TRANSPARENCY AND PRIVACY IN DEMOCRATIC SOCIETIES: TWO SIDES OF THE SAME COIN

TRANSPARENCE ET VIE PRIVÉE DANS LES SOCIÉTÉS DÉMOCRATIQUES : LES DEUX FACES D'UNE MÊME MÉDAILLE

Workshop Proceedings
Strasbourg, 4 November 2025

Actes d'un Atelier
Strasbourg, 4 novembre 2025

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

TRANSPARENCY AND PRIVACY IN DEMOCRATIC SOCIETIES – TWO SIDES OF THE SAME COIN /

TRANSPARENCE ET VIE PRIVÉE DANS LES SOCIÉTÉS DÉMOCRATIQUES : LES DEUX FACES D'UNE MÊME MÉDAILLE

Proceedings of the Workshop

Actes de l'Atelier

Layout: SPDP, Council of Europe

Printed at the Council of Europe

Mise en page : SPDP, Conseil de l'Europe

Imprimé dans les ateliers du Conseil de l'Europe

Opening speech / *Discours d'ouverture*

Strasbourg, 4 November */ novembre* 2025

Welcome members of the Council of Europe Access Info Group, the Committee of Convention 108 and GRECO, as well as independent experts.

Welcome the initiative of this workshop as a good practice of transversal dialogue and co-operation in the Council of Europe.

This facilitates our common understanding of challenges to the protection of privacy and to the strengthening of transparency of our public administrations.

It also renders our voice more coherent and stronger.

The Secretary General of the Council of Europe has launched a New Democratic Pact for Europe.

Its goals are: to confront democratic backsliding; to resist polarisation in our societies; and to restore people's trust in democratic institutions by making it tangible for their daily lives.

It will be one of our Organisation's responses to the multiple challenges that our societies are facing, including to our collective security.

As our Secretary General repeatedly underlines – we must speak not only of military security, but also of democratic security.

The values that you are defending in each of your monitoring bodies are indicators of democratic security and good governance.

Transparency of public authorities is fundamental to good governance. A society's commitment to transparency and anti-corruption efforts serves as an indicator of its democratic strength and resilience.

Transparency empowers citizens to hold those in power accountable, openly criticise governance and engage meaningfully in the decision-making process.

In short, transparency reinforces their legitimacy in the eyes of the public and its confidence in them.

The right to privacy as an enabling right plays a crucial role in the enjoyment of other rights enshrined in the ECHR.

The responsible processing of personal data is also an important indicator of good governance and of the overall state of democracy in a country.

But the protection of privacy cannot serve to cover up corruption, bad management or poor public administration. As the European Court of Human Rights has stated, the right to privacy should be balanced against other rights in the Convention, notably the freedom of expression, for the purpose of transparency, participatory processes and democratic debates.

This event is a perfect forum to start discussing this balancing exercise. The voices of your monitoring bodies are very important in this context.

Transversal dialogues such as this one are necessary to help the Council of Europe monitoring bodies to ensure accuracy, balance, and coherency in their monitoring work.

The theme that you have chosen to debate in this workshop – the intersection between privacy and the transparency of the public administration – shows that you care about getting the balance right.

Invite the TP-D, the AIG and GRECO to view themselves as integral parts of a collaborative community of Council of Europe monitoring bodies, working in an integrated manner towards a shared goal. Each brings unique perspectives and expertise that ensures high quality outcomes, while respecting their distinct mandates and responsibilities.

By promoting coherence in communication with members or State Parties, and aligning messages strategically, all three bodies can ensure that their distinct approaches not only complement and reinforce each other's work but also present a unified front that

enhances impact and credibility in advancing integrity, transparency, and respect for privacy.

The Tromsø Convention now has 17 Parties. All of them are Council of Europe member States.

They represent diverse legal cultures, from the Nordic European countries which have a long-standing legal tradition of openness, to states from eastern and central Europe with recent access to information laws, generally modelled after the Convention.

We have come a long way from December 2020 when the Convention entered into force upon its ratification by its 10th State Party.

When the Convention was drafted, the consensus was that it should contain basic obligations reflecting what was already accepted in existing national laws and could also be accepted and implemented by States that lacked such laws.

This flexibility built into the Tromsø Convention is one of its strengths. It is reflected in the results of the monitoring mechanism of the Convention.

TP-D has more members and observers who can, where appropriate and within their roles, encourage more ratifications of the Tromsø Convention.

For example, in many countries the responsibility for ensuring personal data protection and access to official documents lies with the same authority. These authorities are our natural allies for promoting the ratification of the Tromsø Convention.

Whenever relevant, GRECO has consistently recommended that member states which have not yet done so should ratify the Tromsø Convention, acknowledging its unique value and role in promoting transparency and integrity in public administration. This complementary approach reinforces collective efforts and offers a promising path forward.

Wish to the participants good discussions.

TABLE OF CONTENTS
TABLE DES MATIÈRES

PROGRAMME

Tuesday 4 November 2025		Mardi 4 novembre 2025
Opening of the Workshop by: • **Gianluca ESPOSITO** Director General, Human Rights and Rule of Law • **Helena JÄDERLBLOM** President of the Council of Europe Access Info Group (AIG) • **Beatriz de ANCHORENA** Chair of the Committee of the Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) • **David MEYER** Chairperson Group of States against corruption (GRECO)	09:30	Ouverture de l'Atelier par : • **Gianluca ESPOSITO** Directeur Général, Droits humains et État de droit • **Helena JÄDERLBLOM** Présidente du Groupe Accès à l'Information du Conseil de l'Europe (AIG) • **Beatriz de ANCHORENA** Présidente du Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+) • **David MEYER** Président du Groupe d'États contre la corruption (GRECO)
PANEL 1 **Balancing transparency and privacy – Council of Europe standards** Moderator: **Joan BARATA MIR** Legal expert, Fellow at the Cyber Policy Center of Stanford University • **Päivi KORPISAARI** Professor of Communication Law, Helsinki University, AIG member • **Kristi VÄRK** Director of Data Protection Law Division, Ministry of Justice and Digital Affairs of Estonia	10:00	**SESSION 1** **Équilibre entre transparence et vie privée – les normes du Conseil de l'Europe** Modérateur : **Joan BARATA MIR** Expert juridique, membre du Cyber Policy Center de l'université de Stanford • **Päivi KORPISAARI** Professeure de droit de la communication à l'université d'Helsinki, membre de l'AIG • **Kristi VÄRK** Directrice de la division du droit de la protection des données au ministère de la Justice et des Affaires numériques de l'Estonie

- **Beatriz DE ANCHORENA**
  Head of the Agency for Access to Public Information (AAIP), the Data Protection Authority (DPA) in Argentina

- **Beatriz DE ANCHORENA**
  Head of the Agency for Access to Public Information (AAIP), the Data Protection Authority (DPA) in Argentina

PANEL 2 11:00 **SESSION 2**

Manging information about public officials

Moderator:
Tetyana OLEKSIYUK
Vice-President of the Council of Europe Access Info Group

- **Warren SEDDON**
  Director of Freedom of Information and Transparency, Information Commissioner Office

- **Alessandra PIERUCCI**
  Data Protection Commissioner
  Italy

- **Vladimir GEORGIEV**
  Expert, former Commissioner State Commission for Prevention of Corruption, North Macedonia

- **Carlos CORDERO SANZ**
  Founder of Access Info Europe.

Gestion des Informations relatives aux fonctionnaires

Modératrice:
Tetyana OLEKSIYUK
Vice-presidente du Groupe Accès à l'Information du Conseil de l'Europe

- **Warren SEDDON**
  Directeur de la liberté d'information et de la transparence, Bureau du Commissaire à l'information, Royaume-Uni

- **Alessandra PIERUCCI**
  Commissaire à la protection des données, Italie

- **Vladimir GEORGIEV**
  Expert, ancien Commissaire de la Commission nationale pour la prévention de la corruption, Macédoine du Nord

- **Carlos CORDERO SANZ**
  Fondateur d'Access Info Europe.

PANEL 3 12:00 **SESSION 3**

Managing information about private persons dealing with public authorities

Moderator:
Neus VIDAL MARTÍ
SEEK Initiative Executive Director

- **Elona HOXHAJ**
  General Director on the Right to Information, Albanian Information and Data Protection Commissioner

Gestion des informations relatives aux personnes privées traitant avec les autorités publiques

Modératrice :
Neus VIDAL MARTÍ
Directrice exécutive de *SEEK Initiative*

- **Elona HOXHAJ**
  Directrice générale chargée du droit à l'information, Commissaire à l'information et à la protection des données en Albanie

• **Gonzalo SOSA** Representative of the Electronic Government Agency and the Information and Knowledge Society, Uruguay • **Vita HABJAN BARBORIČ** Head of the Development and Prevention Centre Commission for the Prevention of Corruption, Slovenia • **Ádám FÖLDES** Legal and Advocacy Advisor, Transparency International.		• **Gonzalo SOSA** Représentant de l'Agence pour l'administration électronique et la société de l'information et des connaissances, Uruguay • **Vita HABJAN BARBORIĆ** Cheffe du Centre de développement et de prévention de la Commission pour la prévention de la corruption, Slovénie • **Ádám FÖLDES** Conseiller juridique et chargé de plaidoyer *Transparency International*.
CLOSING REMARKS	13 :00	**ALLOCUTION DE CLÔTURE**
• **Helena JÄDERBLOM** President of the Council of Europe Access Info Group • **Beatriz DE ANCHORENA** Chair of the Committee of Convention 108		• **Helena JÄDERBLOM** Présidente du Groupe « Accès à l'information » du Conseil de l'Europe • **Beatriz DE ANCHORENA** Présidente du Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108)

OPENING SESSION / *SESSION D'OUVERTURE*

Helena JÄDERBLOM

Chairperson of the Council of Europe Access Info Group / *Présidente du Groupe Accès à l'Information du Conseil de l'Europe* (AIG)

Dear colleagues,
Distinguished guests and participants,

I would like to thank, on behalf of the Council of Europe Access Info Group, the Committee of Convention 108 and the GRECO members for having accepted our initiative to jointly hold this workshop.

We hope this first dialogue will lay the basis for future collaboration and will lead to new opportunities for better implementing Council of Europe standards.

The Tromsø Convention is the only international instrument to guarantee a general stand-alone right to access information held by the State.

It is different from other international instruments, including the European Convention on Human Rights, under which the right of access is protected when certain conditions are met.

The right of access guaranteed by the Tromsø Convention is not limited by the content of the information, by the profession or status of the persons requesting access, or by the purposes for which access is sought.

The Tromsø Convention is about maximum but not absolute disclosure of information.

Balance is the main feature of its provisions.

Limitations of access are permissible when they are prescribed by law, necessary and proportionate to legitimate interests which are listed in an exhaustive manner in the Convention. Privacy is one of those interests listed by the Convention.

Limitations cannot be imposed if the disclosure of the requested information does not harm the listed interests. Even if that is the case, access should be granted if there is a higher public interest in the

disclosure of the information compared to the interest in keeping it confidential.

The Tromsø Convention allows for this assessment to be carried out either on a case-by-case basis, or by the legislator when formulating the relevant legal provisions.

During this workshop, we intend to present these standards to you in more details.

We will also look at how we have interpreted them in relation to privacy in our baseline evaluation of the Parties to the Convention.

We hope to get to know better your perspectives on privacy safeguards when it comes to transparency legal regimes.

We hope to learn from your experiences in balancing privacy and transparency. We are lucky to have many experts in the room who work for institutions responsible for both data protection and freedom of information issues.

To start our dialogue, we have chosen two main questions; (1) how do public authorities manage their officials' personal data? and (2) how do they manage personal data of third parties with which they are dealing?

Of course, when it comes to the balance between transparency and privacy the picture is much bigger. But the topics we have chosen are concrete and a very good start.

As one of the persons who was involved in drafting the Convention, I can recall the political momentum, and the enthusiasm of many countries involved in the process.

Unfortunately, today, we do not see this enthusiasm anymore.

This workshop will, hopefully, contribute to our efforts of promoting a favourable environment for the ratification of the Tromsø Convention by more Council of Europe member States and non-member States.

Ratification of an international treaty is not only about harmonising national law and practice in accordance with agreed common standards, although that is of course fundamentally important.

It is also about commitment to international cooperation and supporting multilateralism.

It is also about contributing to the general development of international law on access to State-held information.

I hope this dialogue will help us in our efforts.

I believe that, in any case, it will help us ensure that the results of our monitoring process are realistic and practical, and that our recommendations respond to the actual needs of the Parties.

I shall look forward to our discussions.

Thank you.

Beatriz de ANCHORENA

Chairperson of the Committee of the Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) / *Présidente du Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+)*

Good morning,

On behalf of the Consultative Committee of Convention 108, it is a great honour to open this joint event.

Thank you Gianluca Espósito and Council of Europe for convening this important discussion on how transparency and privacy converge as complementary values for democratic societies, as shared in the title of this event.

Transparency, access to public information, and data protection all aim at the same goal: strengthening democracy, institutional capacities, and citizens' trust. Together, they sustain accountability, participation, and responsible data governance: key elements that bring legitimacy to democracy.

Today's debate gains new meaning in our changing digital landscape: this is our common scenario, where the boundaries between public and private, between personal data and public information, have become increasingly blurred.

Technological developments expose more radically old tensions between these concepts. But this can be an interesting opportunity to rethink how to safeguard both the right of access to public information and the right to personal data protection in a dynamic interplay.

In our evolving digital landscape, international conventions provide common frameworks that help balance these rights across borders. Convention 108+ and the Tromsø Convention, represent universalist steps forward, offering common reference points to align principles across regions.

Each convention incorporates the other's exceptions: Tromsø recognises privacy in its Article 3(f) as a limitation to access to public documents, while Convention 108+, in its Article 11, allows the disclosure of personal data when justified by public interest or by freedom of expression.

However, their real value depends on how they engage with the diverse geographic, historical, cultural, and regulatory realities of each country. These conventions give us a shared language, yet every society must translate it through its own institutions and democratic experiences.

In this context, we can also recognise different legal traditions shaping how these rights are interpreted and implemented across regions. The European and Latin American experiences, while rooted in different institutional developments, show both diversity and growing convergence, enriching the global conversation on how transparency and privacy can be balanced in democratic societies.

Within the Committee of Convention 108, we are working towards the entry into force of the modernised Convention (only five ratifications remain out of 38). Today, Convention 108 brings together 55 countries and 41 observer institutions, reflecting its global reach and its role as a multilateral platform for data protection cooperation.

When that moment comes, both instruments, Tromsø and 108+, will stand side by side as legally binding, truly global conventions, offering robust standards and fostering international cooperation.

Together, they can serve as common grounds for dialogue across legal traditions and regions, bridging different paradigms of data protection and access to public information, promoting a meaningful conversation.

From a Global South perspective, this dialogue is particularly relevant.

Building inclusive information societies means ensuring that all people, regardless of origin, socio-economic condition, or geography, can fully benefit from access to, use of, and protection of information in the digital environment.

Multilateralism remains our strongest tool to navigate complexity, bridge regulatory asymmetries, and ensure the protection of rights.

States must actively develop the institutional, legal, and technical capacities required to guarantee these rights in practice through effective public policies.

Together, through dialogue, cooperation, and commitment to human rights, we can ensure that access to information and privacy remain pillars of inclusive democracies.

David MEYER

Chairperson of the Group of States against corruption (GRECO) / *Président du Groupe d'États contre la corruption* (GRECO)

Madame President of the Council of Europe Access Info Group,
Ms Jäderblom
Madame Chair of the Committee of convention 108,
Ms de Anchorena
Ladies and Gentlemen,
A very good morning to everyone, and Greetings from London.

To introduce myself I am President of GRECO – the Council of Europe's Anti-Corruption Montitoring Body. I have held that role since beginning of the year.

First, let me say what a pleasure it is to be asked to be asked to be one of the speakers opening this event on transparency and privacy in democratic societies. I am very sorry that I am having to appear on screen rather than being with you in person, but unfortunately it just wasn't possible to combine being in Strasbourg today with my Ministry of Justice travel commitments this week. In the interests of transparency I am catching a flight to India this afternoon. But it really is a matter of regret, and seeing so many friends and colleagues on screen and on the participants' list makes me realise how much I would have preferred to have been with you in person.

But the good news is that, while I am joining remotely, GRECO is very much represented in the room with you. A couple of our most experienced experts will be speaking later this morning, and our superb secretariat are also present. I am confident that their interventions will support a constructive exchange.

There will doubles be a lot to discuss, with this being a joint initiative of three Council of Europe bodies. And it's an initiative I personally very much welcome. Each body brings its own mandate and experience, and together we are well placed to address the questions that arise when transparency and personal data protection meet. They are practical, not theoretical, and balancing these two fundamental principles effectively is essential to democratic governance.

I will focus briefly on three key messages that GRECO will bring to the discussion.

First, transparency is essential to GRECO's monitoring work and indeed to strengthening the rule of law and democracy. Across all five evaluation rounds, GRECO has issued numerous recommendations aimed at improving and strengthening transparency in public administration, political party funding, the parliamentary legislative process and the central government decision-making. This focus will continue in GRECO's new Sixth Round, which examines prevention of corruption and promotion of integrity at the sub-national level.

Transparency is not only a safeguard against corruption. It is also a pillar for public trust in public institutions and those who serve them. Where transparency exists, it is harder for corruption to occur and – when it does occur – it is easier to identify. Where transparency does not exist, corruption is free to flourish.

Second, disclosure of and access to information is critical to achieving transparency. GRECO has consistently emphasised that the publication of, and access to, information increases transparency, strengthens the accountability of public authorities and officials, enables citizens to participate in public life and scrutinise those in power, and contributes to preventing and combating corruption through informed oversight. In our recommendations we have encouraged member states to improve both the legal frameworks governing access to information and their practical implementation. Where appropriate, GRECO has encouraged members states to join the Council of Europe Convention on Access to Official Information (the Tromsø Convention). The importance of access to information was recently acknowledged in a thematic paper on access to information published by GRECO.

Disclosure and access to information are particularly relevant in the area of lobbying. Interactions of public officials and lobbyists can play a positive role in shaping policy and informing decision-makers. But disclosure of such interactions helps maintain public confidence and ensure that decision-making remains open to scrutiny. I am very pleased that my dear colleague Vita Habjan Barborič will be presenting GRECO's practice in this evolving area.

The third message relates to the balance that needs to be struck between transparency and privacy. Anyone who has conducted country visits on behalf of GRECO will have heard concerns raised by journalists and civil society organisations about restrictions on access to information. These concerns frequently relate to the protection of personal data of individuals concerned, including that of public officials.

This has also come up in discussions on asset and interest declarations filed by public officials.

The right to personal data protection, as guaranteed by the Council of Europe Convention 108+ for the protection of individuals with regard to the processing of personal data, must be respected. At the same time, there is an ever-growing consensus that public officials, in particular elected or politically appointed officials and those in leadership and management roles, do not enjoy the same level of privacy as ordinary citizens and are subject to a higher level of public scrutiny.

There are several arguments favouring the publication and disclosure of asset and interest declarations: it allows citizens to be informed, it enables civil society to contribute to scrutiny and verification, and it reinforces the message of accountability on the part of the public official. The objective is not to choose one right over the other, but to strike a fair and proportionate balance between the public interest in transparency and the need to protect personal data. Even public figures have a right to privacy. But matters relating to public funds, or factors that may influence decisions that affect the public, are inherently not private.

Achieving this balance is not straightforward, and one of GRECO's experts, Mr Vladimir Georgiev, will describe GRECO's approach and experience on this topic.

I realise that each of our bodies has its own specific mandate, but none of us works in isolation. The issues we will be discussing today concern all of us. It is therefore valuable to come together in such joint events to share perspectives, learn from each other, understand our respective approaches and support coherent standards and practice.

On which note I will close my remarks and wish you a constructive and engaging discussion, and I look forward to learning from your exchange and to continuing our shared work to strengthen transparency, ensure access to information and protect personal data.

Thank you.

PANEL / SESSION 1

Balancing transparency and privacy – Council of Europe standards

Équilibre entre transparence et vie privée – Les normes du Conseil de l'Europe

Moderator */ Modérateur :* **Joan BARATA MIR**, Legal expert, Fellow at the Cyber Policy Center of Stanford University / *Expert juridique, membre du Cyber Policy Center de l'université de Stanford*

Païvi KORPISAARI

Professor of Communication Law, Helsinki University, AIG member / *Professeure de droit de la communication à l'université d'Helsinki, membre de l'AIG*

MEETING POINTS OF TROMSØ CONVENTION AND CONVENTION 108

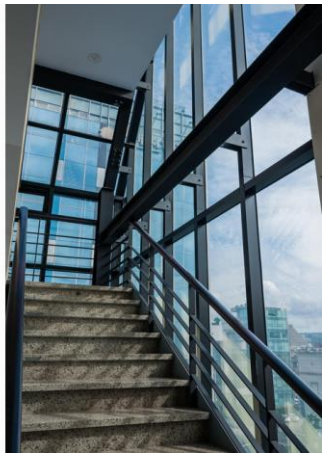
- The Council of Europe Convention on Access to Official Documents (CETS No. 205), 2020 (Tromsø convention)
- Recognises a general right of access to official documents held by public authorities
- Sets forth the minimum standards

- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 1981.
- Respect for rights and fundamental freedoms, in particular the right to privacy, with regard to automatic processing of personal data
- (The transfrontier flow of personal data)

- The two instruments are complementary, not conflicting
- Their joint aim is to promote responsible transparency

WHY IS RIGHT OF ACCESS TO OFFICIAL DOCUMENTS IMPORTANT?

- Link to political freedoms, particularly freedom of speech that contains the right to disseminate and receive information and opinions
- Participating and influencing societal activities
- A prerequisite for criticising the exercise of power and the actions of the authorities
- Legal certainty and legal protection
- Open and good governance; prevention of abuse
- Strengthening the legitimacy of public authority activities
- Utilisation of public information resources



CONVENTION RIGHTS AND THE CONSEPT OF OFFICIAL DOCUMENT

- The convention gives the right for everyone to have access, on request, to official documents held by public authorities

- "Official documents" means
  - all information
  - recorded in any form
  - drawn up or received and
  - held by public authorities

Photo: WolfBlur, Pixabay

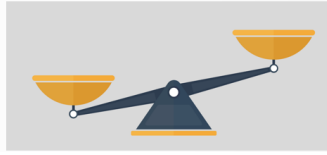
Photo: EsaRiutta, Pixabay

PERSONAL DATA & TROMSØ CONVENTION

- Explanatory report:
- Documents containing personal data are covered by the scope of Tromsø Convention
- Convention 108 does not in principle prohibit access of third parties to official documents containing personal data
  - When access is granted, the use of personal data is governed by Convention 108

LIMITATIONS TO ACCESS TO OFFICIAL DOCUMENTS

- By law
- Necessary in a democratic society
- Proportionate to the aim of protecting some of the 11 listed interests such as for exaple
  - National security
  - Public safety
  - Investigation of criminal activities
  - Privacy and other legitimate private interests (explanatory report refers to ECHR Art. 8)
- Harm test: access may be refused if disclosure would be likely to harm paragraph 1 interestes, unless there is an overriding public interest in disclosure (balancing principle)



REQUESTS OF ACCESS

- No need to give reasons for having access
- Parties may give a right to remain anonymous
- Not too much formalities

PROCESSING OF REQUESTS

- Help to identify the document
- Referral to competent authority
- Equality
- Decision as soon as possible or within a reasonable time limit which has been specified beforehand

DISCUSSION: INTERPLAY BETWEEN ACCESS TO OFFICIAL DOCUMENTS AND PERSONAL DATA PROTECTION

- Broad definition of personal data & stricter rules for special categories of data
- Most public documents include personal data
- Necessity to balance transparency and privacy
- Does data protection restrict access to information too much?
- Opportunity: technology enabling smarter disclosure
- Challenge: reliable anonymisation

Thank you !

Kristi VÄRK
Director of Data Protection Law Division, Ministry of Justice and Digital Affairs of Estonia / *Directrice de la division du droit de la protection des données au ministère de la Justice et des Affaires numériques de l'Estonie*

Balancing Access to Information and Personal Data Protection: The Estonian Approach

Our Starting Point: Open by Design and by Default for almost 25 years, Estonia has applied the principles of openness through the *Public Information Act*. Our approach to "data protection" is comprehensive: it covers both governance of public information and protection of personal data. The supervisory authority—the Data Protection Inspectorate—combines tasks that in many countries are split between Information Commissioners and Data Protection Authorities. This unified oversight has been debated, but our experience shows it delivers more balanced outcomes for society.

Why Balance Matters

Official documents often contain personal data—names, signatures, and more. Public registers amplify this challenge, especially in a country that is in the forefront of digital governance and where data is hardly processed on paper. In Estonia, access to personal data can only be restricted if disclosure would significantly breach the inviolability of private life.

At the same time, the Public Information Act together with special laws mandates proactive publication of certain personal data, such as:

- Composition of state and local government agencies, including officials' names, education, and contact details
- Salaries of officials
- Lists of political party
- members

This openness strengthens transparency but raises risks when large datasets are made publicly available. A single data point may seem harmless, but aggregated and proactively published data can seriously impact privacy.

Tools and Methods for Balancing Rights

Recent years—and Europe's security context—have intensified the debate. Apart from providing legal ground for publication personal data in legislation adopted by parliament, Estonia uses several legislative tools to strike the balance:

- Legitimate Interest Requirement
  Access to personal data in sensitive registers, such as the population registry, now requires demonstrating a legitimate interest. This adds administrative effort but ensures proportionality.
- Redesigning Access Mechanisms
  A recent example: the Land Register. Previously, anyone could query property ownership using a person's name and personal code—both widely available. Abuse of this system led to legislative change: queries must now be based on property address, not personal identifiers.
- Data Tracker as a Transparency Tool
  Estonia introduced a "data tracker" that notifies individuals when their data is accessed and by whom. Initially voluntary, we are moving toward making it mandatory for all public registers. This is a human-centered solution that builds trust.

Lessons Learned

The principles of *open by design/default* and *data protection by design/default* are not mutually exclusive. They can coexist—if systems are continuously redesigned with both principles in mind.

There's a story that everybody knows in Tallinn: every year, a little gray man asks if the city is ready. It never is—because improvement must be ongoing. The same applies here: balancing access and privacy is a *continuous process*, adapting to technology, societal expectations, and security realities.

The same authority overseeing both rights ensures coherence and balance. Our experience shows that transparency and privacy are not opposing forces—they are complementary pillars of democratic governance when managed thoughtfully.

PANEL / SESSION 2

Manging information about public officials

Gestion des informations relatives aux fonctionnaires

Moderator */ Modératrice :* **Tetyana OLEKSIYUK**, Vice Chariperson of the Council of Europe Access Info Group */ Vice-présidente du Groupe « Accès à l'information » du Conseil de l'Europe*

Warren SEDDON

Director of Freedom of Information and Transparency, Information Commissioner Office, UK / *Directeur de la liberté d'information et de la transparence, Bureau du Commissaire à l'information, Royaume-Uni*

Good morning everyone and thanks for having me – it is an honour to be able to speak to you all today. I am Director of FOI and Transparency at the UK ICO and I also started my career on the implementation of FOI in central government.

It has been a big year in the UK for Access to Information, or Freedom of Information (FOI) as we refer to it. This month marks quarter of a century since FOI as a law was passed by the UK parliament and just over two decades since it was implemented across England, Wales and Northern Ireland. The Scottish legislation, which has its own Commissioner, was implemented at the same time.

Last year was a similarly significant year for the Information Commissioner in the UK as a whole, marking 40 years since the first Data Protection law and the establishment of the office.

So, it's fair to say both Data Protection and FOI law are pretty well established in the UK's constitutional framework, but today's panel poses an interesting question about how well they complement each other in certain circumstances.

FOI and Culture

When taking the FOI Bill through parliament at the end of the last Century, Jack Straw, then the Home Secretary argued that, "Unnecessary secrecy in Government and our public services has long been held to undermine good governance and public administration".

He went on to set out that the Bill would "not only provide legal rights for the public and place legal duties on Ministers and public authorities, but will help to transform the culture of Government from one of secrecy to one of openness. It will transform the default setting from "this should be kept quiet unless" to "this should be published unless."

Access to Information in the UK has had many successes since its introduction at all levels of public life. Citizen led scrutiny has helped uncover information about everything from local water quality and restaurant hygiene through to national flu pandemic preparedness and how decisions about benefits to the some of the most vulnerable in society are made.

But, 20 years on, there remains issues about culture and the tone set from the highest levels of public life when it comes to transparency. This can often be the case when it comes to scrutiny around how some of those at the most senior levels of public life are affected by our access to infomation laws.

FOI and public officials

Information about public officials has increased significantly since our Access to Information laws came into effect.

Following a number of requests early in the life of the legislation, since 2010 the UK Government has proactively published a regular organisation chart of senior officials across its departments and key agencies to increase transparency, which includes salary information for some, although not all, officials at this level.

Information about political advisers pay is similarly made available on a regular basis in central government. While information of this nature is made available in the annual reports of public bodies, depending on their size and salary structures at both national and local levels.

There are steps being taken to extend this wider. From 1 October 2026, private registered providers of social housing must publish information publicly about their housing management which will include senior staff names and roles, organisational structure and governance arrangements.

This information is often then compiled and utilised by campaign groups to inform public debate about salary levels across the public sector in the UK, for example.

Its proactive publication helps ensure that public bodies aren't overburdened with requests for information that should clearly be published in the public interest.

In recent years we have also been forced to make clear that where there is an interaction between the personal and professional spaces of those in public life, that there may need to be scrutiny of this.

In 2022 we launched our first ever joint FOI and Data Protection investigation utilising our powers under both laws. This was into the use of private communication channels during the covid pandemic by Ministers and Public Officials in our Department of Health in the UK following high profile concerns raised in the national press.

In the report we laid before the UK parliament the following year, we found their use was significant, but that in general efforts were being made to make sure information was properly preserved for the public record. We also found it highly likely based on what we saw, however, that mistakes would likely have been made in this space.

As a result, we successfully made the case that our national inquiry into the covid pandemic should include exploration of the quality of record keeping during that period to ensure lessons were learned.

And we made clear in our findings that where personal devices are used by public officials and ministers for official business, that our information laws are strong enough to ensure that these devices and channels are covered and that when people make information requests they should be searched.

Interaction of FOI and DP

While this suggests correctly that access to information has stimulated a positive change in culture in the UK, there remains work to do and our legislation continues to be needed to ensure transparency in a number of ways.

At Ministerial level for example, we have a voluntary system with no legal basis that underpins the publication of Ministerial Interests. An official, appointed by and accountable to the Prime Minister of the day, reviews the declaration's that Minister's provide and decides what should be published.

When a national news organisation sought access simply to the blank form provided to Ministers to facilitate this process, the government withheld it. When this decision was appealed to us and we ordered disclosure of the information, the government tried appealing it further to the Tribunal, before finally releasing it when they lost again at that stage.

So there remains some resistance to even basic transparency in some of these spaces before we even get to the issue of the personal data itself.

The interaction between freedom of information and data protection in the UK system is focused on the application of data protection law. In very general terms, if the disclosure of information would contravene any of the data protection principles, then that information cannot be disclosed.

This means that when a public authority responds to an FOI request asking for personal information, it must assess under data protection legislation if disclosing it to a general member of the public would be legitimate.

Unlike the Tromso process, there is no separate public interest test – it is an absolute exemption. However, data protection law can allow disclosure of the information when the public authority has a lawful basis for processing the requested personal information.

In the context of freedom of information, this will generally consider the application of Article 6(1)(f) of the UKGDPR – where disclosure is *"necessary for the purposes of legitimate interests pursued by the controller or by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject".*

This means that there are areas where we have forced the disclosure of information. For example, in local government, we ordered disclosure of information about court summons for councillors who were in council tax arrears. We decided that the legitimate interest in disclosure outweighed that in withholding the information.

Similarly at the national level, there are examples where, in relation to potential breaches of the Ministerial Code of Conduct, the government has tried to rely on the data protection as part of their arguments for withholding information where we have overruled them and information has gone into the public domain.

We have then seen requests where data protection has been used as the defence for withholding information, or even in some cases not even confirming if it is held, based on the law as it stands.

From information about undisclosed ministerial interests to information about criminal convictions, we have upheld the position of public authorities in relation to the protections offered by data protection law as we are required to do by the law as it stands.

It is an interesting question, however, about whether there could or should be stronger gateways through data protection to allow for greater transparency in these spaces, similar to the Tromsø Convention's Article 3(2) overriding public interest in disclosure provisions.

It is not necessarily the role of regulators to answer questions like that, that is the role of lawmakers. But the places where we are forced to draw the lines of transparency based on the law as it stands can hopefully help inform the public debate around them

Protecting the role of Information Commissioners

What I do think these types of cases show is the importance in our access to information systems of robust, independent and impartial regulators that can uphold the rights of citizens and, where needed, speak truth to power. This includes being prepared to order the disclosure of information about even the most important figures in government where appropriate.

Unfortunately, internationally, we are seeing numerous threats in this space as we discussed at the recent International Conference of Information Commissioner's (the ICIC).

We heard about moves such as the dissolution of independent institutions in charge of FOI in Mexico and Tunisia, to the failure to fill the position of information commissioner in India, to threats to the FOI legislation in Germany.

These are concerning events and it is why I was proud to be able to co-lead work, along with colleagues in Brazil, which concluded at this year's conference where we agreed to the 'Berlin Principles for the Protection and Promotion of Information Commissioners'.

These principles set out the importance of our Access to Information institutions. This includes how they should be established and maintained, from their statutory independence to ensuring they are properly funded to be able to deliver their functions.

Agreed unanimously at the ICIC, we are now exploring with UNESCO how they could be adopted at the UN level in a similar way to the human rights and ombudsman equivalents that already exist. Any support from the Council of Europe in this space would also be welcome.

Indeed, if they are, there may be opportunities that could be explored at the different international levels to then examine how states are performing collectively in all of the areas that uphold citizens fundamental rights and support their ability to challenge the institutions of the state.

We look forward to supporting the continued progress of this work over the coming months alongside the Executive Committee of the ICIC, which has agreed it should head in this direction.

I will stop there for now but look forward to any questions at the end of this session or in the breaks.

Vladimir GEORGIEV

Expert, former Commissioner State Commission for Prevention of Corruption, North Macedonia / *Expert, ancien Commissaire de la Commission nationale pour la prévention de la corruption, Macédoine du Nord*

Declaration of assets, income, liabilities and interests

- Importance
  - greater transparency of declarations, while respecting personal data protection, reflects the integrity and accountability of the public service
- Who should declare
  - Public officials proportionate to their level of risk exposure
- Content and thresholds of disclosure
  - detailed inventory is provided in the GRECO IV, V and VI Evaluation rounds questionnaires
- To whom
- Supervision / control
- Balance between transparency and privacy

2

Rationale of disclosure

- Identify and prevent COI
- Public oversight
- Detect illicit enrichment / hidden assets
- Trust in government

……..

- No single best model applies, context matters

3

GRECO's evaluation practice - key findings / recommendations

- Categories of officials and interests to be disclosed must be clearly defined and meaningful
  - Lawfully required
  - Scope and details of declarations to be sufficient and to allow verification (quantitative rather than vague)
- Spouses and dependent family members – "consideration" recommendation:
  - Address issues concerning spouses and dependent family members
  - Involve a broad range of stakeholders in consultations
- Frequency of reporting
- Electronic filling of declarations
- Ensuring public accessibility of declarations - online
- Review mechanisms
  - effective, dissuasive and proportionate sanctions in case of non-compliance

4

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
46 MEMBER STATES
700 MILLION CITIZENS

Publication of declarations and balance with privacy

- Information to be declared, published and accessed
  - financial interests, assets, income, liabilities
  - interests, paid and not-remunerated activities, gifts, hospitality, benefits
  - information to be searchable, preferably online or in e-platforms
- Information may be declared but not necessarily published
  - data on spouses/dependent family members
  - addresses
  - bank accounts and other sensitive information
  - personal identifiers not relevant for scrutiny (PIN, YoB etc)
- Safeguards to ensure balance
  - law must define what should be published or excluded
  - publication on official websites or e-platforms

5

Case examples

Practice of various countries:

- Public disclosure, + information on spouses and dependent family members
- Mixture of public and confidential disclosures
- Available to the public only upon request

6

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
46 MEMBER STATES
700 MILLION CITIZENS

Conclusions

- Transparency and disclosure of public officials' assets and interests **are not competing objectives**
- Effective disclosure system should be **clear, proportionate and verifiable**
- It **enhances public trust** by allowing citizens to be informed and civil society to contribute to scrutiny, while **safeguarding legitimate privacy interests**

7

Thank you !
GRECO website : www.coe.int/greco/
GRECO mailbox address: webmaster.greco@coe.int

Carlos CORDERO SANZ
Founder of Access Info Europe / *Fondateur d'Access Info Europe*

Access Info Europe
10 principles on the right to information and privacy.

Definitions:

Public officials: include any individual with responsible for performing public tasks and/or with decision-making powers (and their advisors).
Executive or legislative branches of power at national, sub-national, or supra-national levels; within private bodies performing public functions and/or operating with public funds

- Basic Personal Data: the full name, professional affiliation, job title, appointments and sanctions processes (including administrative and penal sanctions), employment history, working or personal address, email address, telephone number, ID number, birth date and other identifying data
- Sensitive Personal Data: Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

1. Fundamental Rights to Information and to Privacy. The legal framework shall:

- Recognise both as Fundamental
- Clearly define the relationship between both
- Ensure that there are clear mechanisms permitting decisions to be taken, on a case-by-case basis
- Define the information containing private data should be released into the public domain.

2. Public functions of Public Officials

- Information that relates to the activity of public official, and to persons performing public functions and/or spending public funds should generally be made available.
- At a minimum, the names, job titles, and other relevant basic data about the functions and activities “senior public officials” should be made public
- “Senior” public officials should include those at any level of government who have responsibility for decision making and/or the spending of public funds.

3. Basic data about public officials

- including names, job titles and details of responsibilities and involvement in decision-making processes
- curriculum vitae, assets declarations, and declarations of conflict of interest of all public officials shall be made available
- The participation of all public officials in meetings, inside or outside government, and their participation in decision-making processes shall be considered to be, prima facie, public information.
- The application of exceptions to the publicity of basic personal data about public officials shall be limited, under one of the legitimate exceptions (international standards) and/or reveal sensitive personal data

4. Spending of public funds by public officials

- The basic data on public officials responsible for or directly implicated in the spending of funds shall always made available.
- details of the names and job titles of those responsible for decisions related to the spending of public funds
- Information about spending of public funds directly related to the public officials on salaries and other benefits, on travel

5. Private recipients of public funds

- Individuals working for private legal entities and natural persons who are recipients of public funds in the forms of public procurement contracts, subsidies and grants, basic personal data will be made available along with data on the funds received and the activities
- All private persons who fall under a legal requirement to make public personal data, shall be clearly informed about these obligations in advance

6. Private persons engaging in decision-making processes

- Private persons engaging in decision-making processes, including by participating in meetings with public bodies and by contributing to public consultations, shall do so with an expectation that basic personal data may be made available.
- Information about individuals engaged in lobbying and/or associated with private interest groups (lobbyists and similar organized groups) in accordance with the International Standards on Lobbying Regulation.
- https://lobbyingtransparency.net/standards/transparency/

7. Obligation to Anticipate Disclosure

- Public bodies shall take necessary steps to record, organise, store, and administer data in a way that anticipates and facilitates disclosure
- Storing data in electronic formats so that personal data that is not subject to disclosure may be easily redacted and withheld from disclosure

8. Non-public data about private persons

- shall take every necessary measure to ensure that the private data of private persons, that is not otherwise subject to transparency obligations, and in particular any sensitive personal data, is protected from disclosure
- protections so that when multiple data sets are released under open data policies, it is not possible to identify the personal data of private persons

9. Reuse of Data Sets containing Private Data

- All recipients of personal data shall be given clear instructions on the legal framework for the reuse of the personal data received.
- The legal framework shall establish limits on the reuse of information in ways that might result in the identification of sensitive personal information about private individuals.
- In no case may limits be placed on the reuse of information for the exercise of the right to freedom of expression, be it by journalists, civil society, or members of the public, even where such use is made to criticise or to hold to account the activities of public bodies
- Similarly, the use of personal data obtained in accordance with these principles and as authorised by the national legal framework shall not be limited where that use is made in order to participate in public decision-making processes.

10. Independent Oversight

- Establish oversight mechanisms for ensuring an adequate balance between the right of access to information and protection of privacy personal data
- This responsibility will fall with the Information Commissioner or Commission and the National Data Protection Agency
- Shall establish clear mechanisms for co-decision making and oversight of the release of personal data in public interest.

- Oversight body shall be independent of government, shall have a budget set by and shall report to parliament, shall have powers of investigation and sanction, and shall have sufficient resources adequately to carry out its oversight role.
- The legal framework shall provide clear, rapid, and low-cost mechanisms for appeal, both to the oversight body and to the courts, for any individuals, inside or outside of public bodies, who wish to raise concerns about the protection of their personal data and for those who wish to challenge refusals personal data where there is a public interest

Lessons learnt from our practice regarding the implementation of these principles. *The case study of Spain*.

Case 1: Request of information to General Secretary of the Presidency of the Government. *Regarding the personal advisor to the wife of the President of the Government*

1.- Amount of remuneration paid from appointment to breaking down the concepts and annual payments.
2.- Copy of the documentation stating the functions to be performed, justification of the hiring and copy of the appointment resolution as advisor

There is no response from the Administration

Counsel of transparency & good governance decision & resolution:
Urge the General Secretary of the Presidency of the Government to send the claimant the information:
1.- Amount of remuneration paid from appointment to the present, breaking down the concepts and
annual payments.
2.- Copy of the documentation stating the functions to be performed, justification of the hiring and
copy of the appointment resolution as advisor."

Case 2: Request of information to Ministry of Finance and Public Administration- Advisors in the Ministries

- “(...) list of persons who hold or have held a temporary advisory position, who are not civil servants, and who perform this advisory or assistance function, since the beginning of the current legislative term, distinguishing between the Cabinets of

Ministers and Secretaries of State and identifying the service entrusted to them and the annual remuneration for this concept. In addition to these positions, I request that other advisory figures appear in the List of Government Positions, such as technical advisers and career civil servants appointed by free designation to a position in which they earn more than in their regular position."

- The Ministry of Finance does not identify its advisers even though there is case law from the Transparency Council in favor of making this information public in resolution R-0170-2016.

- In Interpretative Criterion 1/2015, of 24 June, prepared jointly by the Spanish Data Protection Agency and the Council for Transparency and Good Governance by virtue of the mandate contained in the Fifth Additional Provision of the LTAIBG, a clear interpretative guideline was already established in this regard by indicating that, in the case of temporary staff who occupy positions of special trust and advice and at a high level in the hierarchy - positions with levels 30, 29 and 28-, the public interest in access to information prevails over the individual interest in the protection of personal data.

- Contentious-Administrative Chamber of the National High Court by Judgment of 16 March 2021. Article 15.2 of the Transparency Law, corroborating the above statements, "in general, and unless in the specific case the protection of personal data or other constitutionally protected rights prevails over the public interest in disclosure that prevents. Confidentiality may be maintained regarding personal data when the physical integrity of public employees may be compromised, for example, in the cases of female employees who have protection for reasons of gender violence

Case 3: Request of information to the MINISTRY OF FOREIGN AFFAIRS, EUROPEAN UNION AND COOPERATION - Advisors in the Ministries

- "To know the list of people who occupy or have held a position of adviser on a temporary basis, non-civil servants, and who perform this function of advice or assistance, since the beginning of the current legislature, distinguishing the Cabinets of Ministers and Secretaries of State and identifying the service entrusted, the annual remuneration for this concept. In addition to these positions, I request that other figures of advisors that appear in the List of Jobs of the Administration be included, such as technical advisors and career civil servants appointed

by free appointment for a position in which they are paid more than in their position".

- "MINISTRY OF FOREIGN AFFAIRS, EUROPEAN UNION AND COOPERATION RESOLVES: To partially grant access to the information requested. Article 15.2 of Law 19/2013 of 9 December, on transparency, access to public information and good governance establishes that, although in general access will be granted to information that contains merely identifying data related to the organisation, operation or public activity of the body, this access may be limited when "in the specific case the protection of personal data or other constitutionally protected rights prevails over the interest of the body" public in dissemination". For the reasons outlined above, it is considered that, in this case, the rights to privacy and protection of personal data of advisory positions of the Ministry of Foreign Affairs, European Union and Cooperation should prevail and, consequently, the right of access to information should be partially addressed.

- Requestor "Access to part of the requested information was denied. The Ministry does not identify the advisors despite the fact that there is jurisprudence in the Transparency Council that ratifies that these data have to be given, as is the case with resolution R/0170/2016."

- Council of Transparency and Good Governance: TO URGE the MINISTRY OF FOREIGN AFFAIRS, EUROPEAN UNION AND COOPERATION to send the claimant the following information within a maximum period of 10 working days: "List of persons who hold or have held a post of adviser on a temporary basis, non-civil servants, and who have been performing this advisory or assistance function, since the beginning of the present legislature, distinguishing the Cabinets of Ministers and Secretaries of State and identifying the service entrusted, the annual remuneration for this concept…

Lessons learnt from your practice regarding the implementation of these principles. *The case study of UE*.

Case 4: Request of information to the "Rio Tinto meeting with Cabinet of Vice- President Maroš Šefčovič of European Commission" name of lobbies

- In the confirmatory application request the 'names of lobbyists that are redacted from the documents'.
- Directorate SG.D of the Secretariat-General granted wide partial access to these documents based on the exception of Article 4(1)(b) (protection of privacy and integrity of the individual)
- Access to information law – a comprehensive access to information law shall guarantee the public's right of access to information, including information about lobbying.
- Secretariat-General notes that: the representatives of Rio Tinto named in the documents were acting as employees of said organisation, representing it. They were not acting in a private capacity, nor on behalf of a public administration or government

Lessons learnt from your practice regarding the implementation of these principles. *The case study of Spain*.

Case 5 – Research on Conflict-of-Interest Office

- Hypothesis: Assets declarations, and declarations of conflict of interest of all public officials shall be made available
- Office of Conflicts of Interest is attached to the Ministry of Finance and Public Administration with the rank of Directorate-General.
- Its responsibilities are preparing the reports required by law, administering the Registers of Activities and Assets and Property Rights, manage the regime of incompatibilities of senior officials and monitor compliance with their obligations (Assets declarations and declarations of conflict of interest) (Art. 19.4).
- Senior public officials periodically should send their asset information to the Office of Conflicts of Interest
- The Office of Conflicts of Interest do not have enough resources to verify that all Senior Public Officials comply with the accuracy of the contents, and depends directly of the Secretariat of State for the Civil Service.
- Not many disciplinary proceedings are reported by the conflicts of interest office.

Some findings and patterners:

1. Access to Information is not recognized as Fundamental Right, but Privacy yes
2. Unbalance between Data Protection and Access to Info in the public interest assessment
3. Definition on Public official: include any individual with responsible for performing public tasks and/or with decision-making powers (and their advisors). But… information regarding advisors and other eventual public officers, non-civil servants, is not consider as public information in practice
4. Information regarding advisors, lobbies, and other eventual public officers are frequently consider as personal data to be protected
5. Weakness of the oversight bodies on access to information: no resources, no actual independency, no capacity on sanctions or penalties
6. Access to Information depends of the arbitrary decision or political will of the public institution holder of it
7. Litigation is the way to access to information in some sensitive cases

Thank you!

PANEL / SESSION 3

Managing information about private persons dealing with public authorities

Gestion des informations relatives aux personnes privées traitant avec les autorités publiques

Moderator / *Modératrice :* **Neuss VIDAL MARTÍ**, SEEK Initiative Executive Director / Directrice exécutive de *SEEK Initiative*

Elona HOXHAJ
General Director on the Right to Information, Albanian Information and Data Protection Commissioner / *Directrice générale chargée du droit à l'information, Commissaire à l'information et à la protection des données en Albanie*

Balancing Transparency and Privacy in Albania: Practical Lessons from the Information and Data Protection Commissioner of Albania

What are the typical legal disclosure obligations that public authorities have concerning personal data of individuals representing or working for private companies which receive public funds through public procurement, grants or subsidies – the case of Albania. Presentation of practical cases encountered by the Albanian Information and Data Protection Commissioner.

Good afternoon, colleagues,

It is a great pleasure to be here today and to contribute to this important discussion on how we can strike a fair and principled balance between transparency and privacy, two pillars of democratic governance that sometimes seem to pull in opposite directions, yet are in fact deeply complementary.

The legitimacy of public institutions depends increasingly on two things: first, their transparency in how they spend public funds and take decisions; and second, their respect for personal privacy and data protection. The challenge lies precisely at their intersection, particularly when personal data are embedded in official documents that the public has a legitimate interest to access often a complex and sensitive area. Public authorities are therefore challenged to find the right balance, a delicate balance between guaranteeing access to the information they hold and protecting the privacy rights of individuals.

The Council of Europe Convention on Access to Official Documents, establishes that everyone has the right to access State-held information, regardless of its form or medium. In parallel, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data enshrines the right to personal data protection as a fundamental human right.

Therefore, in practice, public authorities often struggle with how to act when:

- providing access to documents containing personal data,
- proactively publishing such documents, or
- responding to complaints either from data subjects or information requesters.

1. Legal Framework and Basis for Disclosure in Albania

Albania's Law No. 119/2014 "On the Right to Information" provides a comprehensive framework guaranteeing the right of every person to access public information held by public authorities. It classifies accessible information into two categories:

1. Proactively published information (available without request); and
2. Information provided upon request by an interested party.

Under Article 7 of the Law, each public authority must prepare and maintain a Transparency Program, which defines and proactively publishes key categories of information on its official website, in accessible and understandable formats.
Among these, paragraph (ë) specifically mandates the publication of:

"Information on procurement procedures or competitive concession/public-private partnership procedures conducted on behalf of the public authority, including:

i) the list of concluded contracts;
ii) the contracted amount;
iii) the contracting parties and a description of the contracted goods or services;
iv) information on implementation and monitoring of contracts, as well as relevant policies and guidelines."

This legal framework clearly obliges public authorities to disclose:

- the identities of private companies or organizations entering into contractual or financial relations with the state;
- the amounts and purposes of contracts or grants; and
- details concerning the monitoring and implementation of these arrangements.

In line with sectoral legislation and the Albanian Law No. 124/2024 "On the Protection of Personal Data", it is important to note that:
Data relating to legal entities (commercial companies or organizations) are not considered personal data and their disclosure is not restricted under data protection law. Accordingly, the names and financial details of companies, NGOs, and other entities benefiting from public funds, through procurement, grants, sponsorships, or donations, must be made public to ensure transparency, accountability, and integrity in public administration.

2. Practical Cases: Balancing Transparency and Privacy

The Information and Data Protection Commissioner of Albania has examined several cases where public authorities have denied access to information, often citing privacy or confidentiality concerns. The following cases illustrate how the Commissioner has interpreted and applied the law in balancing these rights.

Case 1: BIRN journalist vs. Independent Qualification Commission (Sponsorship Case)
Request: Information on the private company that financed the Commission's event "Report & Strategy" (30 September 2021, "Marina Bay" Hotel, Vlora), worth 300,000 ALL, and a copy of the sponsorship contract.

Authority's Response: *Provided an anonymized version of the agreement, citing privacy under Article 17(6) of the Law.*

Commissioner's Finding: The authority wrongfully anonymized the names of private companies. These are not personal data under Law No. 9887/2008 "On Personal Data Protection." Legal entities are not data subjects, and disclosure was necessary to ensure transparency in the financing of a public institution.

Case 2: NGO "Res Publica" Center vs. Ministry of Finance and Economy (Donations after the 2019 Earthquake)
Request:

- The total amount of donations collected from private, domestic, and foreign entities;
- A list of donors and their respective contributions.

Authority's Response: *Refused disclosure, claiming donors had not given consent for publication and that data were held by commercial banks*.

Commissioner's Finding: The Ministry failed to justify its refusal under Article 17 of the LDI. Since the funds were managed through the State Treasury, disclosure was necessary to ensure transparency and accountability in the management of public disaster-relief resources.

"In another case involving the same public authority, the Ministry of Finance and Economy, information was refused regarding loans granted to companies during the COVID-19 period, where the State acted as guarantor of the loan agreements, on the grounds of confidentiality and data protection."

Case 3: NGO vs. National Youth Agency
Request: Information on NGOs benefiting from state funding under Calls No. 4 and No. 5, including project titles, implementation areas, awarded points, and grant amounts.

Authority's Response: *Denied access, arguing NGOs had not consented and invoking privacy protection under Article 17(1).*

Commissioner's Finding: Under Law No. 80/2021 "On the Registration of Non-Profit Organizations", organizational data such as name, purpose, and legal representative are publicly available through the Official Judicial Bulletin.
Since these organizations received public funds, the public interest in disclosure overrides privacy claims. NGO information cannot be treated as personal data.

Case 4: "Albanian Center for Quality Journalism" vs. Agency for Agricultural and Rural Development (IPARD Program)
Request:
Access to all projects funded by the EU and Albanian government for agritourism under the IPARD program (Calls I–IV).

Authority's Response:
Refused disclosure, citing confidentiality clauses in the Sectoral Agreement with the European Commission and copyright protection under Law No. 35/2016 "On Copyright and Related Rights."

Commissioner's Finding:
The authority failed to justify its refusal through a proportionality test. Annex 8 of the Sectoral Agreement explicitly requires publication of funded projects.
Moreover, Article 78 of the Copyright Law permits authorities to reproduce and disseminate works for administrative purposes without author consent.
Thus, disclosure of IPARD project details is lawful and necessary to ensure transparency over EU and national funds.

3. Key Takeaways

- Legal entities (companies, NGOs) are not protected by data protection rules governing personal data.
- Recipients of public funds are subject to enhanced transparency obligations.
- Any restriction to access must be legally grounded, necessary, and proportionate under Article 17 of the LDI.
- The public interest in transparency about how public money is used outweighs privacy claims when the data concern institutional or financial relationships.
- These practices align with European and Council of Europe standards on transparency, integrity, and open governance.

Thank you for your attention!

Gonzalo SOSA
Representative of the Electronic Government Agency and the Information and Knowledge Society, Uruguay / *Représentant de l'Agence pour l'administration électronique et la société de l'information et des connaissances, Uruguay*

First of all, thank you for the invitation to participate in this discussion. It is very important to have these kinds of conversations between data protection and access to public information authorities.

The name of this event refers to two sides of the same coin, reflecting the link between them, but we must not lose sight of the fact that, in reality, we are dealing with two intersecting rights, and the important thing is to find the right balance.

Furthermore, this dialogue should be a first step towards future dialogues where we focus not on the boundaries between these two rights, but on how both rights, together, can provide greater guarantees for individuals. For example, in Uruguay, the Digital Government Agency, the Public Information Access Unit, and the Data Protection Authority have worked together to provide guidelines that bring greater transparency to the use of Artificial Intelligence systems within the government.

Since we are sharing national experiences on these topics at this event, I would first like to provide some context about Uruguay. Laws on access to public information and the protection of personal data emerged in 2008, along with the corresponding regulatory authorities, as cornerstones of digital transformation, recognizing the important role these rights play in protecting individuals not only in physical but also in digital environments.

The specific question in this panel aims at understanding data protection aspects related to individuals who represent or work for private entities that receive funds from or contract with the State.

The first thing to remember is that these individuals are also data subjects, and the companies that employ them or that they represent are bound by the relevant regulations, in particular, data protection laws. In this context, we must consider the modernized Convention 108 of the Council of Europe (Convention 108+).

Secondly, we must remember that in many cases these private entities are not directly obligated by laws on access to public information, or if they are, there are restrictions on access to information about their activities. However, this does not mean that information cannot be obtained from the data held by the public entities that interact with them.

Additionally, other regulations must also be considered, such as those governing anti-corruption measures in public administration and public procurement, among others.

The information of the aforementioned data subjects is ultimately held by both public and private entities, and both can be considered data controllers, bound by data protection laws. This is further supported by point 16 of the explanatory report to the Tromsø Convention.

However, this cannot in any way be used as an argument to maintain that data protection regulations restrict access to public information. This is a notion that must be eradicated, but it is true that, since both are fundamental rights, we must find the appropriate balance.

And how have we sought a balance on this issue in Uruguay? There is a 2023 resolution from the Public Information Access Unit that addresses the personal data of individuals linked to companies contracted by the State. This resolution states that the criteria applied regarding the disclosure of their personal information should follow similar principles to those used for the disclosure of personal data of public officials, applied by both the Public Information Access Unit and the Uruguayan Data Protection Authority (URCDP).

Generally, the distinction in this matter is linked to whether or not the information is strictly related to the service that the data subject is providing to the private entity, and in relation to the obligation assumed by the private entity towards the public entity. There are various examples in Uruguay in different resolutions, both from the Public Information Access Unit and the data protection authority.

But beyond the specific criteria in this regard, I would like to reiterate the importance of dialogue and collaboration among these authorities to develop and provide guidelines for the public administration in general. This dialogue should also involve anti-corruption authorities, public procurement authorities, and others.

This would undoubtedly help to provide greater clarity on aspects such as:

a. The scope of information related to data subjects who work for private entities that contract with or provide services to public entities, which the latter require to comply with various legal provisions, including the personal data protection law (data minimization, purpose limitation and other relevant principles).
b. Mechanisms for complying with transparency and anti-corruption regulations when disclosing personal information, including, for example, generating public versions for publication.
c. The nature and definition of specific contractual clauses for the processing of personal information in tender documents and others.
d. The definition of clear and detailed processes for the anonymization of personal information.
e. Collaboration among Data Protection Officers, transparency officers, and data officers in public entities, through committees or other mechanisms.

It is relevant to reiterate the importance of public entities not being able to evade their transparency obligations under the pretext of possessing personal information. Instead, they must carefully consider the implications and, where appropriate, provide only partial information.

Finally I would like to conclude by emphasizing the need to work on capacity building and education within both public and private entities. In Uruguay, we have several examples of joint courses and training programs. Furthermore, from a personal data protection perspective, we recognize the need to establish a strong community of data protection officers within the public and private sector entities, to ensure this issue permeates all organizations.

Thank you very much.

Vita HABJAN BARBORIĆ
Head of the Development and Prevention Centre Commission for the Prevention of Corruption, Slovenia / *Cheffe du Centre de développement et de prévention de la Commission pour la prévention de la corruption, Slovénie*

Objective of the presentation

- Importance of transparency in lobbying
- GRECO's findings
- Relationship between transparency and privacy

Transparency in lobbying

GRECO's findings and recommendations

GRECO's findings and recommendations:

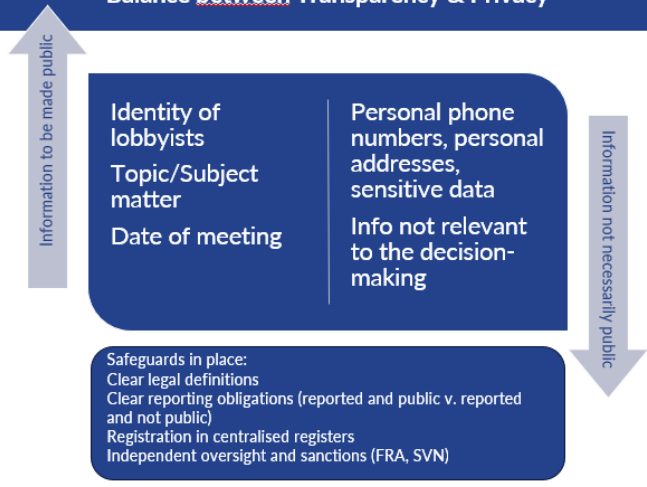
- Focus on officials

  and invite countries to (overwhelming majority of recs.):
  - Introduce rules for how officials interact with lobbyists
  - Require disclosure of lobbying contacts

  and, in rare cases, to:
  - Require registration of all lobbyists in the registration register (FRA)
  - Develop guidance (CYP)

- Oversight and sanctions (AUS)

Balance between Transparency & Privacy



Good practices

- Iceland: guidelines governing communication between PTEFs and lobbyists issued
- Luxemburg: amendments to the Grand Ducal Order → setting out the rules of conduct for members of the government and for advisers
- Estonia: Good Practice in communicating with lobbyists adopted → contains rules to provide a framework for contacts of PTEFs with lobbyists (e.g. following principles of equal treatment and transparency when planning and implementing policy decisions; refusing gifts or other benefits from lobbyists or their representatives; refraining from entering into a contractual relationship as part of ancillary activities with a lobbyist or their representative; refraining from being employed by a lobbyist who directly sought to influence them in their area of government)
- Cyprus: a law is in place, practical guidance issued

Conclusion

- **Transparency & Privacy are compatible**

However:

Thank you !
GRECO website : www.coe.int/greco/
GRECO mailbox address: webmaster.greco@coe.int

Ádám FÖLDES
Legal and Advocacy Advisor, Transparency International / *Conseiller juridique et chargé de plaidoyer, Transparency International*

Please raise your hand if you have ever come across such situation that a court issued a note to explain its own judgment?

Be it a national court or regional/international court. Not a press release, not a summary, not a case in case reporter, but some kind of explanation. Now, keep your hand up if it was in a data protection, right to privacy, or right to information case.

I will start from a bit far away, but will get to the point, why I asked you to raise your hands.

1. **Managing information about private persons dealing with public authorities is the title of the session, but do the authorities know with which persons they actually are dealing with?**
    - Can they identify them at all, or do they just handle personal data of some individuals (but who knows who they are)?
    - Do they handle personal data of some individuals, but in fact these individuals are not more than proxies for other individuals?
    - Are the authorities aware that they are dealing with proxies?

Obviously, these proxies have the right to personal data protection and right to privacy, but their position in this relationship with public authorities is not obvious.

When we talk about balancing right to personal data protection and right to privacy on the one hand, and right to information and public interest in transparency on the other, then do we know (do the authorities know?) whose data protection/privacy rights are balanced? And does it matter whose rights are balanced?

My point is: in order to strike a proper balance, the nature of the relationship between the authority and the individual, and also the entire context, is important. Furthermore, we also have to look at the purpose of the law, such as data protection law.

a) A well-known type of proxy:

In most of these relationships, there is a legal person. The natural person comes in either as a representative of the legal person, such as a manager who is authorised to negotiate and commit to contractual obligations on behalf of the legal person. For example, it can be a bidder or winner of a public tender, or someone requesting a permit in a heavily regulated industry, or someone who is requesting compensation from the state for administrative damages, etc. This relationship is rather transparent. Such manager's personal data are handled in the context of being a representative of a legal person only.

b) A less well-known proxy:

There are less transparent relationships. In the anti-money laundering lingo, there are Trust and Company Service Providers, who provide services such as being nominee shareholder for another person or acting as director of a shell company. There, the purpose is to hide the ultimate beneficial owners, the true owners, those natural persons who ultimately own or control the legal person, or on whose behalf a transaction is being conducted. In these, there is not only a layer of a legal person, but there can be several layers of legal persons and formal or informal human proxies.

2. **We are deep in the jungle: representations, proxies, complex rules of transparency and obscurity. So, how can we cut through this jungle? The Tromsø Convention says: "Limitations shall be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting: […] privacy and other legitimate private interests". It does not mention personal data protection, it merely lists "privacy and other legitimate private interests". I couldn't agree more. If we look at the data protection convention (Convention 108) from 1981/1985, it protects "rights and fundamental freedoms, and in particular his right to privacy". So, how does this relate to corporations and other legal persons?**

According to an oft-quoted 1992 judgment of the European Court of Human Rights (ECtHR), "respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings" which also includes "activities of a professional or business nature".

18 years and few hundred km on, the Luxembourg Court (CJEU), in their farm subsidy judgment, just "forgot" the first part of the sentence about human beings and ruled "there is no reason of principle to justify excluding activities of a professional … nature from the notion of 'private life'".

Three years ago, in the Sovim case, the CJEU used again this truncated reasoning and ruled that letting the general public identify beneficial owners of corporate and other legal entities, in the context of anti-money laundering, is disproportionate interference with these individuals' right to data protection and right to private lives. By the way, not a single word about right to information in the judgment.

Apparently, shining a light on their identities would mean that beneficial owners can no longer establish and develop relationships with other human beings.

3. Putting irony aside, this all can boil down to one question: what is the purpose of protecting personal data?

My answer is that this purpose is the right to privacy. The right to respect for private life. The right to be let alone. When someone is offering services or products, entering into business transactions with the state or with anyone, it has not much to do with privacy, quite the contrary. Or, let's just go back to what the ECtHR said: "respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings".

What is this certain degree?
It is hard to define it precisely. What we can see is that when someone is a private entrepreneur, then he/she is clearly identifiable when taking part in business; all partners can know who one is dealing with, who is subject of rights, obligations, any kind of responsibility in this business relationship.

When the same entrepreneur sets up a company, a legal person for the same purpose, suddenly we are left to the mercy of corporate transparency laws. For the last few decades, very often also to the mercy of laws of tax havens and offshore jurisdictions that withhold beneficial ownership information, and last but not least, also to data protection laws that are often applied disregarding their privacy protection purpose (see the Convention 108 of the Council of Europe).

When, three years ago, the CJEU in the Sovim judgment ruled that beneficial ownership information shall not be accessible to the general public, it not only disregarded the right to information, a vast range of public interest considerations[1] for transparency, the meaning of privacy and the purpose of personal data protection but also brought upon itself a major embarrassment. Less than a month after the judgment they published an explanation of the judgment, a so called "Review of the judgment", on their LinkedIn page.

Three months later, investigative journalists found that the client in one of the two underlying cases that resulted in the judgment "has been the owner or director of over 110 companies registered in countries around the world, including well-known secrecy havens like Belize, the British Virgin Islands, and Luxembourg." He apparently acts as a proxy for very dubious figures – including one of them identified as having been convicted in a grand corruption scandal – and he is also co-founder and CEO of the second largest private jet company in the world.

Obviously, he also has the right to respect for his private life, but his business has nothing to do with it, and acting as proxy to hide the identity of other individuals even less. This is not just some restriction of the right to information but an utter disrespect of the essence of this right when it comes to individuals hiding behind proxies to escape the jurisdiction of the information laws.

[1] The closure of beneficial ownership registers (the personal data of who owns, controls and profits from companies) to the general public gravely undermines among others
- Fair competition for public tenders
- media pluralism
- Free and fair political competition

This publication compiles presentations given in a workshop co-organised by the Council of Europe Access Info Group established under Council of Europe Convention on Access to Official Documents (Tromsø Convention), the Committee of Convention for the protection of individuals with regard to the processing of personal data and the Council of Europe's Group of States against Corruption (GRECO).

The workshop examined the intersection of the right to access information about public officials and persons dealing with public authorities and their individual right to personal data protection in the context of mandatory transparency legal regimes and lobbying. Presentations highlight the standards of the above-mentioned Council of Europe Conventions, relevant GRECO recommendations about assets' declaration and lobbying, as well as various national experiences in balancing the right of access and the right to personal data protection.

Cette publication rassemble les présentations délivrées lors d'un atelier coorganisé par le Groupe Accès à l'information du Conseil de l'Europe, créé en vertu de la Convention du Conseil de l'Europe sur l'accès aux documents publics (Convention de Tromsø), le Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel et le Groupe d'États contre la corruption (GRECO) du Conseil de l'Europe.

L'atelier a examiné le croisement entre le droit d'accéder à des informations sur les fonctionnaires et les personnes traitant avec les autorités publiques et leur droit individuel à la protection des données à caractère personnel dans le contexte des régimes juridiques de transparence obligatoire et du lobbying. Les présentations mettent en évidence les normes des conventions du Conseil de l'Europe susmentionnées, les recommandations pertinentes du GRECO concernant la déclaration de patrimoine et le lobbying, ainsi que diverses expériences nationales en matière d'équilibre entre le droit d'accès et le droit à la protection des données à caractère personnel.

PREMS 166025

BIL

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

Le Conseil de l'Europe est la principale organisation de défense des droits humains du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits humains, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE