COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

DPCOM Report 2011-2015

Activity Report of the Data Protection Commissioner

December 2011 - June 2015

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 17th 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 the problems connected with data protection. The Consultative Committee 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 this Regulation, the DPC shall:

- Investigate complaints from individuals arising out of implementation of this Regulation after completion of the complaints procedure laid down in Article 59 of the Staff Regulation;
- Formulate opinions at the request of the Secretary General on any matter relating to implementation of this 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 as an additional function which is fulfilled by a data protection expert additionally to his/her main profession.

The current DPC was elected by the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereafter T-PD) on 2nd December 2011. Therefore her mandate would have expired in December 2014. As the next plenary meeting of the T-PD (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 T-PD (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 December 2014 to July 2015.

[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.

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 several times[3]. At these visits different meetings with managers of the Organisation took place. Equally, meetings with employees of the Council of Europe (”data subjects”) were organised, whom had the wish to talk to the DPC about their data protection problems.

The DPC frequently contacted the Director of Human Resources to talk to him about specific cases or in general. The dialogue and exchange of views between the Director of Human Resources and the DPC can be regarded as an ongoing process.

Furthermore the DPC participated in the plenary meetings of the T-PD[4] and several Bureau meetings of the T-PD[5].

She participated in a meeting with the Sub-Committee on Media and Information Society of the Parliamentary Assembly which took place on 22nd April 2013 and was invited to give a statement in connection with the Follow-up to Recommendation 1984 (2011) on the protection of privacy and personal data on the internet and online media. After this statement an exchange of views between Members of the Parliamentary Assembly and the Protection Commissioner took place.

On 5th June 2014 the DPC participated in the European Conference of Data Protection Authorities in Strasbourg and acted as a speaker at a panel.

The DPC participated in the Colloquy ‘Common focus and autonomy of international administrative Tribunals in Strasbourg’, where the DPC presented her opinion and mentioned her recommendation concerning the anonymisation of judgments on the intranet/internet. In the following discussion a vivid debate on this question took place (19th-20th March 2015).

2.2 OTHER MEETINGS AND CONFERENCES

The DPC participated in a number of meetings outside Strasbourg, most notably:

- In the stakeholder consultation meeting[6] at the Fundamental Rights Agency in Vienna on 21st-22nd February 2012;
- In the 31st Council of Europe Conference of Ministers of Justice[7] in Vienna on 19th September 2012;
- In the 4th Workshop on Data Protection in International Organisations in the Word Customs Organisation (WCO) Headquarters in Brussels on 8th-9th November 2012;
- In the expert review meeting on biometric data[8] at the Fundamental Rights Agency (FRA) in Vienna on 17th September 2013;

[3] Dates: 8th February 2012, 21st-22nd June 2012, 29th-30th November 2012, 27th May 2013, 14th October 2013, 17th December 2013, 12th May 2014, 18th September 2014, 18th-19th December 2014, 18th and 20th March 2015, 8th June 2015.
[4] Dates: 19th-22nd June 2012, 27th-30th November 2012, 15th-18th October 2013, 2nd-4th June 2014.
[5] Dates: 6th-8th February 2012, 27th-28th September 2012, 5th-7th February 2013, 28th-29th May 2013, 18th-20th December 2013, 17th-18th December 2014.
[6] “Data Protection: Redress Mechanisms and Their Use”.
[7] “Responses of Justice to Urban Violence – Joint meeting of the Chairpersons of the Council of Europe, Committees and Mechanisms”.
[8] “Biometric Data in Large IT Databases in the Areas of Borders, Visa and Asylum – Fundamental Rights Implications”.

- In the CDPD conference acting as a speaker in January 2014 in Brussels (23rd January 2014);
- In the ceremony concerning the 'European Data Protection Day' dedicated to the modernisation of Convention 108 and the Council of Europe in the Federal Chancellery in Vienna where the DPC held a short speech on data protection in the Council of Europe and the role of the DPC (24th January 2014).

The DPC participated also in a number of other panels, including but not limited to: 'Vergangenheit und Zukunft des Datenschutzes in Europa' on 8th May 2014 at the Renner-Institut and in a panel on biometric data and data protection on 13th October 2014 at the 'Depot' in Vienna.

3 ACTIONS TAKEN

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

3.1 DIRECTORATE OF HUMAN RESOURCES (DHR)

The DPC had a number of meetings with the DHR. Specific topics were discussed like the list of all automated or manual files kept by the Council of Europe, concrete complaint procedures, the processing of data in "public folders" and general questions regarding complaints procedures. The DPC gave also advice to the DHR concerning data protection questions referring to the appraisal system.

3.1.1 Health data

The DPC had a meeting with the doctor of the Council of Europe. She was informed that health data are only used for the treatment of employees and that they are not transferred to the DHR. Furthermore the health data are encrypted.

The DPC gave advice to a research assistant about the use of health data for research purposes and recommended to use sensitive data after the removal of identification data.

Regarding the processing of personal data in the context of psychological tests taken by staff members on a voluntary basis, the DPC obtained confirmation that the full results of such tests could be communicated to staff members who would request them. She also checked the service contract with the internal provider carrying out the tests in order to assess the obligations of the provider and the deletion of the data.

3.1.2 Data processing for appraisal purposes

The DPC was consulted regarding the transfer of personal data to a service provider for appraisal purposes. The DPC recommended the Organisation to remove the identification data and replace them by a code before transferring these data to the service provider.

3.1.3 Processing of personal data for recruitment purposes

The DPC was contacted regarding data processing for recruitment purposes. The DPC pointed out that such data must not be stored for an indefinite time without the consent of the data subjects. Such data may only be processed for a certain time without the consent of the

data subjects as long as there is another legal basis, for example if there are deadlines for complaints etc. One crucial issue is the information of the data subject about the length of storage of his/her data. Recruitment data must not be used for other purposes than the original purpose and closely linked purposes (e.g. to deal with complaints in connection with the original purpose).

3.1.4 Data contained in employment certificates

The DPC is of the opinion that certificates established according to Article 48 of the Staff Regulations must be issued without asking the employee for the reasons of his/her request. However, it must be clear that only certificates containing the information mentioned in Article 48 must be given without asking for reasons. This provision does not contain any obligation of the employer to provide information which goes beyond the mentioned elements of information. If a certificate which should contain further information is requested by the staff member, it is not excluded that the employer may ask for the reasons before providing this information to the data subject. This does not address the right of access of the data subject to obtain his/her own data which can be exercised without explaining any reasons. However, it must be clear that the right of access is not identical to the right to ask for a certificate from the employer (which would therefore commit the employer in respect of the information certified).

3.1.5 Use of a records management programme

The DPC recommended the Council of Europe in general, and the DHR in particular, to begin using a Records Management Programme [9] (hereinafter RMP), associated with ERMS[10] (hereinafter ERMS). The DPC gave her comments on several documents referring to these systems and participated in a number of meetings on this subject in the Council of Europe.

The RMP 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 RMP is that in these new systems personal data are automatically deleted when the deletion date is reached (which does not mean that data no longer necessary before that pre-defined date should be kept). RMP also enables a stricter access management.

The DPC found that the newly developed system would help to avoid the duplication of data collection and even to facilitate organisation-wide compliance with internal and external regulations.

3.2 PROCESSING OF EMPLOYEES' DATA FOR PURPOSES OF EMERGENCY

The DPC was contacted concerning the question of the processing of personal data like private and official contacts (addresses and mobile/home phone numbers) of staff members

[9] Records Management, also known as 'Records and Information Management' is the administration 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. It is also known as.

[10] Electronic Recruitment Management System is used with the aim 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.
http://erecords.wikidot.com/what-is-edms-and-erms

to reach them in case of a crisis. It might also be necessary to provide their phone numbers to a partner organisation or an embassy who will take responsibility to evacuate the staff from a duty station.

The DPC acknowledged (as it was also estimated by the legal service of the Council of Europe) that the processing of phone numbers and other contact details of employees falls in principle under the 'Internal Administrative Tasks' of the Council of Europe. However, the question if the collection of contact data of certain third persons (e.g. relatives, spouses) falls also under 'Internal Administrative Tasks' might depend on the specific circumstances and has to be interpreted restrictedly. In cases of doubt the data subjects must be asked for their consent. In any case the data subject has to be informed and has the right to object. The use of any sensitive data must be based on the explicit and written consent of the data subject.

3.3 INTRANET AND INTERNET

3.3.1 Publication of pictures and videos

The DPC was consulted concerning the publication of personal data of staff members on the intranet. At the moment there is no specific regulation existing dealing with this issue. Therefore the Secretary General's Regulation outlining a data protection system for personal data files in the Council of Europe is the only basis to deal with such questions.

The DPC intervened in order to obtain deletion of sensitive data which was filed in a public folder. She pointed out that an e-mail exchange of such kind of data (e-mails between managers that exchange sensitive data of an employee) should not only be avoided, but in any case should not be put into a public folder.

3.3.2 Personal data used for archiving purposes

The DPC was contacted the Council of Europe has the right to publish administrative documents, including personal data, on the Internet once it has been declassified. The DPC pointed out that the processing of these data falls under the Secretary General's Regulation outlining a data protection system for personal data files in the Council of Europe. It would be possible that an internal regulation on the use of data for archiving purposes could be drafted in accordance with the procedure laid down in Article 2 Paragraph 2 and Article 6(b) and 6(c) of the Appendix to this Regulation.

3.3.3 Use of analytic tools by the Council of Europe in its function as website operator

The Council of Europe uses the software instrument of Google Analytics as audience measuring tool on the websites of the Council of Europe. In the last years it became obvious that the use of Google Analytics in its original form is not in conformity with European data protection law. A meeting between the Directorate of Information Technologies, the Directorate of Communication, the Directorate of Legal Advice and Public International Law, the Data Protection and Cybercrime Division and the DPC took place on 30th November 2012. Subsequently, the Commissioner was asked to give her advice on the use of analytic tools by the Council of Europe.

Google Analytics is a service offered by Google that generates detailed statistics about a website´s traffic and traffic sources and measures conversions and sales. Google Analytics uses "cookies", which are text files placed on the computer, to help the website analyse how users use the site. The information generated by the cookie about the use of the website

(including their IP-address) of the users are transmitted to and stored by Google on servers in the United States. Google uses this information for the purpose of evaluating the use of the website by the users, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf.

Different European Data Protection Commissioners came to the conclusion that Google Analytics is not in line with European data protection legislation. Google Analytics therefore raises some privacy concerns. In the last years the German data protection authorities under the leadership of the competent authority, the Commissioner for Data Protection and Freedom of Information of Hamburg, entered into negotiations with Google which finally led to a solution which was acknowledged as in conformity with German data protection law.

After examining the mentioned solution and after a detailed legal analysis the DPC came to the conclusion to recommend that if analytic tools are used by the Council of Europe:

The Council of Europe has to conclude a data processing agreement with the provider of the analytic tool containing the obligation of the provider to act only on the instructions of the customer (hereafter CoE). The processing of personal data on behalf the CoE includes certain control obligations on the part of the CoE, with which the provider will support the CoE by providing appropriate proof.

On the website users must find information about the privacy policy of the CoE. This privacy policy must contain information what kind of personal data of the users is collected and processed for which purposes and which provider is processing these data. The user must be made aware of his/her possibility to object to the collection and processing of their personal data (opt-out) by the CoE via this processor. Furthermore this information should be provided when a user visits the website of the CoE for the first time.

The life duration of tracking cookies should be as short as possible.

IP-addresses may only be used to create a pseudonym and shall not be used for analysing the behaviour of a data subject, unless the data subject has given his/her explicit consent. The CoE should use appropriate settings in the program code to shorten and make anonymous IP-addresses.

It would be advisable to avoid third parties cookies. However, if such cookies are used, the explicit consent of the data subject must be given. In such a case the privacy policy must be clear on that and the user must be given the opportunity to consent explicitly.

The use of personal data collected and processed for statistical purposes for other purposes than statistics should be avoided. Without the informed and explicit consent of the data subject such a transfer would be illegal in any case.

If an analytic tool which is not in line with the above mentioned requirements has already been integrated into the web page, it must be assumed that personal data have been collected unlawfully. These old data must be deleted.

Further to the DPC's recommendation, the use of Google analytics was abandoned and another software platform was used in its place.

3.4 THIRD PARTIES

3.4.1 Data processing for investigation purposes

The DPC is of the opinion that the instructions on investigations should be amended in order to strictly define the extent of powers in the conduct of an investigation and which personal data may be collected and processed in this connection. A sufficient legal basis is in particular necessary in view of the use of sensitive data. Furthermore there must be a clear border between those tasks which may only be exercised by the police and internal investigations operated by the Council of Europe.

3.4.2 The service provider in third states

The DPC was contacted regarding the transfer of personal data to a service provider located in outside Europe, and which, on the basis of the conditions for data processing and the general data protection policy of this service provider, would not comply with European data protection rules. Therefore the DPC advised the Unit not to conclude a contract with this enterprise and preferably use a European service provider.

3.5 INTERNAL SECURITY

The DPC had a meeting with the Directorate of Logistics regarding the processing of data through video surveillance, exclusively taking place for security purposes.

The DPC asked for information on the use of badges and was informed that data which are processed by the use of badges are only accessible to a very limited number of persons and that these data are deleted within a defined period of 10 days.

3.6 PUBLICATIONS OF NAMES IN JUDGEMENTS

3.6.1 European Court of Human Rights

The DPC received several complaints of individuals whose name were published in judgements of the European Courts of Human Rights (ECHR). As even the justice administration of the ECHR is exempted explicitly from the Secretary General's regulation on data protection, the DPC was not able to intervene in such cases due to a lack of expertise in this area.

According to the Rules of the Court (Rules 33 and 47) a request of anonymisation can be sent to the Registry of the Court. However if this request is rejected by the President of the Court the data subject has no possibility to complain with the DPC.

3.6.2 Administrative tribunal

The DPC received several complaints of staff members, but also of representatives of the trade union in the Council of Europe whom complained about the publication of names of employees in judgements of the Administrative Tribunal, in particular in the intranet/internet.

Decisions of the Administrative Tribunal are published on the Council of Europe intranet/internet website. No regular anonymisation takes place. If a data subject asks the Administrative Tribunal for anonymisation, the decision on this question is taken by the chairman of the Tribunal. There is no right of objection for the data subject; his/her objection

to the publication of his/her data contained in a judgment of the Tribunal is not compulsorily followed by the chair.

If a person uses search engines and enters the name of an employee of the Council of Europe, he/she obtains also the full text of judgements linked to this individual.

In various Member States of the Council of Europe, decisions of courts and tribunals may - in principal - only be published in an anonymised version. In other member states, at least the problem of publishing those data in the internet is regarded as a specific problem.

The fact that names and other circumstances regarding the involved persons are used in oral proceedings does not mean that these data are publicly available in general. It can be assumed that normally there are only a limited number of interested persons who follow a public hearing of an administrative tribunal.

However, new technologies, such as the internet, offer a wide range of possibilities to find and connect data about specific individuals. Those measures are much more intrusive than a limited publicity during a public hearing. As mentioned above, with the support of search engines it is possible to link personal data from different areas and use it for creating profiles of an individual. For example, it is quite usual that employers use search engines to gain information about possibly future or current employees. Furthermore it must be taken into account that the publication of a judgement *'in extenso'*[11] could also contain sensitive information on the data subjects, such as the content of his/her personals files or personal e-mails etc. Therefore, the fact that a person was involved in a court procedure or especially a negative decision concerning this employee can damage the reputation of this person and have negative effects on his/her future career.

The question of the applicability of the Secretary's General Regulation of 17th April 1989 instituting a system of data protection for personal data files at the Council of Europe to the publication of judgements of the Administrative Tribunal had to be examined. The text of the regulation remains silent on its concrete scope of application, but does not exclude files which are used in the administration of justice.

As mentioned above it is regulated that the judgements of the Administrative Tribunal are published by the Secretary General. However, in practice the decision to publish or not the name of a person is taken by the Chair of the Administrative Tribunal. This does not exclude that the 1989 Regulation is applicable.

Therefore the DPC issued a recommendation to the Secretary General and the Administrative tribunal that in the case of publication of judgements on the Council of Europe internet or intranet pages it is recommended to ask to the data subjects for their (express and written) consent before publication, or to anonymise the names of the concerned individuals, i.e. in particular parties and witnesses (as far as they are natural persons who are not professional representatives like solicitors) contained in the decisions before publication.

This recommendation dating from 2012 has not been followed yet. The DPC obtained a letter from the Chairman of the Administrative Tribunal that it was decided not to change the current practice, but to improve the information on the website of the Administrative Tribunal. During the Colloquy 'Common Focus and Autonomy of International Administrative Tribunals

[11] *In extenso*: "in full length". A Latin phrase used in legal writings.

in Strasbourg', which took place to the 50th anniversary of the Administrative Tribunal, a debate on the anonymisation of judgements took place, where several speakers shared the view of the DPC. Consequently, this question remains an open point on the agenda of the DPC.

4 LIST OF FILES

According to Article 5 of the Regulation outlining a data protection system for personal data files in the Council of Europe, a list of all automated or manual files kept by the Organisation shall be deposited with the DPC. The list shall specify the person or body responsible for each particular file, the sort of data contained on the file, the persons or bodies to whom the data may be communicated, and the purposes for which communication may legitimately take place.

Any proposal aimed at automating particular files or introducing new data processing techniques shall be communicated to the DPC.

Although foreseen in the quoted regulation stemming from 1989, the list had not been drawn up. The DPC requested the list foreseen in the Regulation and received a compilation of different data processing applications which are done by the Council of Europe. The list is not 'standardised' per se, instead only a compilation of documents in a variety of formats and therefore not in an appropriate format to be published in the intranet of the Council of Europe. However it can serve as a useful instrument for the DPC.

Some details of the list are still missing and will be hopefully completed soon.

5 REVISION OF THE INTERNAL RULES OF DATA PROTECTION

In 2010 the T-PD adopted proposals to amend the Secretary General's Regulation of 17th April 1989 instituting a system of data protection for personal data files at the Council of Europe[12]. This proposal was sent to the Secretary General. However, the regulation was not changed in the following time. In February 2012 the DPC met the Deputy Secretary General to talk about the follow-up of the T-PD proposal. 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[13]. Furthermore some important elements which are contained in more recent data protection instruments are missing in the regulation[14] and the powers of the DPC lack behind other European instruments[15]. Furthermore the DPC should have the power to complain to a court when the Organisation does not comply with her/his decisions.

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

[13] 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.

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

[15] 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 complain directly with the DPC, but has to complain firstly with the Director of Human Resources.

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 the member states of the Council of Europe that are parties to it.

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.

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 Court of Human Rights), the consultant and the DPC took place on 18th March 2015. A first draft was delivered in May 2015. The DPC is expecting to be consulted by the DLAPIL on this draft.

6 CONCLUSIONS

One of the recurrent activities of the DPC is to give advice to employees as well as to managers of the Council of Europe whose daily work or specific projects also touch upon data protection questions. As far as managers ask for advice themselves, the kind of informal consultation procedure that has been generally followed is largely satisfactory in practise.

However, the legal tools which are available to the DPC to improve data protection in the Council of Europe and to ensure the rights of the “data subjects” are not sufficient. For example, if a recommendation of the DPC is not followed, which actually happens, the DPC has no possibility to enforce it and to issue a binding decision vis-à-vis the concerned controller(s). Furthermore, according to the current internal data protection regulation, an employee has no possibility to lodge a complaint directly with the DPC, but he/she has to contact the Director of Human Resources firs, which might constitute an obstacle for the data subject. It is not satisfactory either, that justice administration of the European Court of Human Rights, i.e. when it is not acting in its judicial capacity, is completely exempted from the scope of the internal data protection regulation and cannot be supervised by the DPC.

Regarding the financial situation of the DPC, the DPC has no distinct budget line, nor is any budget for the DPC foreseen in the general budget of the Council of Europe. For example,

the DPC was invited to attend a panel at the International Data Protection Conference which took place in Mauritius in 2014, but she was unable to attend the conference due to a lack of budgetary means.

Therefore it seems to be of utmost importance that the internal regulation of the Council of Europe shall be adapted to European data protection standards.