Strasbourg, 21 May 2024

DPCOM Report 2022-2024

Activity Report
Data Protection Commissioner

November 2022 – June 2024

Table of Contents

Foreword

Not since the fall of the Berlin Wall has the threat of cataclysm weighed so heavily on our societies in Europe and around the world. We are witnessing backsliding on the human rights, democracy, and the rule of law, including with regard to the right to data protection. Devastating wars and persistent terrorist threats have led to a negative climate of insecurity. This in turn encourages the emergence of anti-democratic movements that are likely to challenge human rights, enshrined in particular in the Universal Declaration of Human Rights and the European Convention on Human Rights.

We are witnessing an increase in surveillance policies in the name of the safety of people and property that are not necessarily proportionate to declared objectives. Many governments no longer hesitate to set up widespread video surveillance systems based on facial recognition and biometrics, or to use mass surveillance and tracking technologies aimed at people's activities on the web which can put them at significant risk of discrimination and stigmatization. It should be remembered that the security of citizens cannot be achieved at the expense of human rights and that any measures put in place must guarantee the right to data protection.

This mass surveillance also continues to develop through many players in the digital economy through the limitless collection of data we all often provide unconsciously or thoughtlessly during our digital interactions. The processing of this data using artificial intelligence allows these actors to profile us and influence our actions, behaviours and decisions. It cannot be stressed enough that it is imperative not to abandon decision-making powers related to privacy to a few private actors at the risk of definitively undermining the rule of law, human rights and democracy. These actors must act in a transparent manner in compliance with the legal standards in force in order to restore confidence in the use of information and communication technologies. We must therefore work for the development of solutions based on a more democratic governance of data processing and its algorithms. The adoption on 17 May by the Committee of Ministers of the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, following the adoption by the European Union of its Artificial Intelligence Regulation, is an important and welcome step.

In this year 2024, we therefore find ourselves at a crossroads. While the outlook for the future is unfortunately not the most optimistic, there is a glimmer of hope with the very likely entry into force of Convention 108+ later this year, which should provide a new impetus for the protection of human rights and fundamental freedoms when processing personal data.

The Council of Europe, which is also strengthening its security and planning the use of artificial intelligence, particularly in the field of human resources, cannot be satisfied with seeking greater efficiency, increased productivity and streamlining business processes. It must be an example in the defence of its values, namely by defending of the rule of law, democracy and human rights when using technologies requiring the processing of personal data.

The entry into force of the new data protection regulation thus provides a framework conducive to ensuring the protection of individuals when processing personal data. However, it is necessary to invest quickly in the resources necessary to guarantee the effectiveness of data protection.

1. Introduction

The mandate of the Council of Europe Data Protection Commissioner was initially established by the Regulation of the Secretary General of 17 April 1989 establishing a data protection system for the Council of Europe's personal data files. By its resolution CM/Res(2022)14, the Committee of Ministers adopted the new Council of Europe Regulation on the protection of personal data.

These new regulations entered into force on 1 January 2023, with a two-year transitional period for the Organisation[1].

Thus, according to Resolution CM/Res (2022)14, the Data Protection Commissioner, depending on the date of entry into force of this Regulation, shall continue to carry out his or her duties until the expiry of his/her term of office, without prejudice to the possibility of being re-elected in accordance with the provisions of this Regulation[2].

Pending the entry into force of Convention 108+, the Data Protection Commissioner is elected by the representatives of the Member States to 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).

The current Commissioner, Mr Jean Philippe Walter, was elected at the 36th plenary meeting of the Consultative Committee of Convention 108 (Strasbourg, 19-21 June 2018) and re-elected, under the former regime, in June 2021 at the 41st plenary meeting of the Advisory Committee.

The activity report of the Data Protection Commissioner shall also be presented to the said Convention Committee. Under Article 17 of the new Regulation, the Data Protection Commissioner will prepare and publish an annual report describing their activities. The report must be submitted for information to the said Committee of the Convention; then it is sent to the Secretary General before being made public. This report covers the transitional period between two Regulations and reports on activities carried out between November 2022 and June 2024.

2. Council of Europe Data Protection Regulation

After some ten years of work, the Council of Europe has adopted modern data protection legislation, with the adoption on 15 June 2022 of Resolution CM/Res(2022)14 establishing the Council of Europe Regulation on the protection of personal data. . As stated in the introduction, this new regulation came into force on 1 January 2023.

The new Data Protection Regulation has two main objectives:

- Addressing the challenges arising from the use of new information and communication technologies, and
- Improving data protection within the Council of Europe by strengthening the rights of individuals and giving them more control over their personal data.

It is very important to emphasize that this regulation allows the Council of Europe to comply to a large extent with Convention 108+.

The purpose of the Regulation is to ensure the protection of all persons, regardless of nationality or place of residence, when personal data is processed by the various bodies and bodies of the Organisation, and thus to respect human rights and fundamental freedoms, including the right to privacy.

[1] According to Article 2 of Resolution CM/Res(2022)14 instituting the Council of Europe's Regulation on the protection of personal data, the Secretary General shall ensure that the processing of personal data already underway as of the effective date of this Regulation is brought into compliance with it within two years.
[2] Article 3 of said Resolution..

These rules apply to all processing of the Organisation carried out at the headquarters in Strasbourg or in the various external offices of the Council of Europe. However, it does not apply to the processing of the ECHR and the Administrative Tribunal in the context of their judicial activities. These processing operations must be governed by the rules adopted by these two judicial bodies. On the other hand, processing operations that do not fall within the scope of judicial activities remain governed by the regulations. It should be noted that the CEB is not subject to this and has its own data protection regulations.

The Regulation sets out the basic principles that must govern all processing (Article 4), namely compliance with:
- the principles of proportionality, lawfulness, fairness and transparency;
- the principle of purpose according to which data may only be collected for specified, explicit and legitimate purposes and are not processed in a manner incompatible with these purposes;
- the principle of adequacy, relevance and non-excessivity;
- the principle of accuracy;
- retention that does not exceed what is necessary for the purpose for which the data is processed.

It sets out the conditions legitimising the processing of data and in particular compliance with the principle of legality (Article 4.2).

It sets out the rights of data subjects and in particular the right of access, the right to transparency of processing, the right to rectification or erasure of data, the right not to be subject to an automated decision without the person being able to express his or her point of view, as well as the right to an effective remedy.

The regulation defines the obligations of data controllers, including the obligation to comply, carry out an examination of the potential impact of the processing on the fundamental rights and freedoms of data subjects, compliance with the principles of privacy by design and by default, transparency and reporting of data breaches.

To ensure compliance with data protection provisions, the Regulation provides for the establishment of at least one Data Protection Officer (DPO) who must be involved in all data protection matters. The DPO is the first point of contact before referring matters to the Data Protection Commissioner.

The institution of the Data Protection Commissioner is not new and was already in place under the previous regime. With the new regulation, its position, role and powers are strengthened.

In accordance with Convention 108+, Article 15 of the Regulation specifies that the Commissioner is an independent supervisory authority responsible for ensuring the compliance of the Organisation's processing of personal data. He has powers of intervention and investigation and, in particular, decision-making powers. As such, the Commissioner is responsible to:

- Monitor and ensure the application of the provisions of the regulations;
- Review claims from affected individuals and order corrective actions;
- Conduct investigations;
- Formulate opinions at the request of the DPO;
- Make recommendations to the data controller;
- Cooperate with national or international data protection authorities, including international organisations.

As previously stated, they must also write and publish an annual report on these activities. In line with Convention 108+, they should also be able to raise awareness of current data protection issues and give their opinion on draft legislation or administrative proposals involving the processing of personal data.

Finally, the Commissioner decides on the complaints of the persons concerned and transmits their conclusions, which are final and binding, to the Secretary General, who must decide on this basis. The person concerned may appeal against the decision to the Administrative Tribunal if they are a member of staff, a former member of staff, their successors or a job applicant. For other persons contesting the decision, an amicable agreement must be sought, and, in the event of failure, the dispute will be submitted to final and binding arbitration

Employees who do not comply with the data protection regulations are subject to disciplinary sanctions.

However, the obligation to comply, in particular by examining, before any processing, the potential impact of said processing on the rights and fundamental freedoms of the data subjects or the obligation to consult, when required, the DPO is not yet sufficiently integrated by the various services concerned. Some entities are not yet aware of the importance of data protection and are taking time to provide the requested answers or do so in an incomplete manner, requiring reminders from both the DPO and the Commissioner.

To be effective, the Regulation must be applied in an informed manner. Thus, a significant and priority effort must be made to raise awareness and train the Organization's staff on data protection requirements.

3. Physical presence at the headquarters of the Organization and representation

3.1 Visits to the Council of Europe

The Data Protection Commissioner was able to make several working visits to the Council of Europe. During these missions, he was able to meet with staff at their request and with the heads of various departments, thus continuing to maintain a rich and effective dialogue with representatives of many administrative entities, as well as with several staff involved in the processing of personal data by the Organisation. He also held regular discussions with the Staff Committee and its Chairman in relation to the processing of staff members' data. In addition, he met with the Deputy Secretary General, which was an opportunity to take stock of the situation in the field of data protection within the Council of Europe.

During the reference period, no formal complaint was lodged with the Commissioner[10]. Requests, in particular concerning the exercise of the right of access, were forwarded to him, which could be dealt with in the first instance by the DPO. He also sought clarification in relation to the deployment of several IT tools and opened an investigation into the introduction of Zoom in the Council of Europe.

The Commissioner issued statements on the occasion of the 17th and 18th editions of Data Protection Day and responded to several media requests. He responded to surveys as part of scientific research projects.

During the reporting period, the Commissioner continued to exchange and collaborate with the Committee of Convention 108, its Chairperson and the Bureau of the Committee.

[10] Dates of working visits: 14 December 2022, 20-21 February 2023, 5-6 June 2023, 9-10 October 2023, 12-13 February 2024 and 5-7 June 2024.

3.2 Participation in external events

The Commissioner is regularly asked to participate in seminars or conferences, whether it is to present the internal framework of the Organization or the modernization of Convention 108 ("Convention 108+") and the work of the Convention Committee (data protection and artificial intelligence, digital identity, facial recognition, etc.). During the reporting period, the Commissioner participated in and intervened in the following events, among others:

- 30 June 2023, Strasbourg, Sport and Human Rights Forum;
- 24-25 October 2023, Interpol, Lyon: "International Organisations Workshop on Data Protection";
- 7 November 2023 Strasbourg, Seminar under the aegis of TACE on the Data Protection Regulation.

The Commissioner did not participate, particularly for budgetary and organizational reasons, in the 45th World Privacy Assembly (GPA) which took place in Bermuda from 15 to 20 October 2023. However, he followed the work of the GPA throughout the year and supported several resolutions adopted at the 45th World Assembly.

4. Advice and recommendations to Council of Europe entities

The Commissioner has been called upon to issue opinions or recommendations concerning the respect of the right to the protection of personal data through different fields of activity or different technologies. The main topics covered are summarized below by department/entity concerned.

4.1 Corporate Services Directorate (CSD)

Various topics were discussed, including the issue of video surveillance, which is still on the agenda of the Directorate. The Commissioner notes with satisfaction that new signage in accordance with the new regulation has been put in place and that a document on good practices in video surveillance will be adopted. The Commissioner regularly consults the extraction registers (video surveillance and badges). During its last visit in February 2024, the Directorate informed the Commissioner of the ongoing audit by the Host State of the Council buildings in Strasbourg. Discussions were also held on the implementation of a badge access system to the office. In addition, special efforts are being pursued by the Directorate jointly with the Directorate of Information Technology (DIT), for the Council of Europe offices in the member countries, with the aim of upgrading in line with the Strasbourg standards.

Following the changes in the Organization's modus operandi after the COVID-19 pandemic, the Commissioner and the Administration conducted an intense dialogue on the correlation between the increased practice of online meetings and the need to ensure the protection of personal data. He has intervened on several occasions with the DPO about the use of cameras in meeting rooms and has demanded the establishment of a data protection impact assessment. These interventions made it possible to make a clear distinction in the management of security cameras in meeting rooms and video-conferencing systems. The Commissioner recalled the obligations in terms of transparency and demanded better information for those concerned on the use of cameras. Information should be available in each meeting room. Other issues are still under consideration and include the use of blurring, data handling processes including data deletion policy, file transfer via the cloud, etc. In addition, an audiovisual policy encompassing data protection requirements will have to be put in place.

4.2 Human Resources Department (HRD)

Several topics are on the agenda of the regular dialogue between the HRD and the Commissioner. In particular during the reporting period, the Commissioner made recommendations on the management of personnel files, their digitization and updating, the issue of transparency during internal competitions, the procedure for exercising the right of access, as well as the issue of vetting

or security analysis during recruitment which will be introduced to anticipate reputational and security risks within the Organization. The use of this verification procedure must be closely monitored from the point of view of the guarantees of the protection of personal data. In accordance with the principles of proportionality and necessity, the Commissioner recommends defining the functions to be subject to this procedure and distinguishing the level of analysis with regard to the risks involved. The most invasive level of analysis should be reserved for high-risk functions.

In addition, the interlocutors addressed the issue of the use of Artificial Intelligence in the recruitment process. The Commissioner notes the importance of ensuring the quality of the data processed in the system and also the need for a human eye before any decision is taken.

Finally, it should be noted that the HRD is open to working jointly with the Commissioner and the DPO on the introduction of internal training on the protection of personal data for all agents.

- ***Medical service***

The Commissioner also spoke with the medical service and was able to see that all medical data is treated in a strictly confidential manner. A dual storage system (paper and digital) has been set up. For the digital aspect, the department has used specific, secure and encrypted software, to which only the two doctors and nurses have access. The "paper" files are kept under lock and key. Medical data is kept for 30 years before destruction. The data is not transmitted to the insurance companies.

4.3 Information Technology Directorate (DIT)

The dialogue between the DIT and the Commissioner is regular, especially with regard to data security. In particular, the Commissioner is informed of recent activities in the field of securing the Council of Europe's IT systems in order to ensure data protection and security and to ward off hacker attacks.

The issue of audiovisual media storage tools also remains among the priorities. For some storage tools, the nomenclature is not yet in place and will require additional analyses, in close collaboration with the DIT (e.g. for the implementation of the management table process, on the data deletion policy, etc.). In general, the entire personal data storage policy and its retention period must be reviewed. The Commissioner favours the storage of data, at least for sensitive data, on internal media within the Organisation. The use of cloud info, if necessary, must meet high security requirements and in particular data encryption.

The Commissioner and the DPO are closely following the discussions led by DIT within the Organisation on the introduction of Artificial Intelligence. In particular, the question arises for the use of AI for the evaluation and re-evaluation of data already collected.

The introduction of Zoom in early 2023, of which the Commissioner had not been previously informed, was subject to a thorough review process. On the basis of a detailed report from the Data Protection Unit prepared at its request, the Commissioner addressed a series of questions to the administration in order to ensure that the use of Zoom would be carried out in compliance with the provisions of the Data Protection Regulation. The procedure required several clarification sessions and several reminders from the Commissioner to obtain answers to the various questions. It resulted in two formal recommendations.

In his conclusions and from a data protection point of view, the Commissioner considers that there is no reason to question the use of Zoom. However, the Committee is waiting for its recommendations to be taken into consideration. The conduct of this case was met with a certain misunderstanding, or even underestimation of the administration, of the role, status and functions of the Commissioner, which did not make it easy to obtain answers to the Commissioner's questions. A certain vagueness was also noted in the collaboration between the different services involved.

This file also highlights the weight of large digital companies that want to unilaterally impose their general terms and conditions and their user contracts without taking into account the particularities of an international organisation such as the Council of Europe. The Commissioner's intervention nevertheless allowed Zoom to accept the reference to the standard contractual clauses adopted by the 108 Committee and the CoE's data protection regulation. The Commissioner invites international organisations to examine the possibility of joining forces to negotiate with digital companies with regard to data protection requirements.

4.4 Internal Audit and Evaluation Directorate

During the reporting period, the Commissioner and the Internal Audit and Evaluation Directorate addressed a number of issues. An audit of internal recruitment took place in 2023 and questions about personal data arose. This made it possible to feed the conclusions and recommendations addressed to the HRD. Thus, Internal Audit now includes the protection of personal data in their risk assessment line.

An audit on the management of assignments/trips will take place towards the end of 2024 and the issue of personal data protection will be taken into account during the evaluation of the GDD system.

Finally, an audit of the implementation of the new Data Protection Regulation could be carried out at the end of the transitional period and as such regular exchanges between the Commissioner and the Internal Audit and Evaluation Directorate are necessary.

4.5 Administrative Tribunal (TACE)

The Commissioner also had contacts with the registry of the Administrative Tribunal which made it possible to explain the role of the Commissioner in relation to the TACE, to address various issues related to the anonymization of data and the confidentiality of data when using email. The Commissioner reiterated the need for a secure messaging system.

5. Data Protection Officer (DPO)

As mentioned above, the new Regulation provides in Article 13 for the establishment of at least one data protection officer who must be involved in all data protection matters. Their appointment is made based on their professional qualities, their ability to fulfil the tasks specified in the Regulation, and, in particular, their specialized knowledge of data protection standards and practices.

It should be noted that thanks to the arrival of the DPO, the protection of the data of agents and persons interacting with the Council of Europe has progressed and is beginning – albeit slowly – to be integrated by the Organisation's various services.

However, at present only one DPO is appointed within the Organisation. In accordance with the new Regulation, they handle the files applicable to all members of the Council of Europe Secretariat (agents, secondments, trainees) as well as external interlocutors (experts, consultants, participants in Council of Europe events, visitors) whose personal data are processed by the Council of Europe. These tasks are already considerable for one person, and internal collaboration is not always easy. It should also be noted that the issue of data mapping is becoming urgent for the Organisation and in the absence of a tool at the Council of Europe to manage this data, the task is also insurmountable for a single person.

During the reporting period, the Commissioner worked jointly with the DPO on various topics (adoption of the new Data Protection Regulation, the needs of the data mapping tool, the different privacy policies, in particular those relating to meetings using cameras and videoconferencing systems, requests for access by former Council of Europe employees to their personal data, etc…).

At their request, the Commissioner also gives their opinion on various projects and impact assessments relating to data protection. There are regular exchanges on these different subjects.

In addition, in 2024, the Commissioner and the DPO, with support from the Data Protection Unit and the HELP Unit (DG-1), worked jointly on the content of the internal training for Council of Europe staff to raise their awareness of data protection requirements. This work on e-learning, which is mandatory for all staff in the Organization, is still under development and is a priority.

6. Data security

Data security is enshrined in Article 6 "Data security" of the new Council of Europe Regulation on the protection of personal data. Article 6.5 provides for the obligation of the Data Protection Officer to inform the Commissioner in the event of data breaches. The Commissioner nevertheless reiterated that data breaches must be reported without delay to the Commissioner regardless of any information provided to the Secretary General.

During the past period, several security breaches or data protection breaches have been reported to the Commissioner. For each incident, the services concerned have shown great responsiveness and they have taken all necessary measures, in coordination with the Information Technology Directorate and the DPO.

Priority action must be taken by the Organisation to support the DIT, the DPO and the Commissioner in their efforts to address data security. This is even more important in light of new sensitive issues of the Organisation (in particular the functioning of the new Register of Damage for Ukraine, the willingness of the Organisation to consolidate its cooperation with certain democratic forces and representatives of civil society in exile, etc.).

7. Conclusions

With the adoption of its new Data Protection Regulation, a new era is dawning for the Council of Europe. The entry into force of this regulation is an important step to ensure respect for human rights and fundamental freedoms, including the right to privacy of individuals when processing personal data within the Organisation.

However, the regulatory text is not sufficient to ensure data protection. The Authority has already begun the process of complying with the Regulations. However, a priority must be placed on training and awareness-raising so that the various services and agents integrate data protection on a daily basis. After more than a year of entry into force, for example, data protection impact assessments are still too often carried out only as a follow-up to the intervention of the Commissioner or the DPO.

Human, financial, material and technical resources in particular to the DPO and the Commissioner should also be allocated quickly, which are essential to ensure the effectiveness of data protection within the Organisation. Unfortunately, this is not currently the case. At the moment, the DPO is overwhelmed and cannot accomplish all of their tasks. As for the Commissioner, who works on a voluntary basis, he can only count on limited support from the Data Protection Unit, which already does not have sufficient human and financial resources for the tasks assigned to it, not to mention the evaluation activities provided for in Convention 108+. As a result, it is not in a position to delve into the specific issues it has to deal with as much as it should, nor to carry out effective checks on compliance with data protection provisions.

In accordance with Convention 108+ and the Rules of Procedure, the General Secretariat must provide the Commissioner with the necessary resources for the effective performance of their duties and to exercise of their powers. Without adequate resources and the political will to give priority to the protection of personal data within the Council of Europe, the Regulation risks remaining a dead letter, undermining the credibility of the Organisation.