# Activity Report
# Data Protection Commissioner

June 2024 – May 2025

**Table of Contents**

## *Foreword*

Convention 108 was opened for signature by Council of Europe member states on 28 January 1981 and came into force in 1985. In 2011, work began on updating this treaty – the only legally binding international data protection instrument – which has been ratified by all Council of Europe member states, as well as nine non-member states. The resulting amending protocol was adopted by the Committee of Ministers on 18 May 2018 and opened for signature by the parties on 10 October of the same year. The protocol will enter into force once it has been ratified by at least 38 parties. To date, there have been 33 ratifications, but it is becoming increasingly urgent that the minimum threshold of 38 ratifications be reached quickly, for the future of data protection law both in Europe and around the world. Otherwise, there is a risk of the convention becoming obsolete, which would greatly reduce its relevance beyond Europe and undermine the credibility of the Council of Europe. Let us not forget that the convention constitutes the backbone of universal data protection regulations. It sets a high standard, yet its general nature provides enough flexibility to accommodate the various legal systems and the diversity of situations in the regions of the world. Alongside the Convention on Artificial Intelligence, Convention 108+ establishes a robust framework for safeguarding human rights and fundamental freedoms in the context of AI.

Unfortunately, current trends do not appear to be conducive to data protection. Today, human rights and fundamental freedoms, including the right to privacy and data protection, are under increasing threat. Much of the world, particularly in Europe and the Middle East, is plagued by war. People are becoming victims of conflict, famine, persecution and repression at an alarming rate, and are all too often forced to flee their homeland. Extremist and authoritarian regimes are gaining ground and rising to power at the expense of democracy and the rule of law, in a world where the allure of power and profit outweighs all ethical and legal considerations. Although there is a constant strengthening of security policies, such as plans to install video surveillance systems with facial recognition technology and requirements for messaging providers to reduce data encryption levels or retain data relating to digital communications, the necessity and effectiveness of such policies are rarely understood or assessed. The risk of sliding towards mass surveillance has become very real. However, ensuring the security of people and property must not come at the expense of human rights and fundamental freedoms.

Lobbying by digital oligarchs is calling into question some of the regulations that govern the virtual world in which we operate. As the philosopher Mark Hunyadi has pointed out, the problem with AI-enhanced digital technology “is that it is gradually imposing a relationship with the world mediated by technical devices on everyone, in all areas of their lives, effectively

making digital technology a prerequisite for interacting with the world."[1] Society will increasingly be governed by algorithms. These developments put data protection authorities under pressure, and their independence – which is fundamental to ensuring the effectiveness of the right to data protection – is all too often called into question.

Generative artificial intelligence has become an inescapable reality. The use of AI tools in neuroscience is booming. While AI undoubtedly has many benefits and applications that could have a positive impact on humanity, particularly in terms of performing tedious tasks and treating diseases, it also carries risks that could quickly lead to increased surveillance and monitoring of people's activities, behaviour and even thoughts, which could hinder decision-making skills. The development of predictive AI, particularly in the fields of crime and healthcare, is also advancing rapidly. This brings new challenges, including with regard to data quality and respect for human rights and fundamental freedoms, and the risk of injustice, violations of dignity and discrimination. The risk that advocates of "surveillance capitalism" will exploit the data generated by these technologies and use it to influence and manipulate people's behaviour and choices is becoming all too real. AI is also helping to bolster some governments' mass surveillance policies. "If AI develops in societies whose functioning and decision-making abilities have been completely upended, all the considerable benefits of this technology in fields such as research and healthcare will be negated."[2] Without clear commitments from the various stakeholders to uphold ethical principles that respect human rights and fundamental freedoms – including the right to privacy, the right to informational self-determination and the right to human dignity – and without binding legal frameworks to govern these technologies, we risk opening Pandora's box, and there will be no turning back.

In light of this downward spiral, has data protection become irrelevant and are we powerless to prevent a world in which all policies, including the suspension of the rule of law, democracy and human rights, are justified by the need for security and a desire for technological domination and power?

All hope is not lost! Now more than ever, the Council of Europe must firmly commit to promoting and defending its core values of human rights, democracy and the rule of law. This can only be achieved by promoting the right to data protection and integrating related policies. Convention 108+ must be ratified and enter into force without delay – as must the Framework Convention on Artificial Intelligence.

While the work carried out and the regulations established by data protection authorities are vital, raising awareness, providing education and offering training are also crucial for the future of data protection, particularly among younger generations. If they are able to develop and

[1] "IA: la bataille de l'esprit", *Revue Esprit*, April 2025
[2] Interview with Giuliano da Empoli, *Le Temps*, 5 April 2025

embrace data ethics that respect human rights and fundamental freedoms, they can help to build a world based on mutual trust and respect for everyone's informational autonomy.

The Council of Europe is still in the process of implementing its new data protection regulations and will soon have a modern instrument at its disposal. The training programme for staff members should finally get underway. However, given the Organisation's limited resources, the challenge will be to finally allocate sufficient funds to ensure the effective and exemplary application of these regulations. To remain an active and credible ambassador for the promotion of data protection rights in Europe and around the world, the Council of Europe must lead by example.

## 1. Introduction

The terms of reference of the Council of Europe Data Protection Commissioner were initially set out in the Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe. In Resolution CM/Res(2022)14, the Committee of Ministers adopted the new Council of Europe Regulations on the Protection of Personal Data.

On 1 January 2023, the Organisation's new regulations entered into force, with a two-year transition period.

In accordance with Resolution CM/Res (2022)14, the Data Protection Commissioner in office on the date of the entry into force of these Regulations will continue exercising their duties until the expiry of their mandate, without prejudice to the possibility of them being re-elected pursuant to the provisions of the present Regulations.[3]

Pending the entry into force of Convention 108+, the Data Protection Commissioner is elected by the representatives of the member states in the Convention Committee established under Article 18 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

Jean-Philippe Walter, the current Commissioner, was initially elected at the 36th plenary meeting of the Consultative Committee of Convention 108 held in Strasbourg from 19 to 21 June 2018. He was subsequently re-elected in June 2021 at the 41st plenary meeting of the Consultative Committee, under the previous regulations. His term of office, extended by one year in 2024, runs until the end of June 2025, and his successor will be elected by the Consultative Committee at its 48th meeting. The new Commissioner will take office on 1 July 2025.

Under Article 17 of the new Regulations, the Data Protection Commissioner must prepare and publish an annual report outlining their activities. The report must be presented to the aforementioned Convention Committee for information; it is then forwarded to the Secretary General and made public. The present report covers activities between June 2024 and May 2025.

[3] Article 3 of Resolution CM/Res (2022)14.

## 2. Physical presence at the Organisation's headquarters and representation

### 2.1 *Visits to the Council of Europe*

Since June 2024, the Data Protection Commissioner has made three working visits to the Council of Europe. During these visits, he met with staff members at their request and held discussions with various heads of departments, thereby maintaining productive dialogue with representatives from many administrative entities, as well as with several staff members involved in the Organisation's data processing operations. He also held regular meetings with the Staff Committee and its Chair regarding the processing of staff data. In addition, he met with the Director of the Secretary General's Private Office, which was an opportunity to review recent data protection developments at the Council of Europe. He also held several videoconference meetings. No formal complaint was lodged with the Commissioner during the reporting period.[4] Requests, especially those related to the right of access, were directed to him and dealt with in the first instance by the Data Protection Officer (DPO). The Commissioner also sought clarification in relation to the deployment of several IT tools and the use of AI. He issued an opinion on the internal staff recruitment procedure.

In terms of representation, the Commissioner published a statement to mark the 19th Data Protection Day and responded to several media enquiries. He also responded to surveys conducted as part of scientific research projects.

During the reporting period, the Commissioner continued to exchange information and collaborate with the Committee on Convention 108, its Chairperson and the Bureau of the Committee. At the end of 2024, he also took part in the exchange of views organised by the Secretariat on preparations for the entry into force of Convention 108+, as well as in the seminar on artificial intelligence and data protection.

### *2.2 Participation in external events*

The Commissioner is regularly invited to participate in seminars and conferences, whether to present the Organisation's own data protection framework or to speak about the modernisation of Convention 108 and the work of the Consultative Committee on topics including data protection, artificial intelligence, digital identity and facial recognition. He also participated in the Global Privacy Assembly annual meeting held in Jersey, Channel Islands, from 28 October to 1 November 2024, giving a brief presentation of the Council of Europe's new regulations and his role. However, he was unable to attend the spring conference of European data protection authorities, held in Georgia at the beginning of May, as he had not received the necessary information.

## 3 Advice and recommendations for Council of Europe entities

The Commissioner was asked to provide opinions and recommendations, and even make decisions, on compliance with the right to personal data protection across different fields of activity and technologies. The main topics covered are summarised below, broken down by the relevant department or entity.

### *3.1 Directorate of General Services (DGS)*

Various topics were discussed, including the issue of video surveillance, which remains on the Directorate's agenda. The Commissioner regularly consults the data extraction registers (video surveillance and access badges). During his last visit in February 2025, the DGS

[4] Dates of working visits: 7-8 October 2024, 24-25 February 2025 and 19-20 May 2025.

informed him that, following a security audit, consideration must be given to strengthening certain measures. In the future, AI and facial recognition might also be used. Under Article 9 of the Organisation's data protection regulations, any technological development of this kind must be subject to extensive analysis of its potential impact on the fundamental rights and freedoms of the data subjects prior to its deployment, and the resulting data processing operations must be designed in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. The need for such developments will have to be clearly demonstrated. Where appropriate, the use of AI for safety and security purposes will have to be governed by a specific regulatory framework. However, the Commissioner is calling for some self-restraint; these technologies should not be deployed too quickly without foresight, as this could harm the Organisation's image. In addition, the DGS is working with the Directorate of Information Technology (DIT) to align standards in the Council of Europe's external offices with those in Strasbourg. To ensure a consistent approach to safety and security measures, the Commissioner favours assigning responsibility for external offices to a single entity. Furthermore, as set out in his activity report for July 2018 – November 2020 (p. 8) and his recommendation of 6 June 2019, the Commissioner notes that the use of biometric authentication technologies for access control at the Council of Europe is currently neither necessary nor appropriate, given the risks involved. Lastly, the replacement of access badges, which is due to take place soon, must comply with his previous recommendations, particularly those relating to the issuance of neutral badges on which no personal data is visibly displayed (see Activity report for November 2020 to October 2022, p. 7). Machine reading of data is sufficient for access control purposes; however, badge holders must be clearly informed of the data stored on their badge and in the access control system.

### *3.2 Directorate of Human Resources (DHR)*

The Commissioner continued to liaise regularly with the Directorate of Human Resources.

In particular, he once again raised the issue of the new staff recruitment procedure, which should make it possible to limit the collection of personal data in the first phase of the procedure by simplifying the form used. The use of artificial intelligence in the recruitment process was also discussed. The Commissioner emphasised the importance of ensuring the quality of data processed within the system and welcomed DHR's approach of maintaining the requirement for human review prior to any decision being made. AI would be used for the initial screening process.

The Commissioner also issued an opinion on the internal recruitment procedure. At present, for reasons of transparency, candidate lists are published on the Council of Europe's intranet site and can be consulted by anyone with intranet access. In addition, direct managers are notified when their subordinates submit an application. The Staff Committee is in favour of this procedure because it fears that changes would not guarantee fairness. Having been contacted by several staff members questioning this practice, the Commissioner raised the issue with DHR and was asked for an opinion. In his initial findings, the Commissioner considered that the publication of a list of internal vacancy applicants on the intranet was not grounded in an overriding interest in transparency that outweighed the right to data protection and privacy of the staff members concerned, particularly given the potential risk of harm. Line managers should be informed by the relevant staff member if they so wish, and at a time that is convenient for them. However, publishing the number of candidates shortlisted after the selection process and information about the successful candidate did not raise any data protection issues. To the best of the Commissioner's knowledge, the practice is not used by

any Council of Europe member states or other European institutions. Discussions continued with the Staff Committee and DHR. After further analysis, the Commissioner recommended that DHR stop publishing candidate lists for internal vacancies and implement measures to ensure that recruitment procedures are carried out as they should be. The Commissioner concluded that there was no legal basis for publishing candidate lists. Furthermore, publishing the list of internal vacancy candidates on the intranet does not achieve the desired objective of a fair, objective and non-arbitrary recruitment procedure. Therefore, it is disproportionate, and the protection of data subjects against the risk of infringement of their rights outweighs the interest in publishing such information.

The Commissioner was contacted by a staff member who complained about the excessive collection of personal data in connection with the reimbursement of travel expenses. Following further clarification by the Commissioner in collaboration with the DPO, it was found that unnecessary information had indeed been requested during a system change. The information has now been deleted. On the basis of his findings, the Commissioner concluded that this error had been an isolated incident.

The Commissioner held an initial meeting with the Organisation's Ethics Officer, who outlined the main aspects of her remit. Data protection requirements demand particular attention on her part, especially with regard to maintaining confidentiality and preventing unauthorised disclosure. It was agreed that dialogue would continue and that ways of establishing closer co-operation would be explored.

The Commissioner participated in a meeting of DHR's Well-being Network, which brings together a range of stakeholders who play different, yet overlapping, roles in staff well-being (including the Ethics Officer, DHR, mediators and Staff Committee members). The network meets regularly to discuss issues affecting the Organisation and to co-ordinate the steps to be taken. It is also tasked with dealing with individual situations, which may require knowledge of the identities of those involved. Participants discussed the need for robust guarantees of data protection and confidentiality. The Commissioner emphasised the importance of obtaining consent from data subjects before sharing their personal data and recommended drawing up a charter or set of regulations for the network.

### *3.3 Directorate of Information Technology (DIT)*

Regular dialogue between the DIT and the Commissioner continued. The introduction of generative AI within the Organisation is a priority issue for the DIT, which is currently testing various IT solutions. The Commissioner attended a demonstration showcasing the potential for integrating AI into information processing, including for tasks such as taking minutes, translation, reporting, research and documentation.

The Commissioner considers that the Organisation's future work will inevitably involve the use of AI. Before any decision on deployment is taken, there should be an in-depth consideration of the matter. AI deployment must be properly regulated and a legal framework specific to the Organisation must be adopted, based on the Framework Convention on AI. The use of AI must be transparent, and users must undergo special training. Furthermore, the introduction of any artificial intelligence system must be preceded by and based on an assessment of its potential impact on human rights and fundamental freedoms in relation to the processing of personal data. The threshold of acceptable risk must also be defined, which implies risk management and measures to prevent and minimise such risks. It is recommended that a dynamic assessment methodology be developed and integrated into risk management. This

involves taking a structured approach to assessing the risks and impact of AI systems in relation to data protection.

## 4 Data Protection Officer (DPO)

During the reporting period, the Commissioner worked closely with the DPO on a variety of issues. He regularly sends the DPO requests for further clarification following questions from data subjects in relation to the exercise of their rights. The Commissioner also gives his opinion on various projects and data protection impact assessments. There is regular dialogue on these various issues.

The implementation of the new regulations remains the DPO's top priority. This involves running an awareness-raising and training programme for staff members, which was set to be launched in spring 2025. The mapping of processed data (data processing register) within the Organisation is behind schedule, but remains one of the DPO's priorities. This is an important tool for ensuring the transparency of data processing and, in particular, facilitating the exercise of data subjects' rights.

Under the terms of Article 11 of the regulations, staff members and other members of the Secretariat are required to:

- "treat any personal data with utmost care;
- refrain from any processing of personal data that is not necessary, legitimate and appropriate in the light of their professional duties, these Regulations and the implementing instruments thereof;
- seek the Data Protection Officer's advice, in a timely manner, where required by these Regulations or the related procedures and guidelines; and act in accordance with the Data Protection Officer's recommendations;
- co-operate at all times with the Data Protection Officer and the Data Protection Commissioner;
- identify, at her or his level, and promptly inform her or his hierarchical superior and the Data Protection Officer of any circumstances which may result in risks for the protection of personal data."

Staff members who fail to comply with the regulations are liable to disciplinary action.

To fulfil these obligations and ensure that data protection requirements are adhered to on a daily basis, it is essential that all staff members complete the training programme and receive the necessary data protection information.

The task assigned to the DPO is huge, and the glaring lack of resources at her disposal greatly hinders the effective enforcement of the regulations. It is urgent that these resources be strengthened.

## 5 Remit and organisation of Data Protection Commissioner's work

In accordance with Convention 108+, Article 15 of the Regulations provides that the Commissioner is an independent supervisory authority responsible for overseeing the compliance of personal data processing carried out by the Organisation. The Commissioner has powers of intervention and investigation, including decision-making powers. They are tasked with:

- monitoring and ensuring the application of the provisions of the regulations;
- examining complaints from data subjects and ordering remedial action;
- conducting inquiries;
- formulating opinions at the request of the DPO;
- making recommendations to the controller;
- co-operating with national or international data protection authorities, including those of international organisations.

As noted above, the Commissioner's tasks include writing and publishing an annual report on their activities. Convention 108+ and Article 15 thereof entitle them to express their opinion on current data protection issues and draft regulations or administrative proposals involving the processing of personal data, even though the Organisation's regulations do not explicitly lay down this right. This should be clarified when the regulations are revised to bring them into line with Convention 108+.

Lastly, the Commissioner examines complaints lodged by data subjects and communicates their findings, which are final and binding, to the Secretary General, who must take a decision on that basis. Data subjects may appeal against the decision to the Administrative Tribunal if they are a current or former staff member, a person entitled through them or a job candidate. For other persons contesting the decision, an amicable agreement should be sought, and, if no settlement can be reached, the dispute will be submitted to final and binding arbitration.

The Commissioner's functions and powers have been significantly strengthened and involve carrying out a comprehensive analysis of how the Organisation is dealing with the systematic use of digital technologies, including AI, in the tasks and functions of all staff members, at both the Organisation's headquarters and its other offices. The system itself is robust and provides all the necessary powers and faculties to ensure compliance with data protection provisions at the Council of Europe. In practice, however, the Commissioner lacks the necessary resources to fulfil their mission in full compliance with the regulations. They work on a voluntary basis and do not have a properly staffed secretariat to provide the necessary support for their activities. While the Data Protection Unit provides the Commissioner with dedicated and professional assistance, it is already understaffed for its own tasks and can therefore only offer limited assistance, primarily in organising visits. Consequently, the Commissioner is unable to carry out comprehensive analyses, inquiries or investigations into the various data processing systems, as required by the Regulations. During the reporting period, this support was further reduced due to personnel changes in the secretariat and health-related absences.

In accordance with Article 15, the Commissioner is not an internal body of the Council of Europe, but an independent supervisory authority overseeing the compliance of personal data processing carried out by the Organisation within the provisions of its regulations. The Commissioner must have access to all the necessary resources to perform their duties in an effective, efficient and credible manner. Therefore, it is essential and urgent that the Commissioner be provided with the necessary human and financial resources to ensure the effective operation of their secretariat, which is responsible for preparing the Commissioner's opinions, decisions and reports, conducting research, providing documentation, conducting initial assessments of requests, answering questions and representing the Commissioner in their absence or at their request. The Commissioner should have their own budget. Without the means to uphold the Convention 108+ standard within its own walls, the Council of Europe cannot promote a high level of data protection in the public sphere.

## 6 Conclusions

The entry into force of the regulations on the protection of personal data was an important step towards ensuring respect for human rights and fundamental freedoms, particularly the right to privacy, when processing personal data within the Organisation. The two-year transition period for bringing the various data processing operations into compliance ended at the beginning of this year. However, much remains to be done, particularly with regard to prior consultation with the DPO and the Commissioner and ensuring that data protection impact assessments are carried out in a timely manner. Delays in providing training and running awareness-raising campaigns did not help this deadline to be met. Nevertheless, the Commissioner has noted a general improvement in the integration of data protection requirements and has not identified any serious breaches of the Regulations' provisions. Due to limited resources, the Commissioner was unable to conduct comprehensive analyses of the personal data processing operations submitted to them or carry out checks, however.

Going forward, the Commissioner and the DPO should be provided with the necessary human, financial, material and technical resources to ensure effective data protection within the Organisation.