proposal to establish a High-level expert group on access to data (ref. CM 1815/23)

Slovenia would like to thank the Presidency for preparing the discussion paper "Proposal to establish a High-Level Expert Group on Access to Data", doc. 5601/23 for the COSI meeting of 22 February 2023 and would like to provide the following responses to the questions contained in the discussion paper.

Slovenia thanks the Swedish Presidency for giving such high priority to the issue of access to data, which is key to ensuring that law enforcement authorities can continue to carry out their tasks and responsibilities in an ever more digitalized society.

Slovenia welcomes the initiative of the Presidency to move the discussions towards more practical solutions and fully supports the setting-up of a High-Level Expert Group.

The Group's primary focus should be on finding practical solutions as regards the necessary legal basis for access to data, especially in connection to data retention and encrypted information. Another focus for the group could be finding the necessary technical tools, which will be useful in practice and at the same time subject to adequate safeguards.

Slovenia supports the proposal that the Group should be co-chaired by the Commission and the Presidency.

Slovenia agrees that the Group should bring together a wide variety of stakeholders who could contribute to the discussions, including non-institutional actors, bearing in mind that the primary goal should always be on practical results of the discussions. The involvement of private companies is especially important, since they are best able to contribute with their expertise on cyber tools.

The existing structures and ongoing work should be fully taken into account, to ensure that the activities are consistent, that they are not duplicated and that we are mindful of how we are using our limited resources, both in terms of experts available to work in these initiatives as well as financial and other resources.

SLOVAKIA

03/03/2023

Written contributions for doc. No. 1815/23 and pertaining to doc. No. 5601/23 regarding the creation of the High-level expert group on access to data by the Slovak Republic

We agree with the proposed approach by the presidency.

We consider the main challenge from our point of view to be access to electronic evidence due to the repeal of the Data Retention Directive. As a result of the judgment of the Court of Justice of the European Union in the Joined Cases C-293/12 and C-594/12 of 8th April 2014, and the judgment of the Constitutional Court of the Slovak Republic of 23rd April 2014, certain provisions of the Electronic Communications Act, which required telecoms operators to store and provide data on phone calls and internet communication upon request of the state authorities, were first suspended and then repealed in the Slovak Republic. The provision of this act which set the retention period for the data was also repealed. As a result, each of the telecoms operators in the Slovak Republic now voluntarily determines whether to store these data and if so, for how long. Some do not store these data at all, which complicates and, in some cases, even hinders criminal proceedings for the state authorities.

The legislative status creates a disharmony between the police's capabilities and the protection of personal data in harmony with the respect for private and family life on the other. We believe that the police should have the possibility (at least minimal) to detect perpetrators of criminal activity committed through computer technologies. In correlation with this undesirable state, it is necessary to state that the Police Force in the Slovak Republic always has been and still is under the control of the competent prosecution (which supervises the lawfulness and justification of the request) and it is dependent on the issuance of the order of the relevant court to the telecommunications operator for the provision of such data.

For this reason, we propose that the HLEG focus primarily on the revival of the topic of adoption of legally binding legislation in all Member States of the European Union that would introduce at least minimum possibilities for obtaining telecommunication data necessary for criminal investigations, set firm conditions for obtaining, controlling, misusing, and minimizing criminalization of all citizens on the other hand.

Our recommendation is to add the need to change the commonly used terminology. In documents dedicated to data retention, the discussion should not revolve around the conflict between the effectiveness of law enforcement agencies on one hand and about the protection of personal data on the other. We should regularly emphasize that there is a conflict between the levels of protection of various fundamental rights. Currently, because of the case-law of the Court of Justice of the European Union (derived only from secondary legislation) there is disproportionate protection of the right to privacy (protection of personal data of a possible perpetrator) at the expense of the protection of other (more important) fundamental rights of the victim of a crime. We are convinced that a change in such a terminology can eventually lead to

a change in political perception in the European Parliament, which will be crucial for any future changes to secondary legislation interpreted by the Court of Justice of the EU.

We also agree that the group should be co-chaired by the Commission and the Presidency, as well as regarding the involvement of non-institutional actors where appropriate.

We are of the opinion that the HLEG should make use of the existing working groups such as the Working Party on Judicial Cooperation in Criminal Matters (COPEN) and the Working Party on JHA Information Exchange (IXIM), which have already done a lot of work in connection with the access to data for criminal proceedings. Furthermore, regarding the discussion with the competent authorities, if the discussion is to be held at COSI, we recommend that it should also be reflected in CATS when it pertains to the judicial aspects.

Best regards,

Col. JUDr. Lucia Szlobodová
Director of the International Police Cooperation Bureau
Presidium of the Police Force
Ministry of Interior of the Slovak Republic

&

Zuzana Štofová
Director of the European and Foreign Affairs Division
International Law Department
Ministry of Justice of the Slovak Republic

FRA

COSI – written contribution by EU Fundamental Rights Agency (FRA) regarding a proposal to establish a High-level expert group on access to data (5601/23).

FRA welcomes the proposal to establish a High-Level Expert Group on Access to Data. We stand ready to support the EU Institutions, the Presidency and the Member States in this regard with our evidence-based advice.

With respect to the first question, we would like to outline some basic parameters.

In order for the police and the judiciary to do their job – including when seeking to access data – without infringing fundamental rights, the principles of legality, necessity and proportionality have to be respected when considering any limitations on rights.

The challenge is how to calibrate this, to ensure that any necessary limits on rights – such as the right to privacy – are not excessive.

To this end, various discussions have underlined that any limitation on people's rights, for the purpose of accessing digital data, need to be targeted; that is, not done in a blanket way that impacts everyone.

Herein – it is important that the future HLEG and its sub-groups address not only principles of law in an abstract sense. In our view, they should also focus on practical challenges and solutions when it comes to 'what works' and 'what could work' with respect to access to data, and what this would mean with respect to fundamental rights.

It is important that real-life 'use cases' are addressed through the work of the HLEG and its sub-groups. FRA's own work on artificial intelligence has focused on such use cases, and used computer simulations to test algorithms and identify both the negative and positive implications for fundamental rights – for example, in the field of predictive policing.

Furthermore, FRA considers that fundamental rights should be mainstreamed appropriately across the work of the HLEG and its sub-groups discussing individual topics.

In response to the third question, it is important that the HLEG involves non-institutional actors, as appropriate. This should include not only actors from the industry developing and marketing tools for data analytics in law enforcement, but also actors that can independently assess these tools with respect to their efficacy, technical feasibility and their potential rights implications.

With respect to the fourth question, the HLEG can benefit from on-going work in closely related fields; notably those concerning the proposed AI Act, which at its heart focuses on access to data for different purposes, including by law enforcement. The work of the Innovation Hub for Internal Security, that FRA is part of, also appears highly relevant.

FRA has been a member of other high-level expert groups; namely – HLEGs on information systems and interoperability, on radicalisation, and on artificial intelligence.

We were able to contribute to these groups by drawing on our empirical research, which engages different actors, alongside our broad understanding of the application of fundamental rights in practice – which extends beyond data protection and privacy.