Activity Report of the Data Protection Commissioner

July 2015 - November 2017

Eva Souhrada-Kirchmayer
Council of Europe Data Protection Commissioner

TABLE OF CONTENTS

1 INTRODUCTION

The election, function and powers of the Data Protection Commissioner of the Council of Europe (hereafter DPC) are regulated in the Secretary General's Regulation of 17 April 1989[1] instituting a system of data protection for personal data files at the Council of Europe.

The DPC shall be elected by the Consultative Committee[2] on the basis of his/her genuine independence as well as experience and knowledge of challenges arising in the context of the implementation of data protection. The Consultative Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (hereafter "Convention 108") shall elect the DPC from a list of names drawn up by the Secretary General of the Council of Europe.

The term of office of the DPC shall be three years and may be renewed once.

The operational costs of the DPC shall be borne by the budget of the Council of Europe. The DPC may draw up rules of procedure.

In addition to ensuring respect for the principles set out in the 1989 Regulation, the DPC shall:

- Investigate complaints from individuals arising out of implementation of the 1989 Regulation after completion of the complaints procedure laid down in Article 59 of the Staff Regulations;
- Formulate opinions at the request of the Secretary General on any matter relating to implementation of the 1989 Regulation;
- Bring to the attention of the Secretary General any proposals for improvement of the system of data protection.

In the performance of his/her functions, the DPC shall be assured of the utmost co-operation from the Secretariat General.

If he/she so wishes the DPC may at all times make recommendations to the Secretary General.

In practice, the position of the DPC is only a function which is fulfilled by a data protection expert additionally to his/her main profession.

[1] The Regulation can be found here: http://www.coe.int/t/dghl/standardsetting/DataProtection/DP%20Regulation%2017%20april%201989%20CoE%20E%20_2_.pdf

[2] Article 18 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.

The current DPC was elected by the Consultative Committee of Convention 108 on 2 December 2011, with a term of mandate due in December 2014. As the next plenary meeting of the Consultative Committee (which is the competent committee for the election of the DPC) took place at the beginning of July 2015, her mandate was prolonged provisionally until this date. At the 32nd plenary meeting of the Consultative Committee (1-3 July 2015), she was re-elected for a second mandate of three years. The period covered by the present activity report runs from July 2015 to November 2017.

2 VISITS AND MEETINGS

2.1 AT THE COUNCIL OF EUROPE IN STRASBOURG

During the activity period the DPC undertook visits to the Council of Europe to meet with the top management as well as with employees (staff members) of the Council of Europe (”data subjects”) who expressed the wish to meet the DPC regarding data protection issues (see the list of dates of visits)[3].

The DPC frequently contacted the Director of Human Resources to deal both with specific individual cases or general practices. The dialogue and exchange of views between the Director of Human Resources and the DPC can be regarded as an on-going process.

Furthermore the DPC participated in various plenary and Bureau meetings of the Consultative Committee[4].

2.2 OTHER MEETINGS AND CONFERENCES

The DPC participated in the international data protection conferences in Amsterdam (26 – 29 October 2015) and Marrakesh (17 – 20 October 2016), where she held a lecture on the topic "Data Protection in the International System of Human Rights” at a side event organised by the GIZ.

She also participated in the Spring data protection conferences in Budapest (26-27 May 2016) and in Limassol (27- 28 April 2017).

The DPC was invited to the ETUI-ETUC Conference on 28 June 2016 on the topic “Shaping the new world” of work and held a presentation on Recommendation 2015(5) on the processing of personal data in the context of employment.

The Secretariat of the DPC also participated in the 6th Workshop on Data Protection within International Organisations in Geneva (11 – 12 May 2017), as well as in the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Hong-Kong (26-29 September 2017).The DPC also participated in a number of other panels and held lectures in Vienna.

[3] 2015 : 18 March, 8 June, 30 September and 1st October, 11 December
2016: 1-2 March, 13-14 September, 1-2 December
2017: 17 March, 4-5 October, 21 November.

[4] 37th Bureau meeting (9-11 December 2015), 40th Bureau meeting (30 November – 2 December 2016) and 39th Plenary meeting (22-24 November 2017)

3 ACTIONS TAKEN

The DPC asked for information concerning data protection matters in different areas and gave advice concerning a number of particular topics.

3.1 DIRECTORATE GENERAL OF ADMINISTRATION

3.1.1 Processing of personal data for psychological tests

The DPC was contacted regarding data processing of an employee in a Human Resources context, notably psychological tests. The DPC pointed out that the data subjects should be given full access to the results of the aforementioned tests. Confirmation was also obtained from the Directorate of Human Resources that such data concerning an employee of the Council of Europe have been deleted, both in electronic and hard forms in the Council of Europe's system as well as in the provider's system. Moreover, a copy of the contract for the provision of an online psychometric assessment system was sent to the DPC for verification.

3.1.2 Records Management and ERMS

The DPC has been informed by the Directorate of Information Technology that a Records Management (hereinafter RM)[5] Programme, associated with an Electronic Records Management System (hereinafter ERMS)[6],was being developed. In this context, the DPC provided comments and participated in a number of meetings taking place at the Council of Europe and issued a recommendation on the data protection implications linked to the implementation of this system.

The RM Programme provides a workflow creating alerts with a double verification enabling either the destruction of the records or the extension of the retention period. One of the advantages of the RM Programme is that in this system personal data are automatically deleted when the deletion date is reached (which does not mean that data that are no longer necessary before that pre-defined date should be kept). RM Programme also enables a stricter access management.

Furthermore, Data protection laws are generic in nature while recorded information may be variable in content, form, provenance, etc. An organisation's RM can refer when necessary to the DPC for review of new record types that may involve personal data.

[5] Records Management is the management of recorded information produced by and/or of use to the organisation with informational and/or evidential value. This includes the creation, reception, retention and destruction of recorded information in accordance with organisational needs and in compliance with applicable laws.

[6] ERMS can be described as aiming to manage records for the purpose of providing evidence of business activity. It does this by capturing contextual information (metadata) about the records being created, linking records involved in the same business activity, applying security controls to ensure the authenticity and integrity of the records and by imposing disposal authorities on the records held within the system.

The DPC noted that the fundamental principles of RM and data protection are remarkably similar. A well-structured, formalised RM programme promotes legal compliance by providing the necessary rules and processes that enable non-specialist staff to comply with a legal doctrine that does not specifically address the numerous situations that they face on a daily basis when creating, sharing, storing or deleting records containing personal data. The proposed ERMS furthermore provides a practical "Privacy-Enhancing Tool" that can integrate "user-friendly" compliance with applicable rules. A sound RM programme and a sound data protection compliance programme are mutually dependent and mutually supportive, for it is difficult to achieve successful implementation of the one without the other.

According to the DPC, an organisation that introduces a sound RM programme associated with an ERMS will have a strong tool to facilitate compliance with data protection regulations while simplifying and better framing access to useful recorded information.

The DPC recommended pursuing efforts to speedily implement the RM, associated with an ERMS in the Council of Europe and, therefore, be a role model in this field for member states.

3.1.3 Conduct of investigations into alleged fraud and corruption

The DPC worked with the Director of Internal Oversight concerning the draft of an Instruction on investigations into alleged fraud and corruption affecting the financial interests of the Organisation. The DPC proposed amendments regarding access to the content of individual electronic communications. In that respect, The DPC recommended that checks will solely be carried out on the basis of searches by key words related to the suspected fraud and/or corruption. Private emails should not be subject to digital forensic operations and in case of doubt, the DPC should be consulted. As for the records, the DPC suggested that if the assessment is not giving rise to an investigation, the file with the records of the proceedings shall not be kept more than five years. They shall also be anonymised as soon a personally identifiable format is no longer necessary.

3.1.4 Service provider contracts and standard data protection clauses

The DPC was contacted regarding the negotiation of a contract with a service provider, concerning the provision of Medical and Security Assistance services. The DPC proposed amendments to the drafts submitted, notably providing for a specific appendix containing data protection requirements stipulating in particular that appropriate technical and organisational measures to ensure security should be taken. The data received by the service provider should only be used for the purpose of the contract and complying with the relevant data protection legislation, including the Council of Europe's relevant regulations (rules regarding the processing of data, confidentiality, rights of access, rectification, deletion and objection, duty to provide information of the processing of data to the data subjects and to notify any data breaches, international transfers have thus been stipulated.

Furthermore, after the end of the provision of the service, the processor must delete or return all personal data to the controller. Finally, a written authorisation of the controller is required to enable the processor to engage another processor).

The DPC developed a model clause to be incorporated in the general conditions of DGA contracts that will be one amongst other safeguards which international organisations will have to offer in order to prove their "data protection adequacy". In this context, the DPC stressed once again the importance and urgency of updating the 1989 Regulation and recalled that the EU General Data Protection Regulation (hereinafter: "GDPR") provides that a transfer of personal data by entities which are subject to the GDPR to an international organisation may take place only on the basis of an adequacy test (adequacy decision issued by the European Commission or subject to appropriate safeguards in the absence of such a decision).

3.1.5 Official travels/contracts with suppliers

Following the meetings relating to the processing of personal data by the service provider in charge of official travels of the Organisation, the DPC recommended that a series of actions be taken with a view to ensuring a higher level of protection afforded by the Council of Europe.

Regarding the official travels, the DPC recommended that the existing contract signed between the Organisation and the service provider should contain standard data protection clauses as developed with the Directorate of Legal Advice. More generally, the tenders board should be informed of the necessity, for any contract to be signed by the Organisation and leading to the processing of personal data, to include in the call for tenders specific requirements relating to data protection. The DPC also formulated her wish to be consulted on the preparation of the 2019 contract with the supplier for travel services as it involves the processing of vast amounts of personal data including potential sensitive data.

Moreover, concerning the internal workflow tool used in the management of official travels ("*Gestion des déplacements*" - GDD) used for staff members and experts, the DPC recalled the importance of respecting the purpose limitation principle, which in this specific case is the organisation of official travels. Personal data processed in GDD should therefore not be used for other purposes. The DPC also recommended that the sensitivity and awareness of the staff using GDD should be raised, possibly through the internal network of travel correspondents.

3.1.6 Mediators and their secretariat

The DPC recommended that the contracts with Mediators hired by the Organisation be amended to include a confidentiality clause. Furthermore, regarding the sensitivity of some of the files dealt with by the Mediators, the DPC proposed that colleagues providing Secretariat services to them be requested to sign a confidentiality commitment.

3.2 PROCESSING OF EMPLOYEES' DATA FOR PURPOSES OF EMERGENCY

3.2.1 Use of private phone numbers in case of emergency

The DPC was consulted regarding the intention to make mandatory the provision of private mobile phone numbers in the GDD profiles of Council of Europe staff/experts. Such a measure aimed at enabling to reach travellers of the Council of Europe during a security threat/incident or other major disruption. The DPC underlined that staff/experts should have the ability to consent to give their private mobile phone numbers, and that the provision of such numbers could not be made mandatory.

A privacy statement was prepared relating to the processing of mobile phone numbers in the GDD which stipulates that the Administration of the Council of Europe requests its staff members and experts to indicate their mobile phone numbers at the moment of creation of a GDD profile and lays down the principles for the processing of private mobile phone numbers regarding namely access, security and the rights to verify, modify and delete the information. The option to create a GDD profile without providing a private mobile phone number is also provided.

3.3 INTRANET AND INTERNET

3.3.1 Wi-Fi and internal rules of the Information System

The DPC made recommendations on the compliance of the standards of monitoring the Council of Europe's internet use with applicable data protection safeguards. The aim of the recommendations was to ensure that any monitoring activity of internet use via Wi-Fi does not jeopardise baseline principles and safeguards of personal data protection, recalling in particular the principles of purpose limitation, proportionality and data conservation (data should not be kept for longer than needed). The recommendations also covered the need to implement appropriate measures to prevent data breaches as well as unauthorised data dissemination.

Furthermore, the recommendation stressed that the 1989 Regulation is applicable in the context of monitoring and that data processing activities of IT system administrators and that the DIT (Directorate of Information Technology) also falls under the mandate of the DPC and can thus be supervised by the DPC.

Regarding the Instruction 47 of 28 October 2003 on the use of the information system of the Council of Europe, the DPC raised concerns as to the risks of accessibility to private communications, failing to meet the protection afforded under Article 8 of the European Convention on Human Rights in the workplace. The DPC stressed that the data subjects (employees as well as "outsiders" i.e. experts or visitors) should be informed in advance in a clear and transparent manner of the possibility that the use of Internet via the Council of Europe Information System might be subject to monitoring by IT System Administrators.

As for the IT "Charter for Administrators of the System Information of the Council of Europe", the DPC was of the opinion that its legal status should be clarified, as only regulations can complement the 1989 Regulation.

The DPC suggested that amendments be made to both Instruction No. 47 and the Charter to integrate the points highlighted in the recommendation.

3.3.2 Guidelines for the use of social media

The DPC provided comments on the "guidelines for the use of social media at the Council of Europe" prepared by the Directorate of Communications. They concern the use of social media by staff members in their professional activities and aim at providing practical guidance on rules to follow when using social media.

3.3.3 Model of data protection statements for websites

The DPC provided comments on a general privacy statement for the Council of Europe website, as well as a Specific Privacy Statement relating to webpages offering the possibility to register personal information on specific restricted platforms (such as e-learning platform). The Specific Privacy Statement provides information to the data subject on the data collected, the purpose and means of processing, access and sharing policy, data security, length of conservation and rights of the data subject, including the possibility to contact the DPC.

3.3.4 Declaration of interests

The question put to the DPC was to know whether the European Directorate for the Quality of Medicines and HealthCare (EDQM) could make public the declaration of interests of the external experts, for the sake of transparency. The DPC highlighted firstly that regarding the access to declaration of interests for external experts, the DPC was not in favour of publishing the aforementioned declarations on the EDQM website as such declarations contain a large amount of personal data and that their publication would not be in compliance with personal data protection rules. The DPC pointed out that where a request would be made by an interested party to have access to it, consent of the data subject should be obtained before disclosing such a declaration. Secondly, concerning access to declarations made by staff members, the DPC was of the opinion that the declarations should be kept confidential and not disclosed to third parties.

4 REVISION OF THE INTERNAL RULES OF DATA PROTECTION

In 2010 the Consultative Committee of Convention 108 adopted proposals to amend the 1989 Regulation instituting a system of data protection for personal data files at the Council of Europe[7]. This proposal was sent to the Secretary General. In February 2012 the DPC met the Deputy Secretary General on this particular topic and to enquire about the follow up given to the proposals of the Consultative Committee. After her first experience by implementing the regulation, the DPC came to the conclusion (which seemed to be in line with the opinion of the Deputy Secretary General) that the regulation is in several points 'old-fashioned' and does not fit any more to specific situations, especially in the online-environment[8]. Furthermore some important elements which are contained in more recent data protection instruments are missing in the regulation[9] and the powers of the DPC lack behind other European instruments[10]. Furthermore the DPC should have the power to complain to a court when the Organisation does not comply with her/his decisions.

On the other hand the data subject should have the possibility to complain directly with the DPC, but also to challenge the decisions of the DPC and bring the case before a court. Therefore a fundamental reform of the internal protection rules of the Council of Europe will be necessary.

During the 4th Workshop on Data Protection of International Organisations in the World Customs Organisation (WCO) Headquarters in Brussels in November 2012 the DPC was informed that most international organisations dealing with data protection have developed, adopted and implemented detailed data protection rules successfully. Being such a large organisation as it is, the Council of Europe which furthermore deals particularly with questions of fundamental rights including data protection, should adopt and apply modern data protection rules in line with other generally acknowledged data protection instruments, particularly Convention 108 which has to be implemented by all member states of the Council of Europe (they have all ratified Convention 108).

Furthermore the Parliamentary Assembly Recommendation 1984 (2011) and Resolution 1843 (2011) highlighted the explicit need to strengthen the powers of the DPC of the Council of Europe.

As a consequence, a number of meetings with the responsible Directorates/Units of the Secretariat General including the Directorate of Legal Advice and Public International Law took place.

[7] T-PD-BUR (2010) 06 rev 2

[8] For example: it presents a problem that in case of the need of consent not only the explicit but also the written consent of the data subject is necessary.

[9] For example: the detailed provisions on lawfulness as well as the role and duties of a service provider.

[10] In other European data protection instruments the DPA has the power to issue binding decisions which can be executed. There is also a course of instances to the courts. Furthermore it is not reasonable that a data subject cannot file a complaint directly to the DPC, but has to firstly take action with the Director of Human Resources.

A consultant was tasked to prepare a draft regulation. A kick-off meeting with representatives of different units of the Council of Europe (DGA, Private Office, DLAPIL, Data Protection Unit, and Registry of the European Court of Human Rights), the consultant and the DPC took place on 18th March 2015. A first draft was delivered in May 2015. On 9 December 2015 the DPC had a meeting with the Deputy Secretary General of the Council of Europe and addressed the urgency of the new regulation and the need for a comprehensive regulation which also applies to the European Court of Human Rights as well as provisions which enable the DPC to fulfil her/his tasks efficiently.

On request of the DGA the draft was changed twice. After having explicitly asked for being consulted, the DPC received the drafts and gave her comments to the draft in February 2016, which were also sent to the Deputy Secretary General. During the 6th Workshop on Data Protection within International Organisations held at the IOM in Geneva (11 – 12 May 2017) it was also stressed that international organisations have to align their data protection rules with the GDPR to ensure an adequate level of data protection and create the necessary safeguards.

However, despite the repeated efforts of the DPC, there is still to date no result on this topic, and the DPC was told that there are still political questions open and that factual obstacles to the delivery of an updated regulation remain.

5 CONCLUSIONS

The DPC continues to urge for the revision of the internal regulation of the Council of Europe, which should be adapted to International and European data protection standards.

The DPC witnessed an increase in the awareness and understanding of key data protection requirements in various sectors of the Organisation (she has for instance been spontaneously consulted by different MAEs seeking for recommendations in order to ensure compliance with data protection principles).

At the same time, more resources and synergies are needed in order to ensure that a real and systematic culture of data protection be acquired at all levels and in all sectors of the Organisation.